Cisco Catalyst Center Rogue Management and aWIPS Application Quick Start Guide, Release 3.2.x

Cisco Catalyst Center
Updated May 5, 2026

© 2023-2025 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 New and changed information.....7

New and changed information.....8

2 Catalyst Center Rogue Management and aWIPS Application.....9

Introduction to the Rogue Management and aWIPS application.....10

About Rogue Management.....11

About Advanced Wireless Intrusion Prevention System.....12

Scale information.....15

Basic setup workflow.....17

3 Install Catalyst Center Rogue Management Application Package.....19

Application management.....20

Download and Install the Rogue Management and aWIPS application package.....20

4 Monitor the Rogue and aWIPS Dashboard.....21

Access the Rogue Management and aWIPS application.....22

Monitor the Rogue Management and aWIPS dashboard.....22

Monitor network rogue threats.....26

Get rogue AP and rogue client details from the Threat 360° view.....29

Download aWIPS profile forensic capture from the Threat 360° view.....32

View details of all rogue APs on a floor in a floor map.....32

Deploy your device configurations now or later.....33

Preview and deploy your device configurations.....34

5 aWIPS Profiles.....37

About aWIPS profiles.....38

Prerequisites for aWIPS profile.....38

Create an aWIPS profile configuration workflow.....39

View an aWIPS profile.....41

Assign an aWIPS profile to the network device.....42

Edit an aWIPS profile.....43

Delete an aWIPS profile.....43

Enable or disable aWIPS or aWIPS forensic capture.....44

6 Rogue AP Containment on Wired and Wireless Networks.....47

Rogue AP Containment overview.....48

Wired rogue AP containment.....48

Wireless Rogue AP Containment....49
Cisco Rogue AP Containment Actions Compatibility Matrix....52
View tasks and audit logs of rogue AP containment type....53

7 Custom Classification of Rogue APs....55
About the allowed list workflow....56
Set up the allowed list workflow....56
About custom rogue rule creation....57
Edit a rogue rule....58
Delete a rogue rule....58
Create a custom rogue rule....59
About rogue rule profiles....60
Edit a rogue rule profile....61
Delete a rogue rule profile....62
Create a rogue rule profile....62
View the allowed access points list....63
About the allowed vendor list....63
View vendor rule list information....64
Edit a vendor rule....64
Delete a vendor rule....64
Create a list of allowed vendors....65

8 Rogue and aWIPS Event Notifications....67
Information about the rogue and aWIPS event notifications....68
Rogue events....68
aWIPS events....69

1 New and changed information

Topics:

- New and changed information

New and changed information

Outlines the new features introduced in Catalyst Center Release 3.2.2, specifically highlighting the addition of outdoor area support. This feature is now integrated into the Site Selector for various dashlets, including Overview, Threats, Rogues on Map, Allowed List, and Rules, to enhance location-based network management.

This table summarizes the new and changed features in Catalyst Center Release 3.2.2 and tells you where they are documented.

Table 1: New and changed features for Catalyst Center Release 3.2.2

Feature	Description

Outdoor area support	If **Try Outdoor Area** feature is enabled in Catalyst Center, you will find the outdoor area selection option in the **Site Selector** window in these dashlets.
	- Overview
	- Threats
	  - Threat table > Detecting AP Site
	- Rogues on Map
	- Allowed List
	  - Create Allowed Vendor List
	- Rules
	  - Create Rogue Rule Profile

2 Catalyst Center Rogue Management and aWIPS Application

Topics:

- Introduction to the Rogue Management and aWIPS application
- About Rogue Management
- About Advanced Wireless Intrusion Prevention System
- Scale information
- Basic setup workflow

Introduction to the Rogue Management and aWIPS application

The Rogue Management application is an optional package for Catalyst Center.

After installation, the application helps you monitor threats from unauthorized access points (APs). You can access the Rogue Management functionality as a dashboard within Cisco Catalyst Assurance in the Catalyst Center GUI.

Note:

The Rogue Management and aWIPS application package is applicable for virtual appliances (VAs).

Because the Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is integrated with Catalyst 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 Catalyst Center. This guide also explains prerequisites and configurations, describes how to monitor the rogue and aWIPS dashboard, and offers important notes and limitations.

Note:

- The provisioning actions like rogue and aWIPS subscription enable and disable are supported for IPv6 deployment.
- The provisioning actions like aWIPS profile configuration and manual containment or automatic containment for wired and wireless devices are not supported for IPv6 deployment.

The Rogue Management application supports these 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

These 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 application supports Cisco Catalyst 9800 Series Wireless Controller Release 17.1.x and later Cisco Catalyst 9100 Series Access Points, and Cisco 802.11ac Wave 2 Aironet Access Points.

These 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

Outlines the Rogue Management application in Catalyst Center, which detects and classifies unauthorized APs to mitigate security risks. Details the classification process for rogue devices, including Rogue on wire, Honeypot, Interferer, and Neighbor states, to help administrators identify and monitor potential network threats effectively.

The Rogue Management application in Catalyst Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Catalyst Center helps you quickly identify the highest-priority threats and allows you to monitor these threats in the **Rogue and aWIPS** dashboard within Cisco Catalyst 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 existing LANs and build ad hoc wireless networks without the 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, unauthorized users can easily use the AP to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure AP locations, which increases the odds of enterprise security breaches.

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

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

- If the unknown AP is not managed by Catalyst Center, Catalyst Center applies the rogue classification rules.
- If the unknown AP is not using the same SSID as your network, Catalyst 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, Catalyst Center classifies the AP as **Rogue on wire**.

  Cisco switches managed by Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center, and is using the same SSID as your network, Catalyst Center classifies the AP as a **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 Catalyst Center. The Honeypot classification does not happen when the detected SSID is not restored back on Catalyst Center when the Catalyst 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, Catalyst Center verifies whether it is causing any interference. If it is, Catalyst 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, Catalyst Center verifies whether it is a neighbor. If it is a neighbor, Catalyst Center classifies the AP as **Neighbor** and marks the rogue state as **Informational**. A rogue AP is classified as a neighbor AP if the threshold level is less than or equal to -75 dBm.

About Advanced Wireless Intrusion Prevention System

Introduces the Cisco Advanced Wireless Intrusion Prevention System (aWIPS), which integrates with Catalyst Center to provide comprehensive wireless threat detection. Details the system's monitoring capabilities and lists the specific denial of service (DoS) attack signatures, including various flood and impersonation techniques, that it can proactively identify and mitigate.

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.

Because the aWIPS functionality is integrated into Catalyst Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

aWIPS supports these capabilities:

- static signatures
- standalone signature detection
- alarms, and
- static signature file packaged with controller and AP image.

Catalyst Center supports these signatures that detect various denial of service (DoS) attacks:

- **AP impersonation**: AP impersonation is when a Rogue AP is trying to spoof or impersonate a managed AP in Catalyst Center. The Rogue AP assumes the same BSSID and ESSID of a valid AP.
- **Authentication flood**: A form of DoS attack that floods an AP's 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.
- **Beacon DS attack**: A Rogue AP that impersonates the Beacon Frame also. Beacon Frames are used to advertise the connection characteristics to all the Clients in its vicinity.

- **Beacon wrong channel**: Beacon wrong channel occurs when a rogue AP transmits the beacon packets on a channel that differs from the channel advertised by the managed APs beacon frame. This is a type of AP impersonation attack.
- **CTS flood**: A form of DoS attack when a specific device sends a bulk Clear To Send (CTS) control packet to wireless devices sharing the same radio frequency (RF) medium, and blocking wireless devices from using the RF medium until CTS flood stops.
- **RTS flood**: A form of DoS attack when a specific device sends a bulk RTS control packet to an AP for blocking wireless bandwidth, which leads to performance disturbance for the 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 in immediately 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 a disassociation broadcast to disconnect all the 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 because of 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 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 thus, a DoS 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 is 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 Add Acknowledgment (ADDBA) request to the AP. This request contains sequence numbers to inform the AP of the size of the block being transmitted. The AP then accepts all the 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 is completed.
- **EAPOL-start v1 flood**: 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**: An invalid, unexpected, or random data is introduced into the beacon. The modified frames are then replayed into the air. This can cause unexpected behavior in the destination device, including driver crashes, operating system crashes, and stack-based overflows, which allows execution of arbitrary code on the affected system.
- **Fuzzed probe request**: An invalid, unexpected, or random data is introduced into a probe request. The modified frames are then replayed into the air.
- **Fuzzed probe response**: An invalid, unexpected, or random data is introduced into a probe response. The modified frames are then replayed into the air.
- **Invalid MAC OUI frame**: A spoofed MAC address, which does not have a valid OUI, is used.
- **Malformed association request**: An attacker sends a malformed association request, which can trigger a bug in an AP, leading to a DoS attack.
- **Malformed authentication**: An attacker sends malformed authentication frames, which can expose vulnerabilities, if any, in some drivers.
- **Probe response flood**: A form of DoS that allows an attacker to prevent a station from associating with a valid corporate AP. In a typical wireless transaction, when a station wants to associate with an AP, it transmits a probe request from to obtain information about the AP's network. The station then waits 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 DoS attack is initiated.
- **PS poll flood**: A potential hacker spoofs the MAC address of a 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 the client missing the data frames because it could be in the power save mode.
- **Reassociation request flood**: A form of DoS attack that exhausts an AP's resources, particularly the client association table by flooding the AP with a large number of emulated and spoofed client reassociations. When the client association table overflows, legitimate clients are not able to get associated, causing a DoS attack.
- **Targeted deauthentication**: There is visibility into both the source and the destination of attacks for enhanced context of the threat.
- **CTS virtual carrier sense attack**: A form of DoS attack when the MAC address of an 802.11n AP is modified. This 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 the MAC address of an 802.11n AP is modified. This allows large-duration values for Request To Send (RTS) frame types by preventing channel access to legitimate users.

Scale information

Details the supported capacity for rogue APs, clients, and aWIPS events across various Catalyst Center appliances. Outlines recommended WLC configurations to optimize rogue detection performance by filtering update volume and reducing reporting noise in the management interface.

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

Table 2: Number of Rogue APs and Rogue clients supported

Catalyst Center appliance	No. of Rogue APs supported	No. of Rogue clients supported	No. of aWIPS events per day
44-core Catalyst Center appliance	24,000	32,000	20,000
56-core Catalyst Center appliance	24,000	32,000	30,000
112-core Catalyst Center appliance	96,000	128,000	65,000

Reducing Rogue updates and enhancing Catalyst Center performance with WLC Rogue configuration

The provided configurations are designed to optimize rogue detection and reporting on Cisco Wireless LAN Controllers (WLCs), specifically to reduce the volume of rogue updates sent to Catalyst Center. This optimization improves the loading performance of the **Rogue Overview** page and **Threats** page by filtering out less significant rogue events.

These commands collectively help tune the rogue detection parameters to align with your network's requirements. As a result, Catalyst Center receives more relevant and actionable rogue intelligence, which improves the performance of monitoring interfaces.

Note:

While these recommended values align with Cisco's best practices, it's essential to customize these parameters for your network's unique characteristics and demands.

Command	Configuration details
`wireless wps rogue ap notify-min-rssi -75`	• **Purpose**: Sets the minimum Received Signal Strength Indicator (RSSI) threshold for rogue APs. • **Application**: Apply this configuration to all AP Join profiles. • **Effect**: Only rogue APs detected with an RSSI stronger than -75 dBm are reported. This filters out distant or weak rogue signals (such as -90 dBm) that are far from your managed APs and unlikely to pose a significant threat. It reduces noise in Catalyst Center.
`rogue detection min-transient-time 900`	• **Purpose**: Reduces the number of rogue updates for very short-lived rogue APs. • **Application**: Apply this setting to all AP Join profiles. • **Effect**: Catalyst Center receives reports only for rogue APs that remain active for at least 900 seconds (15 minutes). This prevents alerts for transient signals and focuses reporting on persistent rogue presences.
`wireless wps rogue ap timeout 1200`	• **Purpose**: Defines how long a rogue AP must remain stale (undetected) before the WLC reports it as deleted to the Catalyst Center. • **Application**: Apply globally on all the WLC. • **Effect**: Setting this to 1200 seconds (20 minutes) prevents frequent deleted reports for rogues that briefly go offline or move out of range, so only persistently absent rogues are marked as deleted.
`wireless wps rogue ap notify-rssi-de▶ viation 10`	• **Purpose**: Controls when the WLC notifies Catalyst Center about changes in a rogue AP's RSSI. • **Application**: Apply globally on the WLC. • **Effect**: The WLC notifies Catalyst Center only if the rogue AP’s RSSI changes by plus or minus 10 dBm or more. This reduces the number of updates caused by insignificant signal fluctuations.
`wireless wps rogue client notify-rssi-deviation 10`	

Command	Configuration details
	• **Purpose**: Similar to the rogue AP RSSI deviation, this command controls notifications for rogue client RSSI changes. • **Application** Apply globally on the WLC. • **Effect**: The WLC notifies Catalyst Center only if the rogue client's RSSI changes by plus or minus 10 dBm or more, which minimizes updates for small signal variations.

Basic setup workflow

Guides you through the basic setup workflow for the Rogue Management and aWIPS application in Catalyst Center. This includes installing the package, discovering devices, designing the network hierarchy, and configuring optional integrations like Cisco ISE and Cisco Spaces/CMX to ensure effective threat monitoring and management.

Procedure

1. Install Catalyst Center.

   For more information, see the *Cisco Catalyst Center Installation Guide*.

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

   For more information, see Download and Install the Rogue Management and aWIPS application package on page 20.

3. Enable the Rogue and aWIPS application in the **Assurance** > **Rogue and aWIPS** window.

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

   To access the Rogue and aWIPS application, log in to Catalyst Center. From the main menu, choose **Assurance** > **Rogue and aWIPS**.

4. 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.

   Note:

   If the device is removed from Catalyst Center without enabling a configuration cleanup, the older subscriptions remain intact. If you add the device again to Catalyst Center, existing telemetry subscriptions cause data to flow in, and the dashboard displays rogue and aWIPS threat data. To correct the telemetry subscriptions, assign the device to a site.

5. 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.

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

   You can either create a new network hierarchy or import an existing network hierarchy from Cisco Prime Infrastructure into Catalyst Center.

7. Add the location information of APs and position the APs on the floor map to get a coverage heatmap visualization.
8. (Optional) If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Cisco Catalyst Assurance for Cisco ISE integration. This enables you to see more information about wired clients, such as

the username and operating system, in Cisco Catalyst Assurance. For more information, see "About Cisco ISE Configuration for Catalyst Center" in the *Cisco Catalyst Assurance User Guide*.

9. (Optional) Create access groups that permit or restrict user access to specific Catalyst Center functions and sites. The Rogue and aWIPS feature behavior depends on the user role and site defined in the access group. For more information, see "Catalyst Center user role permissions", "Configure site-based, role-based access control" and "Impact of SRBAC on Catalyst Center features" in *Cisco Catalyst Center Administrator Guide*.
10. Start using the Cisco Rogue and aWIPS application.
11. (Optional) Integrate and synchronize Cisco Spaces/Cisco Connected Mobile Experiences (CMX) with Catalyst Center. For more information, see "About Cisco Connected Mobile Experiences Integration" in the *Cisco Catalyst Assurance User Guide*.

    You can get the precise location details for a specific rogue AP on the floor map by using the detecting AP's strongest signal strength or the x and y coordinates from Cisco CMX.

    Note:

    If Cisco Spaces/Cisco CMX is not integrated with Catalyst Center, the site map displays the rogue AP near the detecting AP with the strongest RSSI.

3 Install Catalyst Center Rogue Management Application Package

Topics:

- Application management
- Download and Install the Rogue Management and aWIPS application package

Application management

Outlines the modular application management approach in Catalyst Center, where functions are packaged separately from the core infrastructure. Provides instructions on using the Software Updates window to view, install, or uninstall specific application packages according to your network requirements.

Catalyst Center provides many of its functions as individual applications. These applications are packaged separately from the Catalyst Center core infrastructure. Depending on your preferences, you can install and run the applications you want, and uninstall those you do not use.

From the main menu, choose **System** > **Software Updates**. The number and type of application packages shown in the **Software Updates** window vary depending on your Catalyst Center version and licensing level. All available application packages are shown, regardless of whether they are currently installed.

To view a package description and determine if it is required, move your cursor over the package name in the **Updates** tab in the **System** > **Software Updates** window.

Download and Install the Rogue Management and aWIPS application package

Provides instructions for downloading, installing, and enabling the Rogue Management and aWIPS application package in Catalyst Center. Details the necessary SUPER-ADMIN-ROLE permissions, DNA licensing requirements, and the steps to activate rogue and aWIPS detection on your wireless controllers.

Before you begin

You must have SUPER-ADMIN-ROLE permissions to perform this procedure.

By default, the Rogue Management and aWIPS application is not installed on Catalyst Center. You must manually install the Rogue and aWIPS application package separately.

You need a DNA Essentials license for Rogue Management, and a DNA Advantage license for aWIPS.

Perform the application management procedure from the **Software Management** window.

1. Install Catalyst Center. For more information, see the *Cisco Catalyst Center Installation Guide*.
2. Review the software requirements described in the release notes.

About this task

Procedure

1. From the main menu, choose **System** > **Software Management**.
2. Scroll to the **Available Applications for 2.3.x.x-xxxxx** area and select **Rogue And AWIPS**.
3. Click **Install**.

   For more information about downloading and installing updates for the Rogue Management and aWIPS application package, see the "Download and Install Application Updates" topic in the *Cisco Catalyst Center Administrator Guide*.
4. After installing the package, enable the Rogue Management application.
   a) From the main menu, choose **Assurance** > **Rogue and aWIPS**.
   b) On the **Overview** dashboard, choose **Rogue** from the **Actions** drop-down list. Click **Enable**.
   c) On the **Overview** dashboard, choose **aWIPS** from the **Actions** drop-down list. Click **Enable**.

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

4 Monitor the Rogue and aWIPS Dashboard

Topics:

- Access the Rogue Management and aWIPS application
- Monitor the Rogue Management and aWIPS dashboard
- Monitor network rogue threats
- Get rogue AP and rogue client details from the Threat 360° view
- Download aWIPS profile forensic capture from the Threat 360° view
- View details of all rogue APs on a floor in a floor map
- Deploy your device configurations now or later
- Preview and deploy your device configurations

Access the Rogue Management and aWIPS application

Provides instructions for accessing the Rogue and aWIPS dashboard within Catalyst Center. Explains how to navigate to the application from the Assurance menu and emphasizes that initial configuration is required before the system can be used for threat management.

Procedure

1. To access the Rogue Management and aWIPS application, log in to Catalyst Center.
2. From the main menu, choose **Assurance** > **Rogue and aWIPS**.

   The **Rogue and aWIPS** dashboard appears.

   Note:

   Before using the Cisco Catalyst Rogue and aWIPS application, you must configure it. For more information, see Basic setup workflow on page 17.

Monitor the Rogue Management and aWIPS dashboard

Guides you through monitoring the Rogue Management and aWIPS dashboard in Catalyst Center. Details how to enable or disable telemetry subscriptions, analyze threat metrics via various dashlets, and use graphical views to identify and respond to high-priority network threats effectively.

About this task

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 shows you the highest-priority threats so you can identify and respond to them quickly. The Rogue Management application uses streaming telemetry to retrieve data on rogue APs.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS**.

   The **Rogue and aWIPS** window opens. By default, Catalyst Center displays the **Overview** dashboard.

   Note:

   - Support for rogues is available starting from Cisco AireOS Controller version 8.8.111.0. When the Cisco AireOS Controller does not meet the minimum required software version, the dashboard displays a notification at the top. To upgrade to the supported version, click **Go To Devices** in the notification.

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

   The **Site Selector** slide-in pane appears.

   a) Enter a site name in the **Search Hierarchy** search bar or expand **Global** to select a site.

   Note:

   - If a site has more than 254 subsites, by default that site is disabled.
   - Site hierarchies without floors and outdoor are not listed in the site selector slide-in pane.

3. From the **Actions** drop-down list, choose **Rogue** > **Enable** to enable rogue subscription on the Cisco Wireless Controller and the Cisco Catalyst 9800 Series Wireless Controller.

   Note:

   This is a global setting. When enabled, the rogue telemetry subscription is applied to all devices currently present, regardless of site. Any new device added later will automatically receive this subscription during the site assignment process.

4. Click **Yes** in the **Warning** dialog box that appears.
5. In the **Rogue and aWIPS Subscription** slide-in pane, complete these steps to enable the rogue subscription:

   Note:

   The **Configuration Preview** tab appears only when the **Configuration Preview** is enabled. For information on how to enable configuration preview or ITSM approval, see the "Enable Visibility and Control of Configurations" topic in the *Cisco Catalyst Center Administrator Guide*.

   a) Schedule the task for deployment.

      Depending on Visibility and Control of Configurations settings, you can either:

      - Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later on page 33.
      - Preview and deploy the device configurations. For details, see Preview and deploy your device configurations on page 34.

   b) On the **Tasks** window, monitor the task deployment.

6. Choose **Rogue** > **Disable** to disable the rogue actions temporarily.
7. Click **Yes** in the **Warning** dialog box that appears.

   When the rogue management functionality is disabled, data from the wireless controller is not pushed to Catalyst Center until re-enabled.

8. In the **Rogue and aWIPS Subscription** slide-in pane, follow these steps to disable the rogue subscription:
   a) Schedule the task for deployment.

      Depending on Visibility and Control of Configurations settings, you can either:

      - Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later on page 33.
      - Preview and deploy the device configurations. For details, see Preview and deploy your device configurations on page 34.

   b) On the **Tasks** window, monitor the task deployment.

9. Choose **Rogue** > **Status** to view the rogue configuration job status.
10. Filter the rogue subscription status by **All**, **Failure**, **Success**, or **In Progress** by clicking the corresponding 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 subscription configuration changes are successfully pushed to the wireless controller.

11. Choose **aWIPS** > **Enable** to enable aWIPS data collection on Catalyst Center.
12. In the **Warning** dialog box that opens, click **Yes**.
13. In the **Rogue and aWIPS Subscription** slide-in pane, follow these steps to enable the aWIPS subscription:

Note:

The **Configuration Preview** tab appears only when the **Configuration Preview** is enabled. For information on how to enable configuration preview or ITSM approval, see the "Enable Visibility and Control of Configurations" topic in the *Cisco Catalyst Center Administrator Guide*.

a) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later on page 33.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations on page 34.

b) On the **Tasks** window, monitor the task deployment.

14. Choose **aWIPS** > **Disable** to disable the aWIPS actions temporarily.

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

15. In the **Rogue and aWIPS Subscription** slide-in pane, complete these steps to disable the aWIPS subscription:

a) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later on page 33.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations on page 34.

b) On the **Tasks** window, monitor the task deployment.

16. Choose **aWIPS** > **Status** to view the aWIPS subscription status.
17. Click the corresponding tabs to filter the aWIPS subscription status by **All**, **Failure**, **Success**, or **In Progress**.

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

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

18. Use the **Threats** dashlets to display this information:

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

  Note:

  Catalyst Center aggregates threats to reduce the total number of reported threats. As a result, the number of rogue threats shown on the Catalyst 9800 Series Wireless Controller may not exactly match the number shown in Catalyst Center. However, no threat information is lost during this aggregation process.

- **TOTAL AWIPS THREATS**: Displays the total number of aWIPS threats.
- **TOTAL UNIQUE ROGUE CLIENTS**: Displays the total number of unique rogue clients.
- **ROGUES CONTAINED**: Displays the total number of rogues contained.

The **Active High Threats** and **High Threats Over Time** graphs display threat details according to the selected timeline.

19. The **Active High Threats**, **Top Locations Affected**, and **High Threats Over Time** graphs display information about rogue APs detected in the last three hours by default. The graph information is based on the time interval that you select from the **Hours** drop-down list.
    - The options are **Last 3 hours**, **Last 24 hours**, and **Last 7 days**.

    Note: Select **Custom** to specify a time range. Choose a start date and end date. The duration cannot exceed 7 days. The time range must be within the past 14 days.

20. Use the **High Threats Summary** dashlet to display this information:

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

21. Use the **High Threats Over Time** dashlet to display this information:

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

22. Use the **Threats By Location** dashlet to view information about threats in the map view:

Location option	
Item	**Description**
 **Map View**	Click this toggle button to display a map view of the locations affected by threats. Hover your cursor over the corresponding location in the map to view all the threat levels and counts.

Location option	
Item	**Description**
 **List View**	Click this toggle button to display a list view of the locations affected by threats.

23. Use the **Threat Setting Summary** dashlet to view this information:

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

24. (Optional) Use the **Tips** dashlet for a direct link to workflows such as Create Allowed AP List, Create Allowed Vendor List, Create Rogue Rule, and so on.
25. (Optional) Click **View All** to view all the available workflows.

Monitor network rogue threats

Provides instructions for monitoring network rogue threats in Catalyst Center by selecting specific sites and time ranges. Details how to utilize the Threats table to filter, customize, and analyze comprehensive information regarding rogue APs and aWIPS attacks across your network infrastructure.

Procedure

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

   The **Site Selector** slide-in pane opens.

   a) Enter a site name in the **Search Hierarchy** search bar or expand **Global** to select a site.

   Note:

   - Sites with more than 254 subsites are disabled by default.
   - Site hierarchies without floors are not listed in the **Site Selector** slide-in pane.

2. Click the time range setting ( ) at the top-right corner to specify the time range of the data that you want to see in the **Threats** table:

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

If you select the **Custom** time range, specify the **Start Date** and time, and the **End Date** and time.

b) Click **Apply**.

3. Use the **Threats** table to view detailed information about the threats in your network:

Threats Table	
Item	**Description**
Filter	Click the icon in the search bar to see the data filter in the table based on this criteria: **Threat Level**, **Threat MAC Address**, **Type**, **Detecting AP**, **Detecting AP Site**, **RSSI (dBm)**, **SSID**, and **Containment Status**. **RSSI**, **SSID**, and **Clients** do not display for aWIPS.

Threats Table	
Item	**Description**

Threat Table	Displays this information about threats in a table format:
	· **Threat Level**: Displays color-coded classified threat levels. Catalyst Center classifies threats into these categories:
	  · **High Threat**
	  · **Potential Threat**
	  · **Informational**
	· **Mac Address**: Displays the MAC address of a rogue AP.
	· **Type**: Displays threat types.
	· **State**: Displays the state of a rogue AP or aWIPS attacks.
	· **Source/Target**: Shows whether the MAC address is the source of an aWIPS attack or the target of an aWIPS attack. This column is not applicable for rogue data.
	· **Connection**: Displays whether the rogue AP is located on the wired network or wireless network. This column shows the aWIPS attacks on the wireless network.
	· **Detecting AP**: Displays the name of the AP that is currently detecting a rogue AP. If multiple APs detect a rogue, the detecting AP displays the highest signal strength. This column is applicable for both rogue AP and aWIPS attacks.
	· **Detecting AP Site**: Displays the site location of the detecting AP. This column is applicable for both rogue AP and aWIPS attacks.
	· **RSSI (dBm)**: Displays the RSSI value reported by the detecting AP. RSSI (dBm) is only applicable for rogue APs.
	· **SSID**: Displays the service set identifier that a rogue AP is broadcasting. SSID is only applicable for rogue APs.
	· **Clients**: Displays the number of rogue clients associated with an AP. This column is only applicable for rogue APs.
	Note:
	The client count that displays in the **Threats** table differs from the client count that displays in the **Threats 360 degrees** window. This happens if the data that is processed in a Catalyst Center release earlier than 2.3.2 is migrated to Catalyst Center 2.3.2 or later. Catalyst Center 2.3.2 or later displays the correct client count for the newly processed data if the time range that is selected has the new data.
	· **Containment Status**: Displays the possible values (**Contained**, **Pending**, **Open**, and **Partial**) of a rogue AP. For autocontained rogue APs, the status displays as **Contained (Auto)**, **Pending (Auto)**, **Open (Auto)**, and **Partial (Auto)**. Wireless containment status is only applicable for rogue APs.
	· **Last Reported**: Displays the date, month, year, and time at which a rogue AP or aWIPS attack was last reported.
	· **Vendor**: Displays the rogue AP vendor information. This column is not applicable for aWIPS attacks.

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

Get rogue AP and rogue client details from the Threat 360° view

Details the Threat 360° view in Catalyst Center, which provides precise location mapping, threat analysis, and forensic data for rogue APs and clients. Guides you through using the floor map, interpreting map icons, and navigating tabs like Switch Port Detail and Forensic Captures to investigate network security threats.

About this task

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

You can get these details only after detecting the AP's strongest signal strength. You can get the exact location of your rogue AP or rogue client using the Cisco Connected Mobile Experiences (CMX) or Cisco Spaces integration.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Threats**.
2. To launch the **Threat 360°** view for a particular rogue AP or aWIPS threat, click the corresponding row in the **Threats** table.

   The **Threat 360°** pane opens.

   The upper part of the pane displays this information:

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

   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.

Note:

The Floor Map section does not display for the global location.

Catalyst Center makes a best effort to detect the rogue vendor name. If the vendor name isn't available, the name is shown as "UNKNOWN."

3. Complete any of these tasks as needed:

   - Click the icon at the right corner of the floor map to see the IP address of the wireless controller that manages the APs, along with the reachability status.
   - Click the icon at the right corner of the floor map to zoom in on a location. Zoom levels depend on the image resolution. High-resolution images provide more zoom levels. Each zoom level consists of a map style shown at a different scale with specific details. Some maps may use the same style at different scales.
   - Click the icon to see a map with fewer details.
   - Click the icon to view the details of the map icons.

   This table explains the floor map icons.

Table 3: Map icons and descriptions

Floor map icon	Description
Devices	
	Access Point
	Sensor
	Rogue AP
	Marker
	Planned AP
	Switch
	Interferer
	Client
	Rogue Client
	Reporting AP
	Detecting AP
Average Health Score	

Floor map icon	Description
	Health score: 8-10
	Health score: 4-7
	Health score:1-3
	Health score: Unknown
AP Status	
	Covered by sensor
	Not covered by sensor

4. You can do these tasks in the area under the **Threat 360°** pane:

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

     Note:

     - The **Admin Status** column shows the interface status as either **UP** or **DOWN**.
     - The **Port Mode** column shows the interface mode as either **ACCESS** or **TRUNK**.
     - Threats classified as Rogue on Wire based on Rogue Client MAC or Gateway MAC remain in the Rogue on Wire state for seven days after the Rogue Client migrates to a new Rogue AP or is no longer detected on the network.

     Note:

     Cisco switches are required for detecting rogue devices on the wired network.

   - Click the **Detections** tab to view information such as **Detecting AP**, **Detecting AP Site**, **Adhoc**, **Rogue SSID**, **RSSI (dBM)**, **Channels**, **Channel WidthRadio Type**, **SNR**, **State**, and **Last Updated**.

     Note:

     Although the wireless controller shows all detecting APs for a given BSSID, Catalyst Center shows only the strongest detecting AP for a given BSSID per wireless controller in the Threat 360° view.

   - 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 the file 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 **Forensic Captures** tab to view details such as **Detecting AP**, **Detecting AP Site** and **Last Updated**.

     Note:

     The **Forensic Captures** tab is shown only for aWIPS threats.

- Click the **Filter** ( ) icon at the left end of the table to limit the results based on your search criteria.

Download aWIPS profile forensic capture from the Threat 360° view

Provides instructions for downloading forensic capture files of DoS attacks from the Threat 360° view inCatalyst Center. Details the requirements for verifying network connectivity and enabling forensic capture on AP profiles to successfully retrieve and analyze pcap files for security investigations.

Before you begin

Verify the network connectivity between the APs and Catalyst Center.

About this task

This procedure explains how to download the forensic capture of various DoS attacks from the Threat 360° view.

Note:

Catalyst Center enables or disables forensic capture only on the default AP profile. You must enable or disable forensic capture in existing deployments where you have created custom AP join profiles.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Threats**.
2. In the **Threat MAC address** column, click the aWIPS attack link.

   The **Threat 360** window opens.
3. Click the **Forensic Capture** tab to view information such as **Detecting AP**, **Alarm ID**, **CaptureFilename**, and **Last Updated**.
4. In the **Capture Filename** column, click the **pcap** file to download the aWIPS profile forensic capture.
5. Click **Download All** to download all the **pcap** files.
6. Click the **Filter** icon to narrow down the search results based on **Detecting AP**.
7. Click the **Export** icon to save the **CSV** file to your workspace.

   Note:

   Catalyst Center shows a maximum of 50 forensic captures at a time.

View details of all rogue APs on a floor in a floor map

Guides you through viewing rogue AP details on floor maps within Catalyst Center. Explains how to select specific floors, interpret threat level legends, and access detailed information such as MAC addresses, threat types, and containment status for rogue devices detected in your network..

You can view the precise location of all rogue APs and their threat levels on a floor map.

Ensure integration of Catalyst Center with Cisco Connected Mobile Experiences (CMX) and Cisco Spaces, so that Catalyst Center can determine the rogue AP location.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Rogues on Map**.

Alternatively, click the menu icon and choose **Design** > **Network Hierarchy**. Select a floor and click the **View Rogue** link to open the **Rogues on Map** tab with the floor preselected.

2. From the left hierarchy tree, select a floor.

   If you select an area or building, a global map with rogue APs distribution is shown. You must select a floor to view the Rogue APs on the floor map.

   By default, **All Threat Levels** and **Display Rogue AP MAC Address** options are selected.

   The floor map shows the rogue APs detected on the selected floor in the past hour and the APs that detected them. Legends at the bottom of the map indicate the counts for **High Threats**, **Potential Threats**, and **Information Threats**.

3. Click the rogue skull icon to view details about the rogue AP:

   - Rogue AP MAC address
   - Threat level
   - Threat type
   - RSSI (dBm)
   - SSID
   - Vendor
   - Wireless containment status
   - Last reported

   When two or more rogue AP locations overlap or are very close, the map displays a stacked icon showing the total number of overlapping rogue APs. Click the rogue AP count in the map to see the MAC addresses of all overlapping rogue APs. Click a MAC address to view details about that rogue AP.

Deploy your device configurations now or later

When you reach the scheduling step of a workflow that supports Visibility and Control of Configurations, use this procedure to deploy your device configurations now or later.

Before you begin

Ensure that you have disabled Visibility and Control of Configurations in the settings.

About this task

At the scheduling step of a workflow that supports Visibility and Control of Configurations, complete this procedure to deploy your device configurations immediately or at a later time.

Procedure

1. Click **Now** or **Later**. Update the task name if needed.

   Note:

   If only visibility is enabled, or if both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected by default. The options **Now** and **Later** are dimmed.

2. On the **Performing Initial Checks** window, prepare and submit the task for deployment.
   a) Address all the issues to deploy the device configurations.

Ensure all validations are successful by clicking **Recheck**.

b) Click **Submit**.

The device configurations deploy at the scheduled time. View the task in the **Tasks** window.

Preview and deploy your device configurations

When you reach the scheduling step of a workflow that supports Visibility and Control of Configurations, use this procedure to preview and deploy your device configurations.

Before you begin

Ensure that Visibility and Control of Configurations is enabled in the settings.

About this task

When you reach the scheduling step in a workflow that supports Visibility and Control of Configurations, complete this procedure to preview and deploy your device configurations.

Procedure

1. Click **Preview and Deploy (Recommended)** and, if necessary, update the task name.

   Note:

   By default, if only visibility is enabled or both visibility and control are enabled, **Preview and Deploy (Recommended)** is selected. The **Now** and **Later** options are dimmed.

2. On the **Performing Initial Checks** window, address all the issues to continue with your current deployment.

   Ensure all validations are successful by clicking **Recheck** in the lower right corner of the window.

3. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations.

   Tip:

   This preparation can take some time. You can click **Exit and Preview Later** and view the work item in the **Tasks** window.

4. In the **Preview Configuration** window, review the device configurations. The window displays a deployment option.

Click...	To...
Deploy or **Submit for Approval**	deploy the device configurations.
Exit and Preview Later	review and deploy the device configurations later. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

   Note:

   You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

5. Schedule the deployment.

a) Indicate when and, if applicable, where you want to deploy the configuration.

   If you are submitting the configurations for review, add notes for the IT administrator.

b) Click **Submit**.

   You can check the work item approval status or the task deployment status on the **Tasks** window. If it is not approved, resubmit the work item for ITSM approval. When it is approved, the item is deployed at the scheduled time.

   Note:

   After submitting the task, view the progress of the provisioning task with the **Task Progress** bar in the **Activities** > **Tasks** window by clicking the task name.

5 aWIPS Profiles

Topics:

- About aWIPS profiles
- Create an aWIPS profile configuration workflow
- View an aWIPS profile
- Assign an aWIPS profile to the network device
- Edit an aWIPS profile
- Delete an aWIPS profile
- Enable or disable aWIPS or aWIPS forensic capture

About aWIPS profiles

Details the configuration of aWIPS profiles, including selecting signatures, setting DoS detection thresholds, and enabling forensic capture. Also outlines supported device models, software versions, and specific requirements for enabling the wireless module on switches for SD-Access use cases.

Configure aWIPS profiles to select required signatures, set thresholds for detecting denial of service (DoS) attacks, and enable forensic capture at the signature level. Adjust thresholds to control the number of alarms generated for each aWIPS signature during a specific time period.

This table lists the supported devices for aWIPS profile configuration for various versions of Catalyst Center:

Table 4: Supported devices for aWIPS profile configuration

Supported devices	IOS-XE version	Catalyst Center version
• 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	17.4 to 17.13 17.4 to 17.14 17.4 to 17.15 17.4 to 17.15	2.3.7.4 2.3.7.5 2.3.7.6 2.3.7.7

Note:

For SD-Access use cases, for aWIPS profiles to work, you must enable the wireless module on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500 Series Switches.

Prerequisites for aWIPS profile

- Verify the network connectivity between the Cisco Wireless Controller and Catalyst Center.
- Make sure that the network device is reachable from Catalyst Center and has downloaded the aWIPS profile configuration from Catalyst Center.

  Note:

  To avoid aWIPS profile download failures in a Fabric in a Box SD-Access setup, ensure that the Infrastructure Virtual Network (Infra_VN) uses a routable IP subnet in the global routing table.

- To enable forensic capture, complete these tasks:
  - Ensure there is network connectivity between APs and Catalyst Center.
  - Establish the Google Remote Procedure Call (gRPC) tunnel interface between APs and Catalyst Center. Use the **show ap icap connection** command to confirm that the status is READY.
  - Open the required ports between Catalyst Center and links to the network devices.

- Configure an NTP server on the AP to prevent time lag between Catalyst Center and APs. For information, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.12.x.

Create an aWIPS profile configuration workflow

Guides you through the workflow for creating and assigning aWIPS profile configurations in Catalyst Center. Details the process of selecting DoS attack signatures, configuring detection thresholds, enabling forensic capture, and assigning profiles to specific wireless controllers to ensure proactive network security.

About this task

This section explains how to create an aWIPS profile.

Procedure

1. From the main menu, choose **Workflows** > **Create an aWIPS Profile**.

   Alternatively, you can create an aWIPS profile by choosing **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** > **Add Profile**.

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

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

   The **aWIPS Profile Creation** window opens.

3. In the **Profile Name** field, enter a name for the aWIPS profile.
4. The **Signatures** table lists these parameters for the aWIPS profile:
   - **Signature**: Shows the standard aWIPS signatures that detect 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.
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.

   Note:

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

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

   For some signatures, the configuration threshold is not applicable. For those signatures, the threshold configuration values appear as **NA** on top of the respective **Configure Threshold** field.

   Note:

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

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

Note:

- Catalyst Center does not allow you to edit the **Default Threshold** value and the **Time Interval (In Seconds)** value for the aWIPS profile.
- If you enable forensic capture for an aWIPS signature, Catalyst Center allows you to download packets from the **Threat 360** window.
- If you disable forensic capture for an aWIPS signature, Catalyst 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 Catalyst Center.

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

   Note:

   The default aWIPS profile is configured for a high-security environment and is not suitable for general-purpose deployment. Configure the aWIPS profile based on your requirements.

9. Click **Next**.

   Note:

   In the **Configure Threshold** column, for the selected aWIPS signature, if you enter a threshold value that is out of the specified range, an error message appears at the top of the **Create an aWIPS Profile** window, asking you to enter a value within the specified range.

10. In the **Profile Summary** window, the **Profile Summary** table displays the summary of the profile that was configured in the **aWIPS Profile Creation** window.
11. Click **Next**.
12. In the **Profile Creation Done** window, click **Assign Profile to Device(s)** to assign this aWIPS profile to a device.

    The **Assign aWIPS Profile** window opens.

    You can also assign an aWIPS profile to a device in the **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** window 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 a device at a time.

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 these 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 pushing the profile configuration URL to the network device. The possible values are **Success**, **Failure**, or **In Progress**.

      If the status is **Failure**, hover your cursor over the **i** icon next to **Failure** to see the 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**.

      If the status is **Failure**, hover your cursor over the **i** icon next to **Failure** to see the reason.

Note:

- If the aWIPS subscription is disabled on Catalyst Center, an error message appears at 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 on page 22.
- HTTP protocol reachability must be possible between the device and Catalyst Center for the device to download the profile configuration from the profile configuration URL.

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

  If the status is **Failure**, hover your cursor over the **i** icon next to a **Failure** to see the reason.

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

  Hover your cursor over the **i** icon next to the corresponding forensic capture. This tooltip appearss: **Shows the current Forensic Capture status on default-ap-profile AP Join Profile on the device**.

  Note:

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

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

14. Click **Next**.

    The **Profile Creation Done** window opens.

View an aWIPS profile

Provides instructions for accessing the aWIPS Profile dashboard in Catalyst Center to view existing profiles, their assigned wireless controllers, and last update timestamps. Also outlines the steps required to subscribe to upgraded services if prompted upon initial navigation.

Before you begin

Procedure

From the main menu, 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, a message appears on top of the **aWIPS Profile** dashboard. The message asks you to subscribe to the upgraded subscription, even if **aWIPS** is enabled in Catalyst Center. To subscribe to the upgraded subscription, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS dashboard on page 22.

The aWIPS Profile dashboard displays this information:

- **Profile Name**: Shows the list of aWIPS profile 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

Outlines the procedure for assigning aWIPS profiles to network devices within Catalyst Center. Details the process of selecting profiles, filtering reachable and supported devices, and verifying assignment summaries to ensure proper threat detection configuration.

Before you begin

If you upgrade Catalyst Center from a release earlier than Release 2.2.2.0, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe to the additional subscription. See Monitor the Rogue Management and aWIPS dashboard on page 22.

Note:

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

Procedure

1. From the main menu, choose **Workflows** > **Assign an aWIPS Profile**.

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

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

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

   The **Assign aWIPS Profile** window appears.

3. From the **Profile Name** drop-down list, select the aWIPS profile name that you want to assign to a device.
4. In the left pane, you can search for a site by entering its name in the **Find Hierarchy** field. Alternatively, you can expand **Global** to select a site.

   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 these 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.

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 the devices or an individual device.

   Note:

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

6. Click **Next**.
7. 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.
8. Click **Next**.

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

Note:

Profile assignment to the devices takes some time to complete. You must wait before retrying the assignment process.

9. 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 an aWIPS profile on page 41.

Edit an aWIPS profile

Explains how to edit existing aWIPS profiles in Catalyst Center, including updating signature thresholds and saving changes. Details that updated configurations are automatically pushed to all assigned network devices and notes that the default aWIPS profile cannot be modified.

Before you begin

To add an additional subscription, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard. See Monitor the Rogue Management and aWIPS dashboard on page 22.

About this task

This procedure describes how to edit an aWIPS profile.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile**.
2. In the **aWIPS Profile(s)** table, click the profile name that you want to edit.
3. In the **Edit aWIPS Profile** window that opens, make the necessary changes and click **Save**.

Note:

The default aWIPS profile cannot be edited.

After the profile saves, it pushes to all devices assigned to the aWIPS profile.

Note:

In the **Configure Threshold** column for the selected aWIPS signature, if a threshold value outside the specified range is entered, an error message appears on the top of the **Edit aWIPs Profile** window requesting the correct value within the specified range.

Delete an aWIPS profile

Provides instructions for deleting an aWIPS profile from Catalyst Center. Explains that default profiles cannot be deleted and that any assigned network devices must be reassigned to the default profile before the deletion process can successfully proceed.

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 on page 22.

About this task

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

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **aWIPS Profile**.

   The **aWIPS Profile** dashboard appears.

2. In the **aWIPS Profile(s)** table, check the check box next to the aWIPS profile name that you want to delete. Click **Delete**.

   Note:

   - You cannot delete a default aWIPS profile.
   - You cannot delete an aWIPS profile that is assigned to a network device. If a device is assigned to an aWIPS profile, reassign the device to the default aWIPS profile before deleting the profile.

3. In the confirmation window, click **Delete**.

Enable or disable aWIPS or aWIPS forensic capture

Provides instructions for enabling or disabling aWIPS and forensic capture at the site level within Catalyst Center. Explains how to configure these settings via AP profiles and emphasizes the necessity of provisioning or reprovisioning devices to apply changes across the network hierarchy.

About this task

Catalyst Center allows you to enable or disable aWIPS or aWIPS forensic capture at the site level. Enable or disable aWIPS for all Cisco Catalyst 9800 Series Wireless Controllers in a network.

Procedure

1. From the main menu, choose **Design** > **Network Settings**.
2. Click the **Wireless** tab.
3. In the left pane, ensure that **Global** is selected.

   Note: The sites, buildings, and floors inherit the settings from the global level. Settings saved at the site, building, or floor level override the global network settings.

4. Click **AP Profiles**.
5. In the **AP Profile** table, hover your cursor over **Add**, and select **AP Profile for IOS-XE**.
6. Click the **Security** tab.
7. To enable aWIPS, click the **aWIPS** toggle button.

   By default, **aWIPS** is enabled at the global level.

8. (Optional) To disable aWIPS, click the **aWIPS** toggle button.
9. To enable forensic capture, click the **Forensic Capture** toggle button.

   Note: To enable forensic capture, aWIPS must be enabled. If you disable aWIPS when forensic capture is enabled, forensic capture also disables.

10. Click **Save**.

    Note: After you configure **aWIPS** or aWIPS Forensic Capture settings, provision or reprovision a device to apply the changes.

11. (Optional) To reset the **aWIPS and Forensic Capture Enablement** settings, click **Reset**.

Note:

If you are migrating from a Catalyst Center release earlier than Release 2.3.2.0, configure the network settings with **aWIPS** or **aWIPS Forensic Capture** settings. This ensures that configurations are updated in the wireless controllers.

AP join profiles on devices use the **aWIPS** or **aWIPS Forensic Capture** settings. When a Cisco Catalyst 9800 Series Wireless Controller device is provisioned, all AP join profiles associated with the device are fetched, and these actions take place:

- Default AP join profiles inherit the **aWIPS** or **aWIPS Forensic Capture** settings from the site assigned to the device.
- Custom profiles, which are created using Catalyst Center as part of row AP provisioning, inherit the **aWIPS** or **aWIPS Forensic** settings from the **Country** site level for which the corresponding row AP profile is created.
- Custom profiles created using Catalyst Center as part of mesh AP provisioning inherit the settings from the floor site level for the corresponding row AP profile.
- Custom AP join profiles created outside Catalyst Center do not inherit the settings.

6 Rogue AP Containment on Wired and Wireless Networks

Topics:

- Rogue AP Containment overview
- Wired rogue AP containment
- Wireless Rogue AP Containment
- Cisco Rogue AP Containment Actions Compatibility Matrix
- View tasks and audit logs of rogue AP containment type

Rogue AP Containment overview

Introduces the Rogue AP Containment feature in Catalyst Center, which mitigates security threats by disabling wired switchports or initiating wireless deauthentication. This overview covers wired and wireless containment methods, auto-containment capabilities, and supported Cisco controller models for effective rogue device management.

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

Rogue AP containment is further classified as:

- **Wired Rogue AP Containment**: The rogue AP MAC addresses classified as **Rogue on Wire** on the Catalyst Center rogue threat dashboard.
- **Wireless Rogue AP Containment**: The rogue AP MAC addresses classified as **Honeypot**, **Interferer**, or **Neighbor** on the Catalyst Center rogue threat dashboard.
- **Auto-Containment**: You can enable automatic containment of the rogue rule. For more information, see Edit a rogue rule on page 58.

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

Details the Wired Rogue AP Containment feature, which allows administrators to shut down ACCESS mode switchports where rogue APs are physically connected. Explains the procedure for initiating containment via the Threat 360 window, reviewing configuration previews, and monitoring the status of the switchport shutdown process.

Before you begin

Download and install the rogue and aWIPS application package. For more information, see Download and Install the Rogue Management and aWIPS application package on page 20.

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

About this task

The Wired Rogue AP Containment feature allows Catalyst Center to shut down the ACCESS mode interface on the switch to which a rogue AP is physically attached. Catalyst 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 Catalyst Center.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Threats**.
2. Click the rogue AP MAC address is classified as **Rogue on Wire** in the **Threat MAC address** column.

The **Threat 360** window appears.

3. From the **Action** drop-down list, select **Shutdown Switchport**.

   A warning dialog box displays the list of ACCESS mode interfaces to be shut down on the corresponding device, and **Configuration Preview** information.

   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 52.

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

4. In the **Configuration Preview** tab, review the configurations and click **Yes**.

   Note:

   The **Configuration Preview** tab appears only when **Configuration Preview** is enabled. For information on how to enable this preview, see the "Enable Visibility and Control of Configurations" topic in the *Cisco Catalyst Center Administrator Guide*.

5. The **Threat 360** window displays 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 be updated 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 no ACCESS mode interfaces are up to initiate the containment, Catalyst 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 to is as long as in the **Rogue on Wire** classification type. For more information, see Wireless Rogue AP Containment on page 49.

Wireless Rogue AP Containment

Explains the Wireless Rogue AP Containment feature in Catalyst Center, which disrupts communication between rogue APs and clients. Details the procedures for starting and stopping containment, monitoring status levels, and understanding operational limitations such as resource constraints, PMF, and DFS channel impacts.

Before you begin

Download and install the rogue and aWIPS application package. For more information, see Download and Install the Rogue Management and aWIPS application package on page 20.

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

About this task

The Wireless Rogue AP Containment feature allows Catalyst 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. Catalyst 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**.**

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Threats**.
2. To use Wireless Rogue AP Containment, click a rogue AP MAC address listed under the **Threat MAC address** column, marked as **Honeypot**, **Interferer**, or **Neighbor** classification types.

   Note:

   Cisco Catalyst 9800 Series Wireless Controller has a limit of only 625 configurations for rogue containment at a time. When the limit is reached, containment won't work for any new rogues on those devices.

   The **Threat 360** window opens.

   Note:

   A rogue AP MAC address comprises multiple rogue BSSIDs.

3. From the **Action** drop-down list, select **Start Containment** and **Configuration Preview**.

   A warning dialog box opens with information about the legal consequences and a list of rogue BSSIDs to be contained on the wireless controller and **Configuration Preview**.

   Note:

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

4. By default, the **Rogue BSSID** list appears.

   In the **Configuration Preview** tab, review the configurations and click **Yes**.

   Note:

   The **Configuration Preview** tab appears only when the **Configuration Preview** is enabled. For information on how to enable **Configuration Preview**, see the "Enable Visibility and Control of Configurations" topic in the *Cisco Catalyst Center Administrator Guide*.

5. The **Threat 360** window displays the Wireless Rogue AP Containment status accordingly:
   - 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:

After containment is initiated, it takes some time for the **Containment Status** column to get an update with another wireless containment status.

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

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

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

   Table 5: Wireless containment status possible values

Wireless containment status	Meaning
Contained	Rogue AP actively contained by the wireless controller.
Pending	Wireless controller has kept this rogue in containment Pending state.
Open	Rogue AP is not contained.
Partial	Some of the rogue BSSIDs are in Open state and the rest of them are either in the **Contained** or the **Containment Pending** state.

Note:

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

The wireless controller can keep the Wireless Rogue AP Containment in **Pending** state because of these reasons:

- **Resource outage**: After the rogue BSSID containment request is submitted, the wireless controller puts the rogue BSSID containment either in **Containment** or **Containment Pending** state because of the three rogue BSSIDs per radio limitation for client-serving radios, and six rogue BSSIDs per radio limitation for monitor mode. When the radio exceeds the specified limitation, the next submitted rogue BSSID for containment goes to the **Pending** state by the wireless controller until one of the rogue BSSIDs goes out of **Contained** state.
- **Protected Management Frames (PMF)**: The wireless controller does not initiate containment when the Protected Management Frames (PMF) are enabled on rogue BSSIDs and the containment status is in **Pending** state. When the PMF is disabled, the wireless controller initiates the containment.
- **Dynamic Frequency Selection (DFS)**: The wireless controller keeps the containment status in the Pending state and does not attempt to contain the rogue BSSID if it broadcasts on the Dynamic Frequency Selection (DFS) channels. After the rogue BSSID moves out of the DFS channel, the wireless controller initiates the containment.

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

   The **Threat 360** window opens.

8. From the **Action** drop-down list, select **Stop Containment**.

Note:

The **Stop Containment** option appears in the **Action** drop-down list only when the wireless rogue AP is in **Contained**, **Pending** or **Partial** state. For more information, see the Cisco Rogue AP Containment Actions Compatibility Matrix on page 52.

- A blue check mark appears as a banner on the **Threat 360** window, indicating the progress of the **Stop Containment** process on the wireless rogue AP.
- A green check mark appears as a banner on the **Threat 360** window, indicating the progress of the **Stop Containment** process on the wireless rogue AP.

Cisco Rogue AP Containment Actions Compatibility Matrix

Details the Cisco Rogue AP Containment Actions Compatibility Matrix, which outlines the availability of specific containment actions—such as Start, Stop, and Shutdown Switchport—based on the rogue AP's threat type and its current containment status within the network.

The table provides the behavior of rogue AP containment actions for the current state of rogue APs in the **Threat 360** window.

Table 6: Rogue AP Containment Actions Compatibility Matrix

Rogue AP threat **Type**	Rogue AP current **Containment Status**	**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	Not Visible
		Shutdown Switchport is shown	**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 type

Provides instructions for viewing tasks and audit logs related to wired and wireless rogue AP containment in Catalyst Center. Details how to filter activities by the ROGUE category and explains the differences in log formats between Cisco AireOS CLI commands and Cisco Catalyst 9800 Series Wireless Controller NETCONF requests.

About this task

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

Procedure

1. From the main menu, choose **Activities** > **Tasks**.
2. In the left pane, under **Type**, click **Task** to view only tasks.
3. In the left pane, do these steps to view only wired and wireless rogue AP containment tasks:
   a. Expand **Categories**.
   b. Click **Show all**.
   c. In the **Search** field, enter **ROGUE**.
   d. Check the **ROGUE** check box.
4. Click the task name to open a slide-in pane with more information, such as the rogue AP containment operation details, status, date, and time.
5. To view the audit logs with the rogue AP containment type and corresponding device IP address information, click the menu icon and choose **Activities** > **Audit Logs**.

   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.

7 Custom Classification of Rogue APs

Topics:

- About the allowed list workflow
- Set up the allowed list workflow
- About custom rogue rule creation
- Edit a rogue rule
- Delete a rogue rule
- Create a custom rogue rule
- About rogue rule profiles
- Edit a rogue rule profile
- Delete a rogue rule profile
- Create a rogue rule profile
- View the allowed access points list
- About the allowed vendor list
- View vendor rule list information
- Edit a vendor rule
- Delete a vendor rule
- Create a list of allowed vendors

About the allowed list workflow

Introduces the allowed list workflow in Catalyst Center, enabling administrators to move specific rogue AP MAC addresses to an allowed list in bulk. Outlines supported rogue types, such as Rogue on Wire and Honeypot, while identifying threat categories that are excluded from this functionality.

The Catalyst Center Rogue Management and aWIPS workflow allows you to review and mark the MAC addresses of rogue access points to move them to the allowed list in bulk. You can then process the allowed list of selected AP MAC addresses.

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

See Set up the allowed list workflow on page 56 for instructions about moving these rogue AP types to the allowed list:

- Rogue on Wire
- Honeypot
- Interferer
- Neighbor

The Rogue Management and aWIPS workflow does not support moving these AP types to the allowed list:

- Beacon Wrong Channel
- Beacon DS Attack
- AP Impersonation
- Friendly

Set up the allowed list workflow

Details the workflow for managing allowed rogue APs in Catalyst Center, including bulk CSV uploads and individual MAC address management. Explains the necessary administrative permissions, file validation requirements, and how to update threat categories to ensure accurate network security monitoring.

Before you begin

To perform this procedure, you must have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions.

About this task

This procedure shows how to move rogue AP MAC addresses to the allowed list in bulk. You do not want to report these addresses as high threat in Catalyst Center.

Procedure

1. From the main menu, choose **Workflows** > **Set up Rogue Management and aWIPS**.

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

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

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

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

3. Using the **Search** field, search for the MAC addresses that were already added in the About the allowed list workflow on page 56.

4. Click **Export** to export the allowed list.
5. Click the **Download the sample CSV template from here** link to download the sample file. Manually add the MAC address, operation, and category to the bulk allowed list template.

   Hover your cursor over the notification symbol to view the format of allowed MAC addresses, operations, and categories.
6. 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 should be 1.2 MB.

   Note:

   Catalyst Center performs a validation check. An error message appears if the uploaded CSV file does not meet these 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.
7. Click **Next**.
8. 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.
9. Click **Continue to allowed list**, and, in the dialog box that opens, click **Yes**.

   The **Done! Allowed List Updated** window opens.
10. Click **Go to Rogue and aWIPS Home Page**.

    The **Rogue and aWIPS** dashboard opens.

    Click the **Threats** tab to display the **Threat** table. Catalyst Center now categorizes the specified rogue AP MAC addresses as **Allowed List** under the **Type** column.
11. 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 opens.
12. From the **Action** drop-down list, select **Add to Allowed list**.

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

About custom rogue rule creation

It looks like you've captured the essence of custom rogue rules in Catalyst Center. This summary effectively highlights how these rules help administrators minimize noise and tailor threat management to their specific organizational needs.

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 these rogue AP types to the custom classification type:

- Interferer
- Neighbor

Edit a rogue rule

Provides instructions for editing existing rogue rules in Catalyst Center, including modifying rule conditions and managing auto-containment settings. Explains that configuration changes apply only to new data and highlights specific constraints for enabling automatic containment for Honeypot and high-level threats.

About this task

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Rules**.
2. In the **Rogue Rules** table, click the rule name that you want to edit.
3. In the **Edit Rogue Rule** window, make changes as needed.

   Note:

   The previous classification remains unchanged, even if old rules are used to modify the rule conditions. The change affects only the new data classification.

4. (Optional) Check the **Enable Auto-Containment** check box to check box to enable automatic containment of the rogue rule.

   Note:

   - Cisco Catalyst 9800 Series Wireless Controllers have a limit of 625 configurations for rogue containment at a time. When the limit is reached, containment won't work for any new rogue on those devices.
   - You can only enable automatic containment for **Honeypot** and the custom rule with the **High** level threat.
   - If you want to disable automatic containment after it has been enabled, you must do so manually. Disabling automatically is not supported.

5. Click **Save**.

   Verify whether the rogue containment is enabled or not in the **Auto-Containment** column.

Delete a rogue rule

Provides instructions for deleting rogue rules in Catalyst Center, noting that predefined rules like Honeypot cannot be removed. Explains that deleting the last rule in a profile removes the entire profile and allows you to view previously deleted items under the Inactive tab.

About this task

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Rules**.
2. In the **Rogue Rules** table, click the **Rule Name** that you want to delete and click **Delete**.

Note:

If you delete the only rogue rule in a rule profile, the rule profile is also deleted.

3. In the confirmation dialog box, click **Delete**.

Note:

Honeypot is a predefined rule; you cannot delete it.

4. (Optional) To view the deleted rules, click the **Inactive** tab in the **Rogue Rules** table.

Create a custom rogue rule

Provides instructions for creating custom rogue rules in Catalyst Centerby defining specific threat conditions and associating them with rule profiles. Details how to configure threat levels, enable auto-containment for high-level threats, and manage rule priorities to effectively classify and mitigate network security risks.

About this task

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

Procedure

1. From the main menu, choose **Workflows** > **Create a Rogue Rule**.
2. In the **Create a Rogue Rule** window, click **Get Started**.
3. In the **Rule Name** field, enter a unique name for the rule.

   While creating new rogue rules, you cannot enter the rogue rule names that were deleted earlier.

4. In the **Description** field, enter a description for the rule.
5. Click **Next**.
6. In the **Create Rogue Rule** window, select one of these threat level options: **High**, **Potential**, and **Informational**.
7. (Optional) Check the **Enable Auto-Containment** check box to automatically contain the rogue rule.

Note:

- Cisco Catalyst 9800 Series Wireless Controllers have a limit of only 625 configurations for rogue containment at a time. After the limit is reached, containment won't work for any new rogue on those devices.
- Automatic containment is only applicable to the rogue rules classified with the **High** threat level. By default, **Enable Auto-containment** is disabled for the **Potential** and **Informational** threat levels.

8. From the **Match** drop-down list, choose either **All** to match all the conditions, or **Any** to match your choice of conditions.
9. From the **Add Condition** drop-down list, choose the rule conditions.

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

10. Click **Next**.
11. (Optional) To assign this rule to an existing rule profile, click **Yes** in the **Do you want to assign this rule to a rule profile?** dialog box.

Note:

Rogue rules must be assigned to a rule profile. A rogue rule cannot function on its own.

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

    You can select one or more rule profiles.

    Note:

    You cannot assign more than five rules to a rule profile.

13. In the confirmation dialog box, click **Proceed**.

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

    Note:

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

14. Review the rogue rule configuration in the **Summary** window.

    Note:

    The existing classification based on earlier rules does not change, even if the new rule conditions apply. The updated rules affect only new data classification.

15. (Optional) To create another rogue rule, click the **Create Another Rogue Rule** button and repeat the preceding steps in this procedure.
16. (Optional) To view the created rogue rules, click **View all Rogue Rules and Profiles**.

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

    You can also view the created rogue rules by clicking the menu icon and choosing **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rules**.

About rogue rule profiles

Introduces rogue rule profiles in Catalyst Center, which allow you to group and prioritize specific rogue rules for site-based threat management. Explains how rule profiles are inherited through the network hierarchy and how direct floor-level assignments take precedence over inherited parent-site configurations.

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 reported from the site are verified against the rules in the rule profile.

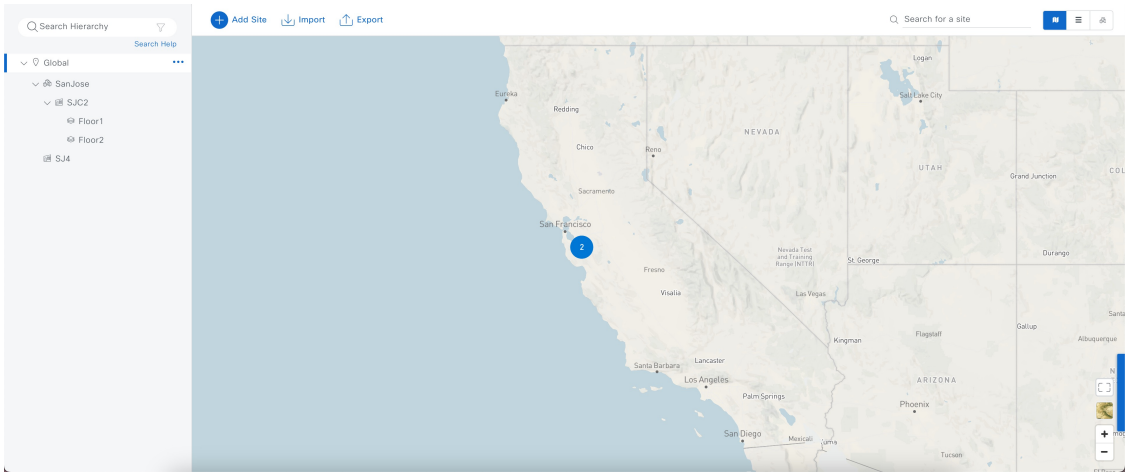
Note:

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

Due to site inheritance, all floors under a particular site inherit the rogue rule profile mapped at the area, site, or building level. For example, as shown in the figure, **Floor1** and **Floor2** will inherit the rogue rule profile that is mapped at the **SanJose** level.

A rogue rule profile mapped to a floor has precedence over a rogue rule inherited from a parent site. For example, as shown in the the figure, Rogue Rule Profile A is directly mapped to **Floor1**. Rogue Rule Profile A takes precedence over Rule Profile B that is assigned to the parent site, **SJC2**.

Figure 1: Network hierarchy



Edit a rogue rule profile

Guides you through editing rogue rule profiles in Catalyst Center, including managing rule associations and auto-containment settings. Explains that configuration updates apply only to new data and notes that the predefined Honeypot rule is automatically included in all new profiles for consistent threat management.

About this task

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Rules**.
2. Click the **Rogue Rule Profiles** tab.
3. In the **Rogue Rule Profiles** table, click the profile name that you want to edit.
4. In the **Edit Rule Profile** window, make the necessary changes.

   Note:

   Edited rule profiles do not modify any previously classified data. The edits only apply to the new modified data that is processed after changes are made.

5. (Optional) Check the **Enable Auto-Containment** check box to autocontain the rogue rule.

   Note:

   - Cisco Catalyst 9800 Series Wireless Controllers have a limit of 625 Rogue Containment configurations at a time. Once the limit is reached, containment won't work for any new rogue on those devices.
   - **Honeypot** is a predefined rule that is added to all the newly created rogue rule profiles by default.
   - If you want to disable autocontainment after enabling autocontainment, you must disable autocontainment manually because it cannot be disabled automatically.

6. In the confirmation window, click **Yes**.
7. (Optional) You can toggle between **User Defined** and **Predefined** to view the corresponding rules.
8. Verify whether the rogue containment is enabled or not in the **Auto-containment** column.
9. Click **Save**.

Delete a rogue rule profile

Provides instructions for deleting rogue rule profiles in Catalyst Center. Explains how to navigate to the Rogue Rule Profiles tab to select and remove specific profiles from the system.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS** > **Rules**.
2. Click the **Rogue Rule Profiles** tab.
3. In the **Rogue Rules** table, click the profile name to delete then click **Delete**.
4. In the confirmation dialog box, click **Delete**.

Create a rogue rule profile

Details the process of creating a rogue rule profile in Catalyst Center, including adding specific rules, setting their priority, and associating the profile with a site. Explains how to configure auto-containment settings and verify the final configuration to ensure effective threat management across your network.

About this task

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

Procedure

1. From the main menu, choose **Workflows** > **Create a Rogue Rule Profile**.
2. In the **Create Rogue Rule Profile** window, click **Get Started**.
3. In the **Profile Name** field, enter a unique name for the rule profile.
4. (Optional) Check the **Enable Auto-Containment** check box to automatically contain the rogue rule.

   Note:

   - Cisco Catalyst 9800 Series Wireless Controllers have a limit of 625 configurations for rogue containment at a time. When the limit is reached, containment won't work for any new rogues on those devices.
   - You can only automatically contain **Honeypot** and the custom rules classified with the **High** threat level.

5. In the confirmation window, click **Yes**.
6. Click **Next**.
7. 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.

8. In the **Sort rules in order of priority** window, drag and drop the rules to set their priority. The highest priority rule is listed first.
9. Click **Next** to associate a rogue rule profile to a location.
10. Check the check box next to a site to associate the rule profile to that site, and click **Next**.

    Rule profiles can exist without being assigned to any site. Rules are only checked when you assign the rule profile to a site.

    Note:

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

11. In the **Summary** window, review the rogue rule profile configuration.

12. Click **Back** to make changes, if any, to the values entered in the previous window.
13. Click **Create Rule Profile**.

    A message appears to confirm the rule profile creation was successful.

14. (Optional) To view all the rogue rules and profiles, click **View all Rogue Rules and Profiles**.

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

    You can also view the created rule profiles by clicking the menu icon and choosing **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rule Profiles**.

View the allowed access points list

Guides you through accessing and managing the Allowed Access Points list in Catalyst Center. Explains how to view MAC addresses, search or filter specific entries, export the list to CSV, and add or remove access points to maintain accurate threat detection.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS**.

   The **Rogue and aWIPS** dashboard appears.

2. In the **Allowed List** tab, click the **Allowed Access Points List**.

   The **Allowed Access Points List** table displays the **MAC Address** and **Last Changed** details of all the allowed access points.

3. Click the search icon or filter icon to find a specific access point in the allowed list.
4. (Optional) Click **Add Access Point List** to add a rogue AP MAC address to the allowed list. For more information, see Set up the allowed list workflow on page 56.
5. (Optional) Click **Export** to save the allowed access points list as a CSV file.
6. (Optional) Select an access point and click **Delete** to remove the access point from the allowed list.

About the allowed vendor list

Introduces the Allowed Vendor List feature, which enables you to reclassify threats from specific vendors as Potential or Informational rather than High. Explains that you can add up to five vendors per workflow and that site-specific vendor rules take precedence over inherited configurations.

The **Allowed Vendor List** feature lets you determine if APs from specific vendors 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 to mark them as **Potential** or **Informational** threats. In a given workflow, you can add up to five vendors to the allowed list.

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

View vendor rule list information

Provides instructions for viewing the list of created vendor rules in Catalyst Center. Details how to navigate to the Allowed Vendor List table to review vendor names, match criteria, assigned threat levels, associated site information, and the last update timestamp.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS**.
2. Click the **Allowed List** tab.
   The **Allowed Vendor List** table lists the allowed vendors with details. Each vendor rule appears as an entity:
   - **Vendor Name**
   - **Match Criteria**
   - **Threat Level**
   - **Associated Site(s)**
   - **Last Changed**

Edit a vendor rule

Details the procedure for editing existing vendor rules in Catalyst Center, including modifying vendor names, match criteria, threat levels, and associated sites. Explains how to save these changes to ensure your allowed vendor configurations remain current and aligned with your network security requirements.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS**.
2. Click the **Allowed List** tab.
3. In the **Allowed Vendor List** table, select the vendor name that you want to edit.
4. In the **Edit Allowed Vendor List** window, edit these parameters as needed:
   - **Threat Level**
   - **Match Criteria**
   - **Vendor Name**
   - **Associated Sites**
5. Click **Save**.

Delete a vendor rule

Provides instructions for deleting vendor rules in Catalyst Center. Explains how to navigate to the Allowed Vendor List tab to select and remove specific vendor rules from your network security configuration.

Procedure

1. From the main menu, choose **Assurance** > **Rogue and aWIPS**.
2. Click the **Allowed List** tab.

3. In the **Allowed Vendor List** table, check the check box of the vendor name that you want to delete, and click **Delete**.
4. At the prompt, click **Delete**.

Create a list of allowed vendors

Provides instructions for creating an allowed vendor list in Catalyst Center, allowing you to reclassify vendor threats as Potential or Informational. Details how to define selection criteria, add up to five vendors per workflow, and apply these rules to specific sites within your network hierarchy.

About this task

You can create a list of allowed vendors. Vendors on this list are not marked as **High** threats.

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

Procedure

1. From the main menu, choose **Workflows** > **Create Allowed Vendor List**.

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

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

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

   The **Create Allowed Vendor List** window opens.

3. From the **Selection Criteria** drop-down list, select a criterion (**Exactly Matches** or **Contains**) for the vendor name.
4. In the **Vendor Name** field, enter the vendor name.

   Vendor name matching is case sensitive.

5. Click ⊕ to add another vendor to the allowed list.

   Per workflow, you can add a maximum of five vendors to the allowed list.

6. In the **Site Selection** window, check the check box next to the site to which you want to apply your allowed vendor list.

   Site inheritance applies the vendor rule to all floors of a site. The rule maps to the area, site, or building level.

7. Click **Next**.
8. In the **Summary** window, view the details about the allowed vendor and site selection.
9. Click **Done**.

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

10. (Optional) To create another allowed vendor list, click **Create New Allowed Vendor List** and repeat Step 3 to Step 8.
11. (Optional) To view the created vendor lists, click **View all allowed Lists**.

8 Rogue and aWIPS Event Notifications

Topics:

- Information about the rogue and aWIPS event notifications

Information about the rogue and aWIPS event notifications

Details how to configure and subscribe to rogue and aWIPS event notifications in Catalyst Center. Explains how to set up destinations like Webhook, PagerDuty, Webex, or syslog servers to receive alerts and notes the notification frequency limitations for specific integration types.

About this task

You can configure Catalyst Center to send a notification whenever a rogue or aWIPS attack takes place. Notifications for these events do not appear in the Catalyst Center Notification Center.

To complete this procedure, ensure that you select and subscribe to a rogue event or an aWIPS event.

Procedure

1. To review threats that occurred before you subscribed to event notifications in the Catalyst Center GUI, click the menu icon and choose **Reports** > **Report Templates** > **Rogue and aWIPS**.
2. To subscribe to a rogue event or an aWIPS event in the Catalyst Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **Event Notifications**.
3. Click **Create New** and complete the **Create a New Notification** workflow. For more information, see the "Create an event notification" topic in the *Cisco Catalyst Center User Guide*.

   Note:

   After you subscribe to a rogue event or an aWIPS event, you receive event notifications.

4. After you subscribe to rogue threat notifications or aWIPS threat notifications, you can receive notifications through REST APIs (Webhook, PagerDuty, and Webex) or a syslog server. See these resources for procedures:
   - To configure the Webhook and syslog destinations, see the “Work with Events” topic in the *Cisco Catalyst Center Platform User Guide*.
   - To configure the PagerDuty destination, see the “Catalyst Center to PagerDuty Integration” topic in the *Catalyst Center ITSM Integration Guide*.
   - To configure the Webex destination, see the “Catalyst Center to Cisco WebEx Integration” topic in the *Catalyst Center ITSM Integration Guide*.

   Note:

   Webex and PagerDuty destinations can send up to 100 event notifications every 5 minutes. If you expect to receive more than 100 events in 5 minutes, use Webhook or syslog destinations.

Rogue events

Outlines the specific conditions and threat types that trigger rogue events in Catalyst Center, including new detections, status changes, and deletions. Details the associated event payload structure, providing key information such as threat MAC addresses, detecting AP details, and containment states for external system integration.

Rogue events are triggered only for these high threat-level rogues:

- Beacon wrong channel
- Beacon DS attack
- AP impersonation
- Rogue on wire
- Honeypot

- Custom rules created with the threat level set to high

Rogue events are triggered when:

- A high threat-level rogue is discovered in the network for the first time `(ROGUE_NEW_THREAT_DETECTED)`
- A high-threat-level rogue is deleted from the network `(ROGUE_THREAT_DELETED)`
- A threat level is changed from **High** to **Potential** or **Informational** `(ROGUE_THREAT_LEVEL_CHANGED)`
- A threat level is changed from **Potential** or **Informational** to **High** `(ROGUE_THREAT_LEVEL_CHANGED)`
- A 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 the 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

That is a spot-on summary of the rogue event triggers and the associated data structure. It accurately captures both the conditions for triggering events and the key fields included in the payload for external integration.

aWIPS events are triggered for all aWIPS threats in the network.

You receive a notification for each detecting AP. If multiple APs detect the same threat, you receive multiple event notifications.

Note:

The maximum aWIPS threat notification limit per signature per day is 2500. When the notifications of a specific signature reach this limit, no more notifications are sent for that signature for that day. A warning message opens in the rogue and aWIPS **Overview** window.

Click **View Signatures** to view the details of aWIPS signatures that have reached the maximum limit.

For source-based aWIPS threats, source information is sent. Destination information is sent as Not Applicable.

For destination-based aWIPS threats, destination information is sent. Source information is sent as Not Applicable.

For pair-based aWIPS threats, both source and destination information are 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
- **detectingApMacAddress**: MAC address of the detecting AP
- **detectingApName**: Name of the detecting AP
- **wlcIp**: IP address of the wireless controller