Cisco DNA Center Rogue Management and aWIPS Application

Introduction to Rogue Management and aWIPS Application

Note In Cisco Digital Network Architecture (DNA) Center releases earlier than Release 2.1.2.0, Rogue Management capabilities were provisioned as a part of Device Controllability. After a Cisco DNA Center upgrade, the provisioned Rogue Management subscriptions are not automatically removed from previously discovered Cisco Wireless Controller. Rogue Management detection might be reported inconsistently on a newly discovered wireless controller.

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

Note Cisco DNA Center release 2.3.7 and later, Rogue Management and aWIPS application package is applicable for Virtual Appliances (VA).

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

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

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 autocontainment for wired and wireless devicesare not supported for IPv6 deployment.

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

- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- Cisco Mobility Express

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

- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-CL Cloud Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-CL Cloud Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Embedded Wireless Controller on Catalyst Access Points

About Rogue Management

The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps

in quickly identifying the highest-priority threats and allows you to monitor these threats in the **Rogue and aWIPS** dashboard within Cisco DNA Assurance.

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

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

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

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

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

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

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

- If the AP is unknown to Cisco DNA Center, and is using the same SSID as your network, Cisco DNA Center classifies the AP as 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 Cisco DNA Center. The Honeypot classification does not happen when the detected SSID is not restored back on Cisco DNA Center when the Cisco DNA Center backup is restored.

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

About Advanced Wireless Intrusion Prevention System

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

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

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

aWIPS supports the following capabilities:

- Static signatures
- Standalone signature detection
- Alarms
- Static signature file packaged with controller and AP image

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

- **Authentication flood**: A form of 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.
- **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

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

Table 1: Number of Rogue APs and Rogue Clients Supported

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

Basic Setup Workflow

Step 1 Install Cisco DNA Center.

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

Step 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 Cisco DNA Center.

Step 3 From Release 1.3.3.0 onwards, you must enable Rogue and aWIPS application in the **Assurance** > **Rogue and aWIPS** window.

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

To access the Rogue and aWIPS application, log in to Cisco DNA Center. From the top-left corner, click the menu icon and choose **Assurance** > **Rogue and aWIPS**.

Step 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.

Step 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.

Step 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, if you have an existing network hierarchy in Cisco Prime Infrastructure, import it into Cisco DNA Center.

Step 7 Add the location information of APs and position the APs on the floor map to get a coverage heatmap visualization.

Step 8 (Optional) If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Cisco DNA Assurance for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system, in Cisco DNA Assurance. For more information see, About Cisco ISE Configuration for Cisco DNA Center topic in the *Cisco DNA Assurance User Guide*.

Step 9 (Optional) Configure syslog, SNMP traps, and NetFlow Collector servers using Telemetry. For more information, See Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry topic in the *Cisco DNA Assurance User Guide*.

Step 10 Start using the Cisco DNA Assurance application.

Step 11 (Optional) Integrate and synchronize Cisco Connected Mobile Experiences (CMX) with Cisco DNA Center. For more information, see About Cisco Connected Mobile Experiences Integration topic in the *Cisco DNA Assurance User Guide*.

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

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