# Rogue and aWIPS Event Notifications



# Information About the Rogue and aWIPS Event Notifications

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

- See the "Work with Events" topic in the *Cisco DNA Center Platform User Guide* to configure the Webhook and syslog destinations.
- See the "Cisco DNA Center to PagerDuty Integration" topic in the *Cisco DNA Center ITSM Integration Guide* to configure the PagerDuty destination.
- See the "Cisco DNA Center to Cisco WebEx Integration" topic in the *Cisco DNA Center ITSM Integration Guide* to configure the Webex destination.

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

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

**Note** You will receive event notifications only after subscription to a rogue or aWIPS event. For threats that occurred before this subscription, in the Cisco DNA Center GUI, click the menu icon and choose **Reports** > **Report Templates** > **Rogue and aWIPS**.

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

## Rogue Events

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

- Beacon Wrong Channel

- Beacon DS Attack
- AP Impersonation
- Rogue on Wire
- Honeypot
- Custom Rules created with Threat Level as 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)`
- Threat level is changed from **High** to **Potential** or **Informational** `(ROGUE_THREAT_LEVEL_CHANGED)`
- Threat level is changed from **Potential** or **Informational** to **High** `(ROGUE_THREAT_LEVEL_CHANGED)`
- Threat level remains **High** but threat type changes `(ROGUE_THREAT_TYPE_CHANGED)`

**Rogue Events Payload Details:**

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

**Commands in Payload**:

- threatMacAddress: MAC address of the rogue AP
- threatType: Type of rogue threat (Beacon DS Attack, AP Impersonation, Rogue on Wire, Honeypot, or Custom Rules created with Threat Level as High)
- threatState: State of the rogue threat (ROGUE_NEW_THREAT_DETECTED, ROGUE_THREAT_DELETED, ROGUE_THREAT_LEVEL_CHANGED), ROGUE_THREAT_LEVEL_CHANGED, or ROGUE_THREAT_TYPE_CHANGED
- threatLevel: State of the rogue (High, Potential, or Informational)
- detectingApName: Name of the strongest detecting AP
- detectingApMacAddress: MAC address of the strongest detecting AP
- detectingApLocation: Location of 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

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

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

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

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

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

**aWIPS Events Payload Details**:

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

**Commands in Payload**:

- **attackType**: Type of the aWIPS attack
- **sourceMacAddress**: MAC address of the attacker
- **sourceVendorName**: Vendor name of the attacker
- **targetMacAddress**: MAC address of the target
- **detectingApLocation**: Location of the detecting AP
- **detectingApMacAddress**: MAC address of the detecting AP
- **detectingApName**: Name of the detecting AP
- **wlcIp**: IP address of the wireless controller