Wireless Intrusion Detection System

- Protected Management Frames (Management Frame Protection), on page 1
- Client Exclusion Policies, on page 4
- Rogue Devices, on page 6
- Rogue Access Point Classification, on page 17
- Cisco Intrusion Detection System, on page 31
- Intrusion Detection System Signatures, on page 35
- SNMP, on page 43
- Wireless Intrusion Prevention System, on page 48

Protected Management Frames (Management Frame Protection)

By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure management frame protection (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.

Infrastructure MFP

Infrastructure MFP protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue APs, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by APs (and not those emitted by clients), which are then validated by other APs in the network. Infrastructure MFP is passive, can detect and report intrusions but has no means to stop them.

Infrastructure MFP consists of three main components:

- **Management frame protection**: The AP protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving AP configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight APs.
- **Management frame validation**: In infrastructure MFP, the AP validates every management frame that it receives from other APs in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives

any frame that does not contain a valid MIC IE from a BSSID belonging to an AP that is configured to transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Time Protocol (NTP) synchronized.

- **Event reporting**: The AP notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.

Infrastructure MFP is disabled by default, and you can enable it globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if you have enabled AP authentication because the two features are mutually exclusive. When you enable infrastructure MFP globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected APs.

Note CCXv5 client MFP is no longer supported. Client MFP is enabled as optional by default on WLANs that are configured for WPA2. However, client MFP is not supported on Wave 2 APs or 802.11ax Wi-Fi6 APs, and there exist no clients that support CCXv5.

802.11w PMF

802.11w standard protects the transmission of control and management frames, between APs and clients, against forgery and replay attacks. The frame types protected include Disassociation, Deauthentication, and Robust Action frames such as:

- Spectrum Management
- Quality of Service (QoS)
- Block Ack
- Radio measurement
- Fast Basic Service Set (BSS) Transition

For information about 802.11w PMF, see the 802.11w section.

Additional Reference: Configure 802.11w Management Frame Protection on WLC

This section contains the following subsections:

Configuring Infrastructure MFP (GUI)

Procedure

Step 1 Choose **Security> Wireless Protection Policies > AP Authentication/MFP** to open the AP Authentication Policy page.

Step 2 Enable infrastructure MFP globally for the controller by choosing **Management Frame Protection** from the **Protection Type** drop-down list.

Step 3 Click **Apply** to commit your changes.

Note If more than one controller is included in the mobility group, you must configure an NTP/SNTP server on all controllers in the mobility group that are configured for infrastructure MFP.

Step 4 Configure client MFP for a particular WLAN after infrastructure MFP has been enabled globally for the controller as follows:

a) Choose **WLANs**.
b) Click the profile name of the desired **WLAN**. The **WLANs > Edit** page appears.
c) Choose **Advanced**. The **WLANs > Edit (Advanced) page** is displayed.
d) From the **MFP Client Protection** drop-down list, choose **Disabled**, **Optional**, or **Required** . The default value is **Optional**. If you choose **Required**, clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the controller and the client supports CCXv5 MFP and is also configured for WPA2).
e) Click **Apply** to commit your changes.

Step 5 Save the configuration.

Related Topics

Configuring 802.11w (GUI)

Viewing the Management Frame Protection Settings (GUI)

To see the controller's current global MFP settings, choose **Security** > **Wireless Protection Policies** > **Management Frame Protection**. The Management Frame Protection Settings page appears.

On this page, you can see the following MFP settings:

- The **Management Frame Protection** field shows if infrastructure MFP is enabled globally for the controller.
- The **Controller Time Source Valid** field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as the NTP/SNTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
- The **Client Protection** field shows if client MFP is enabled for individual WLANs and whether it is optional or required.

Configuring Infrastructure MFP (CLI)

Procedure

- Enable or disable infrastructure MFP globally for the controller by entering this command:

  config wps mfp infrastructure {enable | **disable}**
- Enable or disable client MFP on a specific WLAN by entering this command:

  config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

  If you enable client MFP and use the optional **required** parameter, clients are allowed to associate only if MFP is negotiated.

Related Topics

Configuring 802.11w (CLI)

Viewing the Management Frame Protection Settings (CLI)

Procedure

- See the controller's current MFP settings by entering this command:

  show wps mfp summary

- See the current MFP configuration for a particular WLAN by entering this command:

  show wlan wlan_id

- See whether client MFP is enabled for a specific client by entering this command:

  show client detail *client_mac*

- See MFP statistics for the controller by entering this command:

  show wps mfp *statistics*

Note This report contains no data unless an active attack is in progress. This table is cleared every 5 minutes when the data is forwarded to any network management stations.

Debugging Management Frame Protection Issues (CLI)

Procedure

- Use this command if you experience any problems with MFP:

  debug wps mfp ? {**enable** | **disable**}

  where ? is one of the following:

  client—Configures debugging for client MFP messages.

  capwap—Configures debugging for MFP messages between the controller and access points.

  detail—Configures detailed debugging for MFP messages.

  report—Configures debugging for MFP reporting.

  mm—Configures debugging for MFP mobility (inter-controller) messages.

Client Exclusion Policies

This section contains the following subsections:

Configuring Client Exclusion Policies (GUI)

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** to open the Client Exclusion Policies page.

Step 2 Select any of these check boxes if you want the controller to exclude clients for the condition specified. The default value for each exclusion policy is enabled.

- **Excessive 802.11 Association Failures**—Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- **Excessive 802.11 Authentication Failures**—Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- **Excessive 802.1X Authentication Failures**—Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- **IP Theft or IP Reuse**—Clients are excluded if the IP address is already assigned to another device.
- **Excessive Web Authentication Failures**—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

Step 3 Save your configuration.

Configuring Client Exclusion Policies (CLI)

Procedure

Step 1 Enable or disable the controller to exclude clients on the sixth 802.11 association attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-assoc {**enable** | **disable**}

Step 2 Enable or disable the controller to exclude clients on the sixth 802.11 authentication attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-auth {**enable** | **disable**}

Step 3 Enable or disable the controller to exclude clients on the fourth 802.1X authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion 802.1x-auth {**enable** | **disable**}

Step 4 Configure the controller to exclude clients that reaches the maximum failure 802.1X authentication attempt with the RADIUS server by entering this command:

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts

You can configure the maximum failure 802.1X authentication attempt from 1 to 3 and the default value is 3.

Step 5 Enable or disable the controller to exclude clients if the IP address is already assigned to another device by entering this command:

config wps client-exclusion ip-theft {**enable** | **disable**}

Step 6 Enable or disable the controller to exclude clients on the fourth web authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion web-auth {**enable** | **disable**}

Step 7 Enable or disable the controller to exclude clients for all of the above reasons by entering this command:

config wps client-exclusion all {**enable** | **disable**}

Step 8 Use the following command to add or delete client exclusion entries.

config exclusionlist {**add** *mac-addr description* | **delete** *mac-addr* | **description** *mac-addr description*}

Step 9 Save your changes by entering this command:

save config

Step 10 See a list of clients that have been dynamically excluded, by entering this command:

show exclusionlist

Information similar to the following appears:

```
Dynamically Disabled Clients
----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------

00:40:96:b4:82:55         802.1X Failure           51
```

Step 11 See the client exclusion policy configuration settings by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
 Auto-Immune................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
  Maximum 802.1x-AAA failure attempts............ 3

Signature Policy
  Signature Processing....................... Enabled
```

Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point 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 access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network

resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.
- In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point and FlexConnect mode access point in channel 157 or channel 161 are less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.
- The local and FlexConnect mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.
- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementations might mitigate the effectiveness of ad hoc containment.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three per radio (or six per radio for access points in the monitor mode).
- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller , RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller . The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.
- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.

- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.
- The controller requests to the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling **Validate Rogue Clients Against AAA**.
- The controller has to be added to the AAA server as a AAA client with authentication as RADIUS(CISCO IOS/PIX 6.0). Add the rogue AP in question to the userdatabase with relevant delimiter, username, and password being the MAC address with relevant delimiter. You must define the [009\001] cisco-av-pair for this user with the following keywords:
  - rogue-ap-state=contain—Where, rogue-ap-state can be the following: alert/contain/internal/external/threat
  - rogue-ap-class=malicious—Where, rogue-ap-class can be following keywords: unclassified/malicious/friendly

  The allowed combinations of class/state are:
  - unclassified—alert/contain/threat
  - malicious—alert/contain/threat
  - friendly—alert/internal/external
- All the valid client MAC details should be registered in the AAA authentication server with the same MAC delimiter options as set in the RADIUS configuration on the controller . For more information about configuring MAC delimiter options, see the Configuring RADIUS (GUI) section.
- In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller .
- All rogues that are marked as friendly or contained state (due to auto or rule or manual) are stored in the flash memory of the controller . When you reboot the controller loaded with Release 7.4, these rogues are shown as manually changed. If you wish to reboot the controller , you need to clear all rogue APs and rogue adhoc from the controller , save the configuration, and then reboot the controller .
- All rogues that are marked as friendly or contained state (only due to manual) are stored in the flash memory of the controller . If you upgrade the controller from the Release 7.4 to 7.6 or later versions, then all rogues stored in the Release 7.4 are shown as manually classified (if friendly classified) or manually contained. Hence after upgrading the controller from the Release 7.4 to 7.6 or later versions, you need to delete all rogue APs and rogue adhoc from the controller and then start configuring rogue detection.
- A FlexConnect AP (with rogue detection enabled) in the connected mode takes the containment list from the controller . If auto-contain SSID and auto contain adhoc are set in the controller , then these configurations are set to all FlexConnect APs in the connected mode and the AP stores it in its memory.

  When the FlexConnect AP moves to a standalone mode, the following tasks are performed:
  - The containment set by the controller continues.

- If the FlexConnect AP detects any rogue AP that has same SSID as that of infra SSID (SSID configured in the controller that the FlexConnect AP is connected to), then containment gets started if auto contain SSID was enabled from the controller before moving to the standalone mode.
- If the FlexConnect AP detects any adhoc rogue, containment gets started if **auto-contain adhoc** was enabled from the controller when it was in the connected mode.

When the standalone FlexConnect AP moves back to the connected mode, then the following tasks are performed:

- All containment gets cleared.
- Containment initiated from the controller will take over.

- The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.
- The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.
- In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby controller starts only after the rogue detection pending stabilization time, which is 300 seconds. Therefore, the active configurations on the standby controller are reflected only after 300 seconds.
- After an AP is moved from rogue detection mode to any other mode or after an AP is moved from sniffer mode to local or monitor mode, the rogue detection functionality is not retained on the AP. To enable rogue detection functionality on the AP, you have to explicitly move the AP to the rogue detection mode.
- Some rogue devices exhibit RSSI value of –128 dBm although the minimum RSSI has seen configured to a higher value. In some scenarios, APs show the RSSI value of 0 for some rogue devices. If the controller receives the RSSI value as 0, the controller invalidates the value and replaces it with –128 dBm so that rogue rules or policies are not applied to the rogue device.
- Even though rogue events are reported to Cisco DNA Center instantly, due to a big number of rogue events, the rogue sync occurs only on detection, on moving to contained state, and every half hour. The rogue sync does not occur for any other rogue event.

Note A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.

Note No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the **config trapflags rogueap** {**enable** | **disable**} command, which is also used for rouge APs. In GUI configuration also, you should use the rogue AP flag under **Management** > **SNMP** > **TrapControl** > **Security** > **Rogue AP** to control rogue clients.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Note Use the **debug dot11 rldp enable** command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller .

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller , followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller 's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note The RLDP packets are unable to reach the controller if filtering rules are placed between the controller 's network and the network where the rogue device is located.

Restrictions for RLDP:

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.

- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses FlexConnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **config rogue ap rldp retries** command.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.

   config rogue ap rldp initiate *mac-address*

2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.

   config rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:
   - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   - Either auto RLDP or schedule of RLDP can be enabled at a time.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

This section contains the following subsections:

Configuring Rogue Detection (GUI)

Procedure

Step 1 Make sure that rogue detection is enabled on the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page.

Step 2 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **General**.

The **Rogue Policies** page is displayed.

Step 3 Choose one of the following options from the **Rogue Location Discovery Protocol** drop-down list:

- **Disable**—Disables RLDP on all the access points. This is the default value.
- **All APs**—Enables RLDP on all the access points.
- **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.

Step 4 In the **Expiration Timeout for Rogue AP and Rogue Client Entries** text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

Step 5 To use the AAA server or local database to validate if rogue clients are valid clients, select the **Validate Rogue Clients Against AAA** check box. By default, the check box is unselected.

Note To validate a rogue client against AAA, the format of the Cisco AVP pair is mandatory. The free RADIUS format is:

- e09d3166fb2c Cleartext-Password := "e09d3166fb2c"
- Cisco-AVPair := "rogue-ap-state=threat"

Step 6 If necessary, select the **Detect and Report Ad-Hoc Networks** check box to enable ad hoc rogue detection and reporting. By default, the check box is selected.

Step 7 In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs send the rogue detection report to the Cisco WLC. The valid range is 10 to 300 seconds, and the default value is 10 seconds.

Note The minimum value of 10 seconds is applicable only to APs in monitor mode. For the APs in Local mode, the minimum interval value that you can set is 30 seconds.

Step 8 In the **Rogue Detection Minimum RSSI** text box, enter the minimum Received Signal Strength Indicator (RSSI) value for APs to detect the rogue and for a rogue entry to be created in the controller. The valid range is –128 dBm to –0 dBm, and the default value is 0 dBm.

Note This feature is applicable to all the AP modes. There can be many rogues with weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs detect rogues.

Step 9 In the **Rogue Detection Transient Interval** text box, enter the time interval at which a rogue should be scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the controller. Thus, the APs filter the transient rogues, which are active for a short period and are then silent. The valid range is between 120 to 1800 seconds, and the default value is 0.

The rogue detection transient interval is applicable to the monitor mode APs only.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues is avoided.

Step 10 If you want the controller to automatically contain certain rogue devices, enable the following parameters. By default, these parameters are in disabled state.

Caution When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed: "`Using this feature may have legal consequences. Do you want to continue?`" The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

- **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to **1**.
- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.
- **Using Our SSID**—Configure the auto containment of rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **Valid Client on Rogue AP**—Configure the auto containment of a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

- **AdHoc Rogue AP**—Configure the auto containment of ad hoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring Rogue Detection (CLI)

Procedure

Step 1 Ensure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all the access points that are associated with the controller. You can enable or disable rogue detection for individual access points by entering this command:

config rogue detection {**enable** | **disable**} *cisco-ap command.*

Note To see the current rogue detection configuration for a specific access point, enter the **show ap config general** *Cisco_AP* command.

Note Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Step 2 Enable, disable, or initiate RLDP by entering these commands:

- **config rogue ap rldp enable alarm-only**—Enables RLDP on all the access points.
- **config rogue ap rldp enable alarm-only** *monitor_ap_only*—Enables RLDP only on the access points in the monitor mode.
- **config rogue ap rldp initiate** *rogue_mac_address*—Initiates RLDP on a specific rogue access point.
- **config rogue ap rldp disable**—Disables RLDP on all the access points.
- **config rogue ap rldp retries**—Specifies the number of times RLDP to be tried per rogue access point. The range is from 1 to 5 and default is 1.

Step 3 Specify the number of seconds after which the rogue access point and client entries expire and are removed from the list by entering this command:

config rogue ap timeout *seconds*

The valid range for the *seconds* parameter is 240 to 3600 seconds (inclusive). The default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for a classification type.

Step 4 Enable or disable ad hoc rogue detection and reporting by entering this command:

config rogue adhoc {**enable** | **disable**}

Step 5 Enable or disable the AAA server or local database to validate if rogue clients are valid clients by entering this command:

config rogue client aaa {**enable** | **disable**}

Step 6 Specify the time interval, in seconds, at which APs should send the rogue detection report to the controller by entering this command:

config rogue detection monitor-ap report-interval *time in sec*

The valid range for the *time in sec* parameter is 10 seconds to 300 seconds. The default value is 10 seconds.

Note This feature is applicable only to the monitor mode APs.

Step 7 Specify the minimum RSSI value that rogues should have for APs to detect them and for the rogue entries to be created in the controller by entering this command:

config rogue detection min-rssi *rssi in dBm*

The valid range for the *rssi in dBm* parameter is –128 dBm to 0 dBm. The default value is 0 dBm.

Note This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

Step 8 Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned for by entering this command:

config rogue detection monitor-ap transient-rogue-interval *time in sec*

The valid range for the *time in sec* parameter is 120 seconds to 1800 seconds. The default value is 0.

Note This feature is applicable only to the monitor mode APs.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

Step 9 If you want the controller to automatically contain certain rogue devices, enter these commands.

Caution When you enter any of these commands, the following message is displayed: `Using this feature may have legal consequences. Do you want to continue?` The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

- **config rogue ap rldp enable auto-contain**—Automatically contains the rogues that are detected on the wired network.
- **config rogue ap ssid auto-contain**—Automatically contains the rogues that are advertising your network's SSID.

Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap ssid alarm** command.

- **config rogue ap valid-client auto-contain**—Automatically contains a rogue access point to which trusted clients are associated.

  Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap valid-client alarm** command.

- **config rogue adhoc auto-contain**—Automatically contains ad hoc networks detected by the controller.

  Note If you want the controller to only generate an alarm when such a network is detected, enter the **config rogue adhoc alert** command.

- **config rogue auto-contain level** *level monitor_mode_ap_only*—Sets the auto containment level for the monitor mode access points. The default value is 1.

Step 10 Configure ad hoc rogue classification by entering these commands:

- **config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
- **config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
- **config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*

The following is a brief description of the parameters:

- **internal**—Trusts a foreign ad hoc rogue.
- **external**—Acknowledges the presence of an ad hoc rogue.
- **alert**—Generates a trap when an ad hoc rogue is detected.
- **contain**—Starts containing a rogue ad hoc.

Step 11 Configure RLDP scheduling by entering this command:

config rogue ap rldp schedule { **add** | **delete** | **disable** | **enable** }

- **add**—Enables you to schedule RLDP on a particular day of the week. You must enter the day of the week (for example, **mon**, **tue**, **wed**, and so on) on which you want to schedule RLDP and the start time and end time in HH:MM:SS format. For example: **config rogue ap rldp schedule add mon 22:00:00 23:00:00**.
- **delete**—Enables you to delete the RLDP schedule. You must enter the number of days.
- **disable**— Configure to disable RLDP scheduling.
- **enable**— Configure to enable RLDP scheduling.

Note When you configure RLDP scheduling, it is assumed that the scheduling will occur in the future, that is, after the configuration is saved.

Step 12 Save your changes by entering this command:

save config

Note Rogue client detection on non monitor AP on serving channel was not done until 8.1 Release . From Release 8.1 onwards, serving channel rogue client detection will happen only if WIPS submode is turned on non monitor AP's.

Rogue Access Point Classification

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified. For the Custom type, you must specify a severity score and a classification name.

Note Manual classification and classification that is the result of auto-containment or rogue-on-wire overrides the rogue rule. If you have manually changed the class and/or the state of a rogue AP, then to apply rogue rules to the AP, you must change it to unclassified and alert condition.

Note If you manually move any rogue device to contained state (any class) or friendly state, this information is stored in the standby Cisco WLC flash memory; however, the database is not updated. When HA switchover occurs, the rogue list from the previously standby Cisco WLC flash memory is loaded.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, custom, and unclassified) in the Alert state only.

You can configure up to 64 rogue classification rules per controller.

You can also apply rogue rules to ad hoc rogues except for client count condition.

The number of rogue clients that can be stored in the database table of a rogue access point is 256.

If a rogue AP or an ad hoc rogue is classified because of an RSSI rogue rule condition, the RSSI value that caused the trigger is displayed on the controller GUI/CLI. The controller includes the classified RSSI, the classified AP MAC address, and rule name in the trap. A new trap is generated for every new classification or change of state due to rogue rule but[3] is rate limited to every half hour for every rogue AP or ad hoc rogue. However, if there is a change of state in containment by rogue rule, the trap is sent immediately. The ‘classified by,’ ‘classified at,’ and ‘classified by rule name’ are valid for the non-default classification types, which are Friendly, Malicious, and Custom classifications. For the unclassified types, these fields are not displayed.

Note For the RSSI condition of rogue rule, reclassification occurs only if the RSSI change is more than 2 dBm of the configured RSSI value.

The rogue rule may not work properly if friendly rogue rule is configured with RSSI as a condition. Then, you need to modify the rules with the expectation that friendly rule is using maximum RSSI and modify rules accordingly.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

Table 1: Classification Mapping

Rule-Based Classification Type	Rogue States
Friendly	• Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.
Malicious	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.
Custom	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.

Rule-Based Classification Type	Rogue States
Unclassified	• Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

The classification and state of the rogue access points are configured as follows:

- From Known to Friendly, Internal
- From Acknowledged to Friendly, External
- From Contained to Malicious, Contained

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

This section contains the following subsections:

Guidelines and Restrictions for Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.
- Some are sent for containment by rule and every 30 minutes for rogue classification change. For custom classification, the first trap does not contain the severity score because the trap has existed before the custom classification. The severity score is obtained from the subsequent trap that is generated after 30 minutes if the rogue is classified.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a higher priority rule and is classified, it does not move down the priority list for the same report.
- Previously classified rogue gets re-classified on every new rogue report with the following restrictions:
  - Rogues which are classified as friendly by rule and whose state is set to ALERT, go through re-classification on receiving the new rogue report.
  - If a rogue is classified as friendly by the administrator manually, then the state is INTERNAL and it does not get re-classified on successive rogue reports.
  - If rogue is classified as malicious, irrespective of the state it does not get re-classified on subsequent rogue reports.

- Transition of the rogue's state from friendly to malicious is possible by multiple rogue rules if some attribute is missing in new rogue report.
- Transition of the rogue's state from malicious to any other classification is not possible by any rogue rule.
- The status change of a rogue device to contain or alert does not work when you move it between different class types until you move the class type of the rogue to unclassified.
- If a rogue AP is classified as friendly, it means that the rogue AP exists in the vicinity, is a known AP, and need not be tracked. Therefore, all the rogue clients are either deleted or not tracked if they are associated with the friendly rogue AP.
- Until the controller discovers all the APs through neighbor reports from APs, the rogue APs are kept in unconfigured state for three minutes after they are detected. After 3 minutes, the rogue policy is applied on the rogue APs and the APs are moved to unclassified, friendly, malicious, or custom class. Rogue APs kept in unconfigured state means that no rogue policy has yet been applied on them.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** to open the Rogue Rules page.

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

Note To delete a rule, hover your cursor over the blue drop-down arrow for that rule and click **Remove**.

Step 2 Create a new rule as follows:

a) Click **Add Rule**. An Add Rule section appears at the top of the page.

b) In the **Rule Name** text box, enter a name for the new rule. Ensure that the name does not contain any spaces.

c) From the **Rule Type** drop-down list, choose from the following options to classify rogue access points matching this rule as friendly or malicious:

- **Friendly**
- **Malicious**
- **Custom**

d) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.

Rule description:

- **All**—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure.
- **Global**—Notifies only a trap receiver such as Cisco Prime Infrastructure.
- **Local**—Notifies only Cisco WLC.

- **None**—No notifications are sent.

Note Rogue Rule Notification options **All**, **Global**, **Local**, and **None** can control only the following rogue traps mentioned:

- Rogue AP Detected (Rogue AP: XX:XX:XX:XX:XX:XX detected on Base Radio MAC: XX:XX:XX:XX:XX:XX Interface no: 0(1) Channel: 6 RSSI: 45 SNR: 10 Classification: unclassified, State: alert, RuleClassified : unclassified, Severity Score: 100, RuleName: rule1, Classified AP MAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue Adhoc Detected (Adhoc Rogue : XX:XX:XX:XX:XX:XX detected on Base Radio MAC : XX:XX:XX:XX:XX:XX Interface no: 0(1) on Channel 6 with RSSI: 45 and SNR: 10 Classification: unclassified, State: alert, RuleClassified: unclassified, Severity Score: 100, RuleName: rule1,Classified APMAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue AP contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX has been contained due to rule with containment Level : 1)
- Rogue AP clear contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX is no longer contained due to rule

e) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.
f) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.
g) Click **Add** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 Edit a rule as follows:

a) Click the name of the rule that you want to edit. The **Rogue Rule > Edit** page appears.
b) From the Type drop-down list, choose from the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**
- **Custom**

c) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.
d) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.
e) From the Match Operation text box, choose one of the following:

Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.

Match Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.

f) To enable this rule, select the **Enable Rule** check box. The default value is unselected.
g) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.
h) From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click **Add Condition**.

- **SSID**—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the **User Configured SSID** text box, and click **Add SSID**.

  Note To delete an SSID, highlight the SSID and click **Remove**.

- **RSSI**—Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the **Minimum RSSI** text box. The valid range is 0 to –128 dBm (inclusive).
- **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the **Time Duration** text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
- **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the **Minimum Number of Rogue Clients** text box. The valid range is 1 to 10 (inclusive), and the default value is 0.
- **No Encryption**—Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  Note Cisco Prime Infrastructure refers to this option as "Open Authentication."

- **Managed SSID**—Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

  Note The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

  You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

  Note To delete a condition from this rule, hover your cursor over the blue drop-down arrow for that condition and click **Remove**.

i) Click **Apply**.

Step 4 Click **Save Configuration**.

Step 5 If you want to change the order in which rogue classification rules are applied, follow these steps:

a. Click **Back** to return to the Rogue Rules page.

b. Click **Change Priority** to access the Rogue Rules > Priority page.

The rogue rules are listed in priority order in the Change Rules Priority text box.

c. Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

d. Continue to move the rules up or down until the rules are in the desired order.

e. Click **Apply**.

Step 6 Classify any rogue access points as friendly and add them to the friendly MAC address list as follows:

- Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Friendly Rogue** to open the Friendly Rogue > Create page.
- In the MAC Address text box, enter the MAC address of the friendly rogue access point.
- Click **Apply**.
- Click **Save Configuration**. This access point is added to the controller's list of friendly access points and should now appear on the Friendly Rogue APs page.

Viewing and Classifying Rogue Devices (GUI)

Before you begin

Caution When you choose to **contain a rogue device**, the following warning appears: "There may be legal issues following this containment. Are you sure you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Procedure

Step 1 Choose **Monitor** > **Rogues**.

Step 2 Choose the following options to view the different types of rogue access points detected by the controller:

- **Friendly APs**
- **Malicious APs**
- **Unclassified APs**
- **Custom APs**

The respective rogue APs pages provide the following information: the MAC address and SSID of the rogue access point, channel number, the number of radios that detected the rogue access point, the number of clients connected to the rogue access point, and the current status of the rogue access point.

Note To remove acknowledged rogues from the database, change the rogue state to Alert. If the rogue is no longer present, the rogue data is deleted from the database in 20 minutes.

Note To delete a rogue access point from one of these pages, hover your cursor over the blue drop-down arrow and click **Remove**. To delete multiple rogue access points, select the check box corresponding to the row you want to delete and click **Remove**.

Note You can move the Malicious or Unclassified rogue APs that are being contained or were contained back to Alert state by clicking the **Move to Alert** button on the respective pages.

Step 3 Get more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears.

This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device.

The Class Type text box shows the current classification for this rogue access point:

- **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.
- **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

  Note Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

- **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.
- **Custom**—A user-defined classification type that is tied to rogue rules. It is not possible to manually classify a rogue as Custom. Custom class change can occur only using rogue rules.

Step 4 If you want to change the classification of this device, choose a different classification from the Class Type drop-down list.

Note A rogue access point cannot be moved to another class if its current state is Contain.

Step 5 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 View any rogue clients that are connected to the controller by choosing **Rogue Clients**. The Rogue Clients page appears. This page shows the following information: the MAC address of the rogue client, the MAC

address of the access point to which the rogue client is associated, the SSID of the rogue client, the number of radios that detected the rogue client, the date and time when the rogue client was last reported, and the current status of the rogue client.

Step 9 Obtain more details about a rogue client by clicking the MAC address of the client. The Rogue Client Detail page appears.

This page provides the following information: the MAC address of the rogue client, the MAC address of the rogue access point to which this client is associated, the SSID and IP address of the rogue client, the dates and times when the rogue client was first and last reported, and the current status of the rogue client.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue client:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.

The bottom of the page provides information on the access points that detected this rogue client.

Step 11 Click **Apply**.

Step 12 If desired, you can test the controller's connection to this client by clicking **Ping**.

Step 13 Click **Save Configuration**.

Step 14 See any ad-hoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the ad-hoc rogue, the number of radios that detected the ad-hoc rogue, and the current status of the ad-hoc rogue.

Step 15 Obtain more details about an ad-hoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the ad-hoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 16 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this ad-hoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.
- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

Step 17 From the Maximum number of APs to contain the rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this ad-hoc rogue: **1**, **2**, **3**, or **4**.

The bottom of the page provides information on the access points that detected this ad-hoc rogue.

- **1**—Specifies targeted rogue access point is contained by one access point. This is the lowest containment level.
- **2**—Specifies targeted rogue access point is contained by two access points.
- **3**—Specifies targeted rogue access point is contained by three access points.

- **4**—Specifies targeted rogue access point is contained by four access points. This is the highest containment level.

Step 18 Click **Apply**.

Step 19 Click **Save Configuration**.

Step 20 View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.

This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to Cisco Prime Infrastructure maps by the users. The controller regards these autonomous access points as rogues even though the Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to the Prime Infrastructure. If the Prime Infrastructure finds this access point in its autonomous access point list, the Prime Infrastructure sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If a user removes an autonomous access point from the Prime Infrastructure, the Prime Infrastructure sends a command to the controller to remove this access point from the rogue-ignore list.

Configuring Rogue Classification Rules (CLI)

Procedure

Step 1 Create a rule by entering this command:

config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious**} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 2 Create a rule by entering these commands:

- Configure a rule for friendly rogues by entering this command:

  config rogue rule add ap priority *priority* **classify friendly notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **internal** | **external**} *rule-name*

- Configure a rule for malicious rogues by entering this command:

  config rogue rule add ap priority *priority* **classify malicious notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*

- Configure a rule for custom rogues by entering this command:

  config rogue rule add ap priority *priority* **classify custom** *severity-score classification-name* **notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious** | **custom** *severity-score classification-name*} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 3 Configure the state on the rogue AP upon rule match by entering this command:

config rogue rule state {**alert** | **contain** | **internal** | **external**} *rule-name*

Step 4 Configure the notification upon rule match by entering this command:

config rogue rule notify {**all** | **global** | **local** | **none**} *rule-name*

Step 5 Disable all rules or a specific rule by entering this command:

config rogue rule disable {*all* | *rule_name*}

Note A rule must be disabled before you can modify its attributes.

Step 6 Add conditions to a rule that the rogue access point must meet by entering this command:

config rogue rule condition ap set *condition_type condition_value rule_name*

The following condition types are available:

- **ssid**—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the controller. If you choose this option, enter the SSID for the *condition_value parameter*. The SSID is added to the user-configured SSID list.

  Note If you ever want to delete all of the SSIDs or a specific SSID from the user-configured SSID list, enter the **config rogue rule condition ap delete ssid** {**all** | **ssid**} *rule_name* command.

  Note The sub-string should be specified in full or part of SSID (without any asterisks). This sub-string is matched in the same sequence to its occurrence in the rogue AP SSID. Once the condition is met, the rogue AP is classified (depending on OR or AND match condition).

- **rssi**—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the *condition_value parameter*.

  In Release 8.0 and later releases, for friendly rogue rules, you are required to set a maximum RSSI value. The RSSI value of the rogue AP must be less than the RSSI value set, for the rogue AP to be classified as a friendly rogue. For malicious and custom rogue rules, there is no change in functionality.

For example, for a friendly rogue rule, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is less than –80 dBm are classified as friendly rogues. For malicious and custom rogue rules, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is more than –80 dBm are classified as malicious or custom rogue APs.

- **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the *condition_value parameter*. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
- **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the *condition_value parameter*. The valid range is 1 to 10 (inclusive), and the default value is 0.
- **managed-ssid**—Requires that the rogue access point's SSID be known to the controller. A *condition_value parameter* is not required for this option.

Note You can add up to six conditions per rule. If you ever want to delete all of the conditions or a specific condition from a rule, enter the **config rogue rule condition ap delete all** *condition_type condition_value rule_name* command.

Step 7 Specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule by entering this command:

config rogue rule match {**all** | **any**} *rule_name*

Step 8 Enable all rules or a specific rule by entering this command:

config rogue rule enable {**all** | **rule_name**}

Note For your changes to become effective, you must enable the rule.

Step 9 Add a new friendly access point entry to the friendly MAC address list or delete an existing friendly access point entry from the list by entering this command:

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

Step 10 Save your changes by entering this command:

save config

Step 11 View the rogue classification rules that are configured on the controller by entering this command:

show rogue rule summary

Step 12 View detailed information for a specific rogue classification rule by entering this command:

show rogue rule detailed *rule_name*

Viewing and Classifying Rogue Devices (CLI)

Procedure

- View a list of all rogue access points detected by the controller by entering this command:

  show rogue ap summary
- See a list of the friendly rogue access points detected by the controller by entering this command:

  show rogue ap friendly summary
- See a list of the malicious rogue access points detected by the controller by entering this command:

  show rogue ap malicious summary
- See a list of the unclassified rogue access points detected by the controller by entering this command:

  show rogue ap unclassified summary
- See detailed information for a specific rogue access point by entering this command:

  show rogue ap detailed *ap_mac_address*
- See the rogue report (which shows the number of rogue devices detected on different channel widths) for a specific 802.11a/n/ac radio by entering this command:

  show ap auto-rf 802.11a *Cisco_AP*
- See a list of all rogue clients that are associated to a rogue access point by entering this command:

  show rogue ap clients *ap_mac_address*
- See a list of all rogue clients detected by the controller by entering this command:

  show rogue client summary
- See detailed information for a specific rogue client by entering this command:

  show rogue client detailed *Rogue_AP client_mac_address*
- See a list of all ad-hoc rogues detected by the controller by entering this command:

  show rogue adhoc summary
- See detailed information for a specific ad-hoc rogue by entering this command:

  show rogue adhoc detailed *rogue_mac_address*
- See a summary of ad hoc rogues based on their classification by entering this command:

  show rogue adhoc {**friendly** | **malicious** | **unclassified**} **summary**
- See a list of rogue access points that are configured to be ignore by entering this command:

  show rogue ignore-list
- Classify a rogue access point as friendly by entering this command:

  config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

  where

  internal means that the controller trusts this rogue access point.

external means that the controller acknowledges the presence of this rogue access point.

Note A rogue access point cannot be moved to the Friendly class if its current state is Contain.

- Mark a rogue access point as malicious by entering this command:

  config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

  where

  alert means that the controller forwards an immediate alert to the system administrator for further action.

  contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

Note A rogue access point cannot be moved to the Malicious class if its current state is Contain.

- Mark a rogue access point as unclassified by entering this command:

  config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

Note A rogue access point cannot be moved to the Unclassified class if its current state is Contain.

alert means that the controller forwards an immediate alert to the system administrator for further action.

contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

- Choose the maximum number of access points used to contain the ad-hoc rogue by entering this command:

  config rogue ap classify unclassified state contain *rogue_ap_mac_address 1, 2, 3, or 4*

  - **1**—Specifies targeted rogue access point will be contained by one access point. This is the lowest containment level.
  - **2**—Specifies targeted rogue access point will be contained by two access points.
  - **3**—Specifies targeted rogue access point will be contained by three access points.
  - **4**—Specifies targeted rogue access point will be contained by four access points. This is the highest containment level.

- Specify how the controller should respond to a rogue client by entering one of these commands:

  config rogue client alert *client_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

  config rogue client contain *client_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

- Specify how the controller should respond to an ad-hoc rogue by entering one these commands:

config rogue adhoc alert *rogue_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

config rogue adhoc contain *rogue_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

config rogue adhoc external *rogue_mac_address*—The controller acknowledges the presence of this ad-hoc rogue.

- Configure the classification of ad hoc rogues by entering any one of these commands:
  - Friendly state—**config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
  - Malicious state—**config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
  - Unclassified state—**config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*
- View a summary of custom rogue AP information by entering this command:

  show rogue ap custom summary
- See custom ad hoc rogue information by entering this command:

  show rogue adhoc custom summary
- Delete the rogue APs by entering this command:

  config rogue ap delete {**class** | **all** | *mac-addr*}
- Delete the rogue clients by entering this command:

  config rogue client delete {**state** | **all** | *mac-addr*}
- Delete the ad hoc rogues by entering this command:

  config rogue adhoc delete {**class** | **all** | *mac-addr*}
- Save your changes by entering this command:

  save config

Cisco Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect potential attacks:

- IDS sensors
- IDS signatures

You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the controller can query the sensor to get the list of shunned clients.

This section contains the following subsections:

Shunned Clients

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.

Configuring IDS Sensors (GUI)

Procedure

Step 1 Choose **Security** > **Advanced** > **CIDS** > **Sensors** to open the CIDS Sensors List page.

Note If you want to delete an existing sensor, hover your cursor over the blue drop-down arrow for that sensor and choose **Remove**.

Step 2 Click **New** to add a new IDS sensor to the list. The **CIDS Sensor Add** page is displayed.

Step 3 From the **Index** drop-down list, choose a number (between 1 and 5) to determine the sequence in which the controller consults the IDS sensors. For example, if you choose 1, the controller consults this IDS sensor first.

Cisco WLC supports up to five IDS sensors.

Step 4 In the **Server Address** text box, enter the IP address of your IDS server.

Step 5 In the **Port** text box, enter the number of the HTTPS port through which the controller has to communicate with the IDS sensor.

We recommend that you set this parameter to 443 because the sensor uses this value to communicate by default. The default value is 443 and the range is 1 to 65535.

Step 6 In the **Username** text box, enter the name that the controller uses to authenticate to the IDS sensor.

Note This username must be configured on the IDS sensor and have at least a read-only privilege.

Step 7 In the **Password** and **Confirm Password** text boxes, enter the password that the controller uses to authenticate to the IDS sensor.

Step 8 In the **Query Interval** text box, enter the time (in seconds) for how often the controller should query the IDS server for IDS events.

The default is 60 seconds and the range is 10 to 3600 seconds.

Step 9 Check the **State** check box to register the controller with this IDS sensor or uncheck this check box to disable registration. The default value is disabled.

Step 10 Enter a 40-hexadecimal-character security key in the **Fingerprint** text box. This key is used to verify the validity of the sensor and is used to prevent security attacks.

Note Make sure you include colons that appear between every two bytes within the key. For example, enter AA:BB:CC:DD.

Step 11 Click **Apply**. Your new IDS sensor appears in the list of sensors on the CIDS Sensors List page.

Step 12 Click **Save Configuration**.

Viewing Shunned Clients (GUI)

Procedure

Step 1 Choose **Security** > **Advanced > CIDS** > **Shunned Clients** to open the CIDS Shun List page.

This page shows the IP address and MAC address of each shunned client, the length of time that the client's data packets should be blocked by the controller as requested by the IDS sensor, and the IP address of the IDS sensor that discovered the client.

Step 2 Click **Re-sync** to purge and reset the list as desired.

Note The controller does not take any action on shun entries when the corresponding timers have expired. The shun entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.

Configuring IDS Sensors (CLI)

Procedure

Step 1 Add an IDS sensor by entering this command:

config wps cids-sensor add index ids_ip_address username password.

The index parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. Enter a number (between 1 and 5) to determine the priority of this sensor. For example, if you enter 1, the controller consults this IDS sensor first.

Note The username must be configured on the IDS sensor and have at least a read-only privilege.

Step 2 (Optional) Specify the number of the HTTPS port through which the controller is to communicate with the IDS sensor by entering this command:

config wps cids-sensor port index port

For the port-number parameter, you can enter a value between 1 and 65535. The default value is 443. This step is optional because we recommend that you use the default value of 443. The sensor uses this value to communicate by default.

Step 3 Specify how often the controller should query the IDS server for IDS events by entering this command:

config wps cids-sensor interval index interval

For the interval parameter, you can enter a value between 10 and 3600 seconds. The default value is 60 seconds.

Step 4 Enter a 40-hexadecimal-character security key used to verify the validity of the sensor by entering this command:

config wps cids-sensor fingerprint index sha1 fingerprint

You can get the value of the fingerprint by entering show tls fingerprint on the sensor's console.

Note Make sure to include the colons that appear between every two bytes within the key (for example, AA:BB:CC:DD).

Step 5 Enable or disable this controller's registration with an IDS sensor by entering this command:

config wps cids-sensor {**enable** | **disable**} *index*

Step 6 Enable or disable protection from DoS attacks by entering this command:

The default value is disabled.

Note A potential attacker can use specially crafted packets to mislead the IDS into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Step 7 Save your settings by entering this command:

save config

Step 8 See the IDS sensor configuration by entering one of these commands:

- **show wps cids-sensor summary**
- **show wps cids-sensor detail** index

Step 9 The second command provides more information than the first.

Step 10 See the auto-immune configuration setting by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
  Auto-Immune.................................. Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
Signature Policy
  Signature Processing........................... Enabled
```

Step 11 Obtain debug information regarding IDS sensor configuration by entering this command:

debug wps cids enable

Note If you ever want to delete or change the configuration of a sensor, you must first disable it by entering the config wps cids-sensor disable index command. To delete the sensor, enter the config wps cids-sensor delete index command.

Viewing Shunned Clients (CLI)

Procedure

Step 1 View the list of clients to be shunned by entering this command:

show wps shun-list

Step 2 Force the controller to synchronize with other controllers in the mobility group for the shun list by entering this command:

config wps shun-list re-sync

Note The controller does not take any action on shun entries when the corresponding timers have expired. The shun entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.

Intrusion Detection System Signatures

You can configure intrusion detection system (IDS) signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, appropriate mitigation is initiated.

Cisco supports 17 standard signatures. These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures.

- **Broadcast deauthentication frame signatures**—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
- **NULL probe response signatures**—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe

response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures are as follows:

- NULL probe resp 1 (precedence 2)
- NULL probe resp 2 (precedence 3)

Note Controller does not log historical NULL Probe IDS events within the Signature Events Summary output.

- **Management frame flood signatures**—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

  When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristic of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to Cisco Prime Infrastructure.

  The management frame flood signatures are as follows:

  - Assoc flood (precedence 4)
  - Auth flood (precedence 5)
  - Reassoc flood (precedence 6)
  - Broadcast probe flood (precedence 7)
  - Disassoc flood (precedence 8)
  - Deauth flood (precedence 9)
  - Reserved mgmt 7 (precedence 10)
  - Reserved mgmt F (precedence 11)

    The reserved management frame signatures 7 and F are reserved for future use.

- **Wellenreiter signature**—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.
- **EAPOL flood signature—**During an EAPOL flood attack, a hacker floods the air with EAPOL frames that contain 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.
- **NetStumbler signatures**—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached).

If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version:

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures are as follows:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

Uploading or Downloading IDS Signatures

Procedure

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a Trivial File Transfer Protocol (TFTP) server available. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

Step 3 If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.

Step 4 Choose **Commands** to open the **Download File to Controller** page.

Step 5 Perform one of the following:

- If you want to download a custom signature file to the controller, choose **Signature File** from the File Type drop-down list on the Download File to Controller page.

- If you want to upload a standard signature file from the controller, choose **Upload File** and then **Signature File** from the **File Type** drop-down list on the **Upload File from Controller** page.

Step 6 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

The SFTP option was added in Release 7.4.

Step 7 In the **IP Address** text box, enter the IP address of the **TFTP**, **FTP**, or **SFTP** server.

Step 8 If you are downloading the signature file using a TFTP server, enter the maximum number of times that the controller should attempt to download the signature file in the **Maximum retries** text box.

The range is 1 to 254 and the default value is 10.

Step 9 If you are downloading the signature file using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the signature file in the **Timeout** text box.

The range is 1 to 254 seconds and the default is 6 seconds.

Step 10 In the **File Path** text box, enter the path of the signature file to be downloaded or uploaded. The default value is "/."

Step 11 In the **File Name** text box, enter the name of the signature file to be downloaded or uploaded.

Note When uploading signatures, the controller uses the filename that you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 12 If you are using an FTP or SFTP server, follow these steps:

a. In the **Server Login Username** text box, enter the username to log into the FTP or SFTP server.

b. In the **Server Login Password** text box, enter the password to log into the FTP or SFTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP or SFTP server through which the download occurs. The default value is 21.

Step 13 Choose **Download** to download the signature file to the controller or **Upload** to upload the signature file from the controller.

Enabling or Disabling IDS Signatures

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Custom Signatures** to open the Standard Signatures page or the Custom Signatures page.

The Standard Signatures page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. This page shows the following information for each signature:

- The order, or precedence, in which the controller performs the signature checks.
- The name of the signature, which specifies the type of attack that the signature is trying to detect.
- The frame type on which the signature is looking for a security attack. The possible frame types are data and management.
- The action that the controller is directed to take when the signature detects an attack. The possible actions are None and Report.
- The state of the signature, which indicates whether the signature is enabled to detect security attacks.
- A description of the type of attack that the signature is trying to detect.

Step 2 Perform one of the following:

- If you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled, select the **Enable Check for All Standard and Custom Signatures** check box at the top of either the Standard Signatures page or the Custom Signatures page. The default value is enabled (or selected). When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.
- If you want to disable all signatures (both standard and custom) on the controller, unselect the **Enable Check for All Standard and Custom Signatures** check box. If you unselected this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

Step 3 Click **Apply** to commit your changes.

Step 4 Click the precedence number of the desired signature to enable or disable an individual signature. The **Standard Signature (or Custom Signature) > Detail** page appears.

This page shows much of the same information as the Standard Signatures and Custom Signatures pages but provides these additional details:

- The tracking method used by the access points to perform signature analysis and report the results to the controller. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.
- The pattern that is being used to detect a security attack

Step 5 In the Measurement Interval text box, enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 6 In the Signature Frequency text box, enter the number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 7 In the Signature MAC Frequency text box, enter the number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 8 In the Quiet Time text box, enter the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 9 Select the **State** check box to enable this signature to detect security attacks or unselect it to disable this signature. The default value is enabled (or selected).

Step 10 Click **Apply** to commit your changes. The Standard Signatures or Custom Signatures page reflects the signature's updated state.

Step 11 Click **Save Configuration** to save your changes.

Viewing IDS Signature Events (GUI)

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Signature Events Summary** to open the Signature Events Summary page.

Step 2 Click the Signature Type for the signature to see more information on the attacks detected by a particular signature. The Signature Events Detail page appears.

This page shows the following information:

- The MAC addresses of the clients identified as attackers
- The method used by the access point to track the attacks
- The number of matching packets per second that were identified before an attack was detected.
- The number of access points on the channel on which the attack was detected
- The day and time when the access point detected the attack

Step 3 Click the **Detail link** for that attack to see more information for a particular attack. The Signature Events Track Detail page appears.

- The MAC address of the access point that detected the attack
- The name of the access point that detected the attack
- The type of radio (802.11a or 802.11b/g) used by the access point to detect the attack
- The radio channel on which the attack was detected
- The day and time when the access point reported the attack

Configuring IDS Signatures (CLI)

Procedure

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a TFTP server available.

Step 3 Copy the custom signature file (*.sig) to the default directory on your TFTP server.

Step 4 Specify the download or upload mode by entering the **transfer** {**download** | **upload**} **mode tftp** command.

Step 5 Specify the type of file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} **datatype signature** command.

Step 6 Specify the IP address of the TFTP server by entering the **transfer** {**download** | **upload**} **serverip** *tftp-server-ip-address* command.

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 7 Specify the download or upload path by entering the **transfer** {**download** | **upload**} *path absolute-tftp-server-path-to-file* command.

Step 8 Specify the file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} *filename filename.sig* command.

Note When uploading signatures, the controller uses the filename you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 9 Enter the **transfer** {**download** | **upload**} *start* command and answer y to the prompt to confirm the current settings and start the download or upload.

Step 10 Specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval by entering this command:

config wps signature interval *signature_id interval*

where signature_id is a number used to uniquely identify a signature. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 11 Specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected by entering this command:

config wps signature frequency*signature_id frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 12 Specify the number of matching packets per interval that must be identified per client per access point before an attack is detected by entering this command:

config wps signature mac-frequency *signature_id mac_frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 13 Specify the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop by entering by entering this command:

config wps signature quiet-time *signature_id quiet_time*

The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 14 Perform one of the following:

- To enable or disable an individual IDS signature, enter this command:

  config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

- To enable or disable IDS signature processing, which enables or disables the processing of all IDS signatures, enter this command:

  config wps signature {**enable** | **disable**}

  Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Step 15 Save your changes by entering this command:

save config

Step 16 If desired, you can reset a specific signature or all signatures to default values. To do so, enter this command:

config wps signature reset {*signature_id* | *all*}

Note You can reset signatures to default values only through the controller CLI.

Viewing IDS Signature Events (CLI)

Procedure

- See whether IDS signature processing is enabled or disabled on the controller by entering this command:

  show wps summary

Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

- See individual summaries of all of the standard and custom signatures installed on the controller by entering this command:

  show wps signature summary

- See the number of attacks detected by the enabled signatures by entering this command:

  show wps signature events summary

- See more information on the attacks detected by a particular standard or custom signature by entering this command:

show wps signature events {**standard** | **custom**} **precedence# summary**

- See information on attacks that are tracked by access points on a per-signature and per-channel basis by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-signature** *source_mac*

- See information on attacks that are tracked by access points on an individual-client basis (by MAC address) by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-mac** *source_mac*

SNMP

This section contains the following subsections:

Configuring SNMP (CLI)

Note Starting from Release 8.3, SNMP over IPSec, and SNMP Traps over IPSec is supported over IPv6 interfaces.

Note To view the controller trap log, choose **Monitor** and click **View All** under "Most Recent Traps" on the controller GUI.

Procedure

- Create an SNMP community name by entering this command:

  config snmp community create *name*

- Delete an SNMP community name by entering this command:

  config snmp community delete *name*

- Configure an SNMP community name with read-only privileges by entering this command:

  config snmp community accessmode ro *name*

- Configure an SNMP community name with read-write privileges by entering this command:

  config snmp community accessmode rw *name*

- For IPv4 configuration—Configure an IPv4 address and subnet mask for an SNMP community by entering this command:

  config snmp community ipaddr *ip-address ip-mask name*

Note This command behaves like an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0.

Note The controller can use only one IP address range to manage an SNMP community.

- For IPv6 configuration—Configure an IPv6 address and prefix-length for an SNMP community by entering this command:

  config snmp community ipaddr *ipv6-address ip-mask name*
- Enable or disable a community name by entering this command:

  config snmp community mode {**enable** | **disable**}
- Enable or disable a community name by entering this command:

  config snmp community ipsec {**enable** | **disable**}
- Configure a destination for a trap by entering this command:

  config snmp trapreceiver create *name ip-address*
- Delete a trap by entering this command:

  config snmp trapreceiver delete *name*
- Change the destination for a trap by entering this command:

  config snmp trapreceiver ipaddr *old-ip-address name new-ip-address*
- Configure the trap receiver IPSec session entering this command:

  config snmp trapreceiver ipsec {**enable** | **disable**} *community-name*

  Trap receiver IPSec must be in the disabled state to change the authentication mode.
- Enable or disable the traps by entering this command:

  config snmp trapreceiver mode {**enable** | **disable**}
- Configure the name of the SNMP contact by entering this command:

  config snmp syscontact *syscontact-name*

  Enter up to 31 alphanumeric characters for the contact name.
- Configure the SNMP system location by entering this command:

  config snmp syslocation *syslocation-name*

  Enter up to 31 alphanumeric characters for the location.
- Verify that the SNMP traps and communities are correctly configured by entering these commands:

  show snmpcommunity

  show snmptrap

Note Related issue: CSCvr33858.

Read-only community does not get snmpEngineID. As per RFC 2575, the recommendation is such that, some of the OIDs are to be restricted and one of them is SnmpEngineId(engineId). For more information, see https://tools.ietf.org/html/rfc2575.

- See the enabled and disabled trap flags by entering this command:

  show trapflags

  If necessary, use the **config trapflags** command to enable or disable trap flags.

- Configure when the warning message should be displayed after the number of clients or RFID tags associated with the controller hover around the threshold level by entering this command:

  config trapflags {**client** | **rfid**} max-warning-threshold {*threshold-between-80-to-100* | **enable** | **disable**}

  The warning message is displayed at an interval of 600 seconds (10 minutes).

- Configure the SNMP engine ID by entering this command:

  config snmp engineID *engine-id-string*

- View the engine ID by entering this command:

  show snmpengineID

- Configure the SNMP version by entering this command:

  config snmp version {**v1** | **v2c** | **v3**} {**enable** | **disable**}

SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Changing the SNMP Community String Default Values (GUI)

Procedure

Step 1 Choose **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

Step 2 If “public” or “private” appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose **Remove** to delete this community.

Step 3 Click **New** to create a new community. The SNMP v1 / v2c Community > New page appears.

Step 4 In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter “public” or “private.”

Step 5 In the next two text boxes, enter the IPv4/IPv6 address and IP Mask/Prefix Length from which this device accepts SNMP packets with the associated community and the IP mask.

Step 6 Choose **Read Only** or **Read/Write** from the Access Mode drop-down list to specify the access level for this community.

Step 7 Choose **Enable** or **Disable** from the Status drop-down list to specify the status of this community.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your settings.

Step 10 Repeat this procedure if a “public” or “private” community still appears on the SNMP v1 / v2c Community page.

Changing the SNMP Community String Default Values (CLI)

Procedure

Step 1 See the current list of SNMP communities for this controller by entering this command:

show snmp community

Step 2 If "public" or "private" appears in the SNMP Community Name column, enter this command to delete this community:

config snmp community delete *name*

The *name* parameter is the community name (in this case, “public” or “private”).

Step 3 Create a new community by entering this command:

config snmp community create *name*

Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter “public” or “private.”

Step 4 For IPv4 specific configuration, enter the IPv4 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address ip_mask name*

Step 5 For IPv6 specific configuration, enter the IPv6 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address prefix_length name*

Step 6 Specify the access level for this community by entering this command, where **ro** is read-only mode and **rw** is read/write mode:

config snmp community accessmode {**ro** | **rw**} *name*

Step 7 Enable or disable this SNMP community by entering this command:

config snmp community mode {**enable** | **disable**} *name*

Step 8 Enable or disable SNMP IPSec sessions for all SNMP communities by entering this command:

config snmp community ipsec {**enable** | **disable**} *name*

By default SNMP IPSec session is disabled. SNMP IPSec session must be disabled state to change the authentication mode.

Step 9 Configure the IKE authentication methods by entering this command:

config snmp community ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret*}

- If authentication mode is configured as pre-shared-key, then enter a secret value. The secret value can either be an ASCII or a hexadecimal value. If auth-mode configured is certificate, then WLC will use the ipsecCaCert and ipsecDevCerts for SNMP over IPSEC.
- If authentication mode is configured as certificate, then controller uses the IPSEC CA and IPSEC device certificates for SNMP sessions. You need to download these certificates to the controller using the **transfer download datatype** {**ipseccacert** | **ipsecdevcert**} command.

Step 10 Save your changes by entering this command:

save config

Step 11 Repeat this procedure if you still need to change the default values for a "public" or "private" community string.

Configuring Real Time Statistics (CLI)

SNMP traps are defined for CPU and memory utilization of AP and controller. The SNMP trap is sent out when the threshold is crossed. The sampling period and statistics update interval can be configured using SNMP and CLI.

Note To get the right value for the current memory usage, you should configure either sampling interval or statistics interval.

- Configure the sampling interval by entering this command:

  config service statistics sampling-interval *seconds*
- Configure the statistics interval by entering this command:

  config service statistics statistics-interval *seconds*
- See sampling and service interval statistics by entering this command:

  show service statistics interval

SNMP Trap Enhancements

This feature provides soaking of SNMP traps and resending of traps after a threshold that you can configure called the hold time. The hold time helps in suppressing false traps being generated. The traps that are supported are for CPU and memory utilization of AP and controller. The retransmission of the trap occurs until the trap is cleared.

Procedure

- Configure the hold time after which the SNMP traps are to be resent by entering this command:

  config service alarm hold-time *seconds*

- Configure the retransmission interval of the trap by entering this command:

  config service alarm trap retransmit-interval *seconds*

- Configure debugging of the traps by entering this command:

  debug service alarm {**enable** | **disable**}

Configuring SNMP Trap Receiver (GUI)

Procedure

Step 1 Choose **Management** > **SNMP** > **Trap Receivers**.

Step 2 Click **New**.

The **SNMP Trap Receiver > New** page is displayed.

Step 3 In the **SNMP Trap Receiver Name** box, enter the SNMP trap receiver name.

Step 4 In the **IP Address (IPv4/IPv6)** box, enter the IP address of the trap receiver. Both IPv4 and IPv6 address formats are supported.

Step 5 From the **Status** drop-down list, choose to **Enable** or **Disable** the trap receiver.

Step 6 Check the **IPSec** check box if you want to enable IPSec parameters for the trap receiver.

Step 7 (Optional) If you enable the IPSec for the trap receiver, choose an **IPSec Profile Name** from the drop-down list.

Step 8 Save the configuration.

You can create a maximum of 6 such SNMP trap receivers.

Wireless Intrusion Prevention System

The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) uses an advanced approach to wireless threat detection and performance management. 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 the wired and wireless networks and use that network intelligence to analyze attacks from many sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

Cisco Adaptive wIPS is a part of the Cisco 3300 Series Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet APs. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the Cisco MSE, the wIPS can configure and monitor wIPS policies and alarms and report threats.

Note If your wIPS deployment consists of a controller, access point, and Cisco MSE, you must set all the three entities to the UTC time zone.

Cisco Adaptive wIPS is not configured on the controller. Instead, the Cisco Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the controller. The profile is stored in flash memory on the controller and sent to APs when they join the controller. When an access point disassociates and joins another controller, it receives the wIPS profile from the new controller.

Local-mode or FlexConnect mode APs with a subset of wIPS capabilities are referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in the wIPS mode if the AP is in any of the following modes:

- Monitor
- Local
- FlexConnect

The regular local mode or FlexConnect mode AP is extended with a subset of wIPS capabilities. This feature enables you to deploy your APs to provide protection without needing a separate overlay network.

wIPS ELM has the limited capability of detecting off-channel alarms. AN AP periodically goes off-channel, and monitors the nonserving channels for a short duration, and triggers alarms if any attack is detected on the channel. But off-channel alarm detection is best effort, and it takes a longer time to detect attacks and trigger alarms, which might cause the ELM AP to intermittently detect an alarm and clear it because it is not visible. APs in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the controller. The wIPS service stores and processes the alarms and generates SNMP traps. Cisco Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the Cisco MSE.

This table lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of that trap control are also enabled.

Note The controller uses only SNMPv2 for SNMP trap transmission.

Table 2: SNMP Trap Controls and Their Respective Traps

Tab Name	Trap Control	Trap
General	Link (Port) Up/Down	linkUp, linkDown
	Spanning Tree	newRoot, topologyChange, stpInstanceNewRootTrap, stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated, bsnDot11EssDeleted, bsnConfigSaved, ciscoLwappScheduledResetNotif, ciscoLwappClearResetNotif, ciscoLwappResetFailedNotif, ciscoLwappSysInvalidXmlConfig

Tab Name	Trap Control	Trap
AP	AP Register	bsnAPDisassociated, bsnAPAssociated
	AP Interface Up/Down	bsnAPIfUp, bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName, cldcClientIPAddress, cldcApMacAddress, cldcClientQuarantineVLAN, cldcClientAccessVLAN
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedIn, cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained, bsnRogueApAutoContained, bsnTrustedApHasInvalidEncryption, bsnMaxRogueCountExceeded, bsnMaxRogueCountClear, bsnApMaxRogueCountExceeded, bsnApMaxRogueCountClear, bsnTrustedApHasInvalidRadioPolicy, bsnTrustedApHasInvalidSsid, bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap

Tab Name	Trap Control	Trap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	Channel Update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR, ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

The following are the trap descriptions for the traps mentioned in the *SNMP Trap Controls and Their Respective Traps* table:

- General Traps
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users log in with the same ID.

- Rogue AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
- Config Save—Notification that is sent when the controller configuration is modified.

- Cisco AP Traps
  - AP Register—Notification sent when an access point associates or disassociates with the controller.
  - AP Interface Up/Down—Notification sent when an access point interface (802.11X) status goes up or down.

- Client-Related Traps
  - 802.11 Association—Associate notification that is sent when a client sends an association frame.
  - 802.11 Disassociation—Disassociate notification that is sent when a client sends a disassociation frame.
  - 802.11 Deauthentication—Deauthenticate notification that is sent when a client sends a deauthentication frame.
  - 802.11 Failed Authentication—Authenticate failure notification that is sent when a client sends an authentication frame with a status code other than successful.
  - 802.11 Failed Association—Associate failure notification that is sent when the client sends an association frame with a status code other than successful.
  - Exclusion—Associate failure notification that is sent when a client is exclusion listed (in a blocked list).

Note The maximum number of static blocked list entries that the APs can have is 340.

  - Authentication—Authentication notification that is sent when a client is successfully authenticated.
  - Max Clients Limit Reached—Notification that is sent when the maximum number of clients, defined in the Threshold field, are associated with the controller.
  - NAC Alert—Alert that is sent when a client joins an SNMP NAC-enabled WLAN.

    This notification is generated when a client on NAC-enabled SSIDs completes Layer2 authentication to inform the NAC appliance about the client's presence. cldcClientWlanProfileName represents the profile name of the WLAN that the 802.11 wireless client is connected to, cldcClientIPAddress represents the unique IP address of the client. cldcApMacAddress represents the MAC address of the AP to which the client is associated. cldcClientQuarantineVLAN represents the quarantine VLAN for the client. cldcClientAccessVLAN represents the access VLAN for the client.
  - Association with Stats—Associate notification that is sent with data statistics when a client is associated with the controller, or roams. Data statistics include transmitted and received bytes and packets.
  - Disassociation with Stats—Disassociate notification that is sent with data statistics when a client disassociates from the controller. Data statistics include transmitted and received bytes and packets, SSID, and session ID.

Note When you downgrade to Release 7.4 from a later release, if a trap that was not supported in Release 7.4 (for example, NAC Alert trap) is enabled before the downgrade, all traps are disabled. After the downgrade, you must enable all the traps that were enabled before the downgrade. We recommend that you disable the new traps before the downgrade so that all the other traps are not disabled.

- Security Traps
  - User Auth Failure—This trap informs that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS servers are responding to authentication requests sent by the RADIUS client.
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
  - Rouge AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

    Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Multiple Users—Two users log in with the same ID.
- SNMP Authentication
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.
- Auto RF Profile Traps
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.

- Auto RF Update Traps
  - Channel Update—Notification sent when the access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when the access point dynamic transmit power algorithm is updated.
- Mesh Traps
  - Child Excluded Parent—Notification that is sent when a defined number of failed association to the controller occurs through a parent mesh node.
  - Notification sent when a child mesh node exceeds the threshold limit of the number of discovery response timeouts. The child mesh node does not try to associate an excluded parent mesh node for the interval defined. The child mesh node remembers the excluded parent MAC address when it joins the network, and informs the controller.
  - Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers previous parent and informs the controller about the change of parent when it rejoins the network.
  - Child Moved—Notification sent when a parent mesh node loses connection with its child mesh node.
  - Excessive Parent Change—Notification sent when the child mesh node changes its parent frequently. Each mesh node keeps a count of the number of parent changes in a fixed time. If it exceeds the defined threshold, the child mesh node informs the controller.
  - Excessive Children—Notification sent when the child count exceeds for a RAP and a MAP.
  - Poor SNR—Notification sent when the child mesh node detects a lower SNR on a backhaul link. For the other trap, a notification is sent to clear a notification when the child mesh node detects an SNR on a backhaul link that is higher then the object defined by 'clMeshSNRThresholdAbate'.
  - Console Login—Notification is sent by the agent when a login on a MAP console is either successful or fail after three attempts.
  - Default Bridge Group Name—Notification sent when the MAP mesh node joins its parent using the default bridge group name.

Note The remaining traps do not have trap controls. These traps are not generated too frequently and do not require any trap control. Any other trap that is generated by the controller cannot be turned off.

Note In all of the above cases, the controller functions solely as a forwarding device.

wIPS Support for 40 and 80 MHz

Release 8.2 introduces wIPS support for 40 and 80 MHz range. This feature detects alarms in the 40 and 80 MHz range (if RRM channel scanning is selected) and provides information to the Cisco Prime Infrastructure. The channel-width information is derived from the packet data rate and sent to the wIPS module that stores

the channel width per alarm. Using the **show capwap am alarm** *alarm-id* command, you can view the channel width in which the attack has occured.

The wIPS alarm report contains the *channel-width* of the attack and device capability (11a/b/g/n/ac). No wIPS specific configuration is required to enable this feature. The only prerequisite is that RRM scanning should be enabled for this feature to work properly.

Restrictions for wIPS

- wIPS ELM is not supported on the following APs:
  - 702i
  - 702W
- Request to Send (RTS) and Clear to Send (CTS) frames are not forwarded to driver if RTS and CTS are for the BSSID of the AP.
- WIPS and Rogue Detection must be disabled on the AP in IPv6 mode to prevent it from leaking traffic outside CAPWAP towards 32.x.x.x destination.

Configuring wIPS on an Access Point (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** > **ap-name**.

Step 2 Set the **AP Mode** parameter. To configure an access point for wIPS, you must choose one of the following modes from the **AP Mode** drop-down list:

- **Local**
- **FlexConnect**
- **Monitor**

Step 3 Choose **wIPS** from the **AP Sub Mode** drop-down list.

Step 4 Save the configuration.

Configuring wIPS on an Access Point (CLI)

Procedure

Step 1 Configure an access point for the monitor mode by entering this command:

config ap mode {monitor | local | flexconnect} *Cisco_AP*

Note To configure an access point for wIPS, the access point must be in **monitor**, **local**, or **flexconnect** modes.

Step 2 Enter **Y** when you see the message that the access point will be rebooted if you want to continue.

Step 3 Save your changes by entering this command:

save config

Step 4 Disable the access point radio by entering this command:

config {802.11a | 802.11b} disable *Cisco_AP*

Step 5 Configure the wIPS submode on the access point by entering this command:

config ap mode *ap_mode* **submode wips** *Cisco_AP*

Note To disable wIPS on the access point, enter the **config ap mode** *ap_mode* **submode none** *Cisco_AP* command.

Step 6 Enable wIPS-optimized channel scanning for the access point by entering this command:

config ap monitor-mode wips-optimized *Cisco_AP*

The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose one of these options:

- **All**—All channels are supported by the access point's radio
- **Country**—Only the channels supported by the access point's country of operation
- **DCA**—Only the channel set used by the dynamic channel assignment (DCA) algorithm, which, by default, includes all of the nonoverlapping channels allowed in the access point's country of operation

The 802.11a or 802.11b Monitor Channels information in the output of the **show advanced** {**802.11a** | **802.11b**} **monitor** command shows the monitor configuration channel set:

```
Default 802.11b AP monitoring
  802.11b Monitor Mode.......................... enable
  802.11b Monitor Channels...................... Country channels
  802.11b AP Coverage Interval.................. 180 seconds
  802.11b AP Load Interval...................... 60 seconds
  802.11b AP Noise Interval..................... 180 seconds
  802.11b AP Signal Strength Interval............ 60 seconds
```

Step 7 Reenable the access point radio by entering this command:

config { **802.11a** | **802.11b**} **enable** *Cisco_AP*

Step 8 Save your changes by entering this command:

save config

Viewing wIPS Information (CLI)

Note You can also view the access point submode from the controller GUI. To do so, choose **Wireless** > **Access Points** > **All APs** > *access point name* > the **Advanced** tab. The **AP Sub Mode** field shows *wIPS* if the access point is in the monitor mode and the wIPS submode is configured on the access point, or *None* if the access point is not in the monitor mode or the access point is in the monitor mode, but the wIPS submode is not configured.

Procedure

- See the wIPS submode in the access point by entering this command:

  show ap config general *Cisco_AP*
- See the wIPS-optimized channel-scanning configuration in the access point by entering this command:

  show ap monitor-mode summary
- See the wIPS configuration forwarded by Cisco Prime Infrastructure to the controller by entering this command:

  show wps wips summary
- See the current state of the wIPS operation in the controller by entering this command:

  show wps wips statistics
- Clear the wIPS statistics in the controller by entering this command:

  clear stats wps wips

Cisco Adaptive wIPS Alarms

The controller supports five Cisco Adaptive wIPS alarms that serve as notifications for potential threats. You must enable these alarms based on your network topology using Cisco Prime Infrastructure. For more details on this, see the Cisco Prime Infrastructure User Guide.

- Device not protected by VPN—The controller generates an alarm when a wireless client and access point does not communicate over secure VPN, as all controller traffic must be routed through a VPN connection.
- WPA Dictionary Attack—The controller generates an alarm when a dictionary attack on the WPA security key occurs. The attack is detected before the initial handshake message between the client and the access point.
- WiFi Direct Session Detected—The controller generates an alarm when Wifi direct sessions of clients are detected with Wifi direct and prevents enterprise vulnerability.
- RSN Info Element Out-of-Bound Denial-of-Service—The controller generates an alarm when there are large values for RSN information element that results in an access point crash.
- DS Parameter Set DoS—The controller generates an alarm when confusion exists in the channel for the client while multiple channels overlap.