Configuring wIPS

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 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 1: Trap Controls and Descriptions

Type	Trap Control	Description
General	Config Save	Notification that is sent when the controller configuration is modified.
AP	Auth Failure	Trap sent when an AP authorization fails
	AP Interface Up/Down	Trap sent when an AP interface (A or B) comes up
	Mode Change	Trap sent when an AP mode is changed
	AP Register	Trap sent when an AP registers with a switch
	Neighbor AP Signal	Trap sent when an AP detects a neighbor AP signal

Type	Trap Control	Description
Client	802.11 Association	Associate notification that is sent when a client sends an association frame
	Enhanced 802.11 Association	Associate notification that is sent when a client sends an enhanced 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
	Enhanced 802.11 Deauthentication	Deauthenticate notification that is sent when a client sends an enhanced 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
	Enhanced Authentication	Notification that is sent when a client has successfully gone through enhanced authentication
	MaxClients Limit Reached Threshold	Notification that is sent when the maximum number of clients, defined in the **Threshold** field, is associated with the controller

Type	Trap Control	Description
	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.
	802.11 Assoc 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
	WebAuth User Login	Trap sent for web authentiction user login
	WebAuth User Logout	Trap sent for web authentiction user logout
	Neighbor Client Detection	Trap sent for neighbor client detection

Type	Trap Control	Description
AAA	User Authentication	This trap informs that a client RADIUS authentication failure has occurred
	RADIUS Servers Not Responding	This trap is to indicate that RADIUS servers are not responding to authentication requests sent by the RADIUS client
802.11 Security Traps	WEP/WPA Decrypt Error	Notification sent when the controller detects a WEP decrypting error
	IDS Signature Attack	Trap sent for IDS signature attacks
	MFP	Trap sent for management frame protection (protected management frames)
Rogues	Rogue AP	Whenever a rogue AP is detected, this trap is sent with its MAC address; when a rogue AP that was detected earlier no longer exists, this trap is sent.
Management	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.
	Multiple Users	Multiple users have logged in using the same ID
	Strong Password	Trap sent for strong password check

Type	Trap Control	Description
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

Type	Trap Control	Description
Mesh	Child Excluded Parent	Notification that is sent when a defined number of failed association to the controller occurs through a parent mesh node
	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
	Authfailure Mesh	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
	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'

Type	Trap Control	Description
	Console Login	Notification is sent by the agent when a login on a MAP console is either successful or fail after three attempts
	Excessive Association	Notification sent when cumulative association counter at parent mesh node exceeds the value configured
	Default Bridge Group Name	Notification sent when the MAP mesh node joins its parent using the default bridge group name

For more information about trap logs, see *Cisco Wireless Controller Trap Logs* at https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html.

Restrictions for wIPS

- wIPS ELM is not supported on the following APs:
  - 702i
  - 702W
  - 1130
  - 1240
- 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)

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)

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