Configuring wIPS

- Finding Feature Information, on page 1
- Information About wIPS, on page 1
- How to Configure wIPS on an Access Point, on page 8
- Monitoring wIPS Information, on page 9
- Examples: wIPS Configuration, on page 9
- Additional References for Configuring wIPS, on page 10
- Feature History for Performing wIPS Configuration, on page 10

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About wIPS

The Cisco Adaptive wireless Intrusion Prevention System (wIPS) is 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 more accurately pinpoint and proactively prevent attacks rather than waiting until damage or exposure has occurred.

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

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

The Cisco Adaptive wIPS is not configured on the controller. Instead, the 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 access points 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 access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in wIPS mode if the access point is in any of the following modes:

- Monitor
- Local

The regular local mode access point is extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

wIPS ELM has limited capability of detecting off-channel alarms. The access point periodically goes off-channel, and monitors the non-serving channels for a short duration, and triggers alarms if any attack is detected on the channel. But the off-channel alarm detection is best effort and it takes longer time to detect attacks and trigger alarms, which might cause the ELM AP intermittently detect an alarm and clear it because it is not visible. Access points 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. The Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the MSE.

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

Note The controller uses only SNMPv2 for SNMP trap transmission.

Table 1: 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
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

Tab Name	Trap Control	Trap
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
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

Tab Name	Trap Control	Trap
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 description 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 on 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 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 the client sends an association frame.
  - 802.11 Disassociation—Disassociate notification that is sent when the client sends a disassociation frame.

  - 802.11 Deauthentication—Deauthenticate notification that is sent when the client sends a deauthentication frame.
  - 802.11 Failed Authentication—Authenticate failure notification that is sent when the 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 (blacklisted).
  - 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, have 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 complete Layer2 authentication to inform about the client's presence to the NAC appliance. 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 associates with the controller or roams. The 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. The data statistics include transmitted and received bytes and packets, SSID, and session ID.

Note When you downgrade to Release 7.4 from a higher 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 is to inform that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) 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, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Multiple Users—Two users log on 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 send 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, it informs the controller.
  - Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers its previous parent and it informs the controller about the change of its 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 then child mesh node informs the controller.
  - Excessive Children—Notification sent when the child count exceeds for a RAP and 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 login on MAP console is successful or failure after three attempts.
  - Default Bridge Group Name—Notification sent when MAP mesh node joins parent using '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.

Note
To download the MIBs, click here.

How to Configure wIPS on an Access Point

Configuring wIPS on an Access Point (CLI)

SUMMARY STEPS

1. **ap name** *name* **mode** *submode wips*
2. **end**
3. **show wireless wps wips summary**
4. **show wireless wps wips statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *name* **mode** *submode wips* **Example:** `Switch# ap name ap1 mode local wips`	Configure an access point for local or monitor mode and then set the submode to wIPS.

Step 2	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 3	**show wireless wps wips summary** **Example:** `Switch# show wireless wps wips summary`	View the wIPS configuration on the access point.
Step 4	**show wireless wps wips statistics** **Example:** `Switch# show wireless wps wips statistics`	View the current state of wIPS configuration.

Configuring wIPS on an Access Point (GUI)

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page appears with a list of all access points that are associated with the switch.

Step 2 Click the name of the access point for which you want to configure wIPS.

The **AP** > **Edit** page appears.

Step 3 In the General area, 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**
- **Monitor**

Step 4 Set the **AP Sub Mode** to wIPS by choosing **wIPS** from the **AP Sub Mode** drop-down list.

Step 5 Click **Apply**.

Step 6 Click **Save**.

Monitoring wIPS Information

This section describes the new command for wIPS.

The following command can be used to monitor wIPS configured on the access point.

Table 2: Monitoring wIPS Command

Command	Purpose
show wireless wps wips summary	Displays the wIPS configuration on the access point.
show wireless wps wips statistics	Displays the current state of wIPS configuration.

Examples: wIPS Configuration

This example shows how to configure wIPS on AP1:

```
Switch# ap name ap1 mode local submode wips
Switch# end
Switch# show wireless wps wips summary
```

Additional References for Configuring wIPS

Related Documents

Related Topic	Document Title
wIPS commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for Performing wIPS Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.