



# **Cisco Wireless and Network IDS/IPS Integration**

A secure Cisco Unified Network, featuring both wired and wireless access, requires an integrated, defense-in-depth approach to security, including cross-network threat detection and mitigation that is critical to effective and consistent policy enforcement. Wireless and network IDS/IPS are both critical elements of network security, performing complementary roles in threat detection and mitigation.

This chapter outlines these complementary roles of wireless and network Intrusion Detection System/Intrusion Prevention System (IDS/IPS), along with how they are fulfilled by the Cisco WLAN Controller (WLC) and Cisco IPS platforms respectively. This chapter also presents how, by enabling collaboration between these two Cisco platforms, they can be used to provide a simple, but effective, automated threat mitigation tool.

Guidelines for deploying and integrating Cisco IPS with a Cisco Unified Wireless Network are provided, along with how to enable WLC and IPS collaboration for automated threat mitigation.

Software implementation, screenshots, and behavior referenced in this chapter are based on the releases listed in Test Bed Hardware and Software, page 8-50. It is assumed that the reader is already familiar with both the Cisco Unified Wireless Network and Cisco IPS.



This chapter addresses only IDS/IPS integration features specific to the Cisco WLC and Cisco IPS platforms.

# **Roles of Wireless and Network IDS/IPS in WLAN Security**

Cisco IPS are network-based platforms designed to accurately identify, classify, and stop malicious traffic, including worms, spyware, ad ware, network viruses, application abuse, and policy violations. This is achieved through detailed traffic inspection at Layers 2 through 7.

The wireless IDS/IPS features of the Cisco WLC and the network IDS/IPS features of the Cisco IPS platforms are key elements of an integrated, defense-in-depth approach to WLAN security, performing complementary and collaborative roles in threat detection and mitigation on a WLAN.

## **Complementary Roles of Wireless and Network IDS/IPS**

The complementary roles of wireless and network IDS/IPS enable the same principles and policies of threat detection and mitigation employed on a wired network to be extended to a WLAN.

Wireless and network IDS/IPS are complementary in the following ways:

- Wireless IDS/IPS is critical to the monitoring, detection, and mitigation of threats and anomalies specific to the 802.11 RF medium.
- Network IDS/IPS is key to the monitoring, detection, and mitigation of general threats and anomalies in client traffic, as well as the protection of network infrastructure devices and services (see Figure 8-1).

Figure 8-1 Wireless and Network IDS/IPS for WLAN Threat Detection and Mitigation



A summary of the key complementary roles and features of the Cisco WLC and Cisco IPS in WLAN threat detection and mitigation is presented in Table 8-1.

IDS/IPS Element	WLAN Threat	WLAN Threat Detection and Mitigation Feature		
Wireless IDS/IPS features of WLC <sup>1</sup>	Rogue AP	Detection, location, and containment, including traceback on the wired network		
	Rogue client	Detection and containment		
	Wireless ad-hoc network	Detection and containment		
	802.11 DoS	802.11 DoS attack signatures <sup>2</sup>		
		Cisco Management Frame Protection <sup>3</sup>		
	802.11 attack tools	802.11 reconnaissance signatures <sup>2</sup>		
	Excessive 802.11 associations and authentications	Detection, tracking and containment through clien exclusion settings		
	IP theft and re-use	Detection and containment		
	RF interference	Dynamic radio resource management		
Network IDS/IPS features of Cisco IPS platform	Malicious WLAN client traffic For example, worms, viruses, application abuse, spyware, adware, and so on, as well as policy violations <sup>4</sup>	Signature-based detection, identification and classification of malicious traffic Range of response actions available including alert, SNMP trap, packet drop, connection block, and host block		

Table 8-1 WLAN Threat Detection and Mitigation Roles

1. Wireless IDS/IPS features are provided by the Cisco WLC. The adaptive wireless IPS features of the Cisco Mobility Services Engine (MSE) are not addressed in this guide.

2. The WLC and WCS include standard signatures but also support custom signatures that can be developed to extend their threat detection capabilities.

 Cisco Management Frame Protection is a unique feature that provides signature-based management frame authentication that can be used to address 802.11-based DoS attacks but also enables easy identification of a rogue AP. For more information on Management Frame Protection, refer to Management Frame Protection, page 4-16.

4. A Cisco IPS platform deployed in a WLAN environment performs the same monitoring, detection, and mitigation of malicious traffic for WLAN clients as it does for wired clients, and the same policies are generally applied.

Wireless IDS/IPS features are addressed in more detail in Cisco Unified Wireless Network Architecture— Base Security Features, page 4-1 and Wireless IDS, page 4-9.

For more information on Cisco IPS refer to Reference Documents, page 8-51.

## **Collaborative Role of Cisco WLC and Cisco IPS**

Collaboration of the Cisco WLC and Cisco IPS provides a simple, but effective, automated threat mitigation tool that offers centralized control with local enforcement, right on the access edge. This collaboration requires no additional hardware and very simple configuration, using the deployment of these two platforms to further enhance their value in threat detection and mitigation (see Figure 8-2).





The Cisco IPS monitors client traffic and, upon identifying threats and anomalies, triggers a client disconnect through creation of a host block. For a WLAN client, this mitigation action is automatically enforced by the WLC through collaboration with the Cisco IPS. The client is removed from the network at the access edge and denied re-entry until the host block is either removed or times out. Cisco WLC and Cisco IPS collaboration thus offers operational staff an additional automated threat mitigation tool that can be employed when anomalous behavior is detected.

# How Cisco WLC and IPS Collaboration Works

Collaboration between a Cisco WLC and Cisco IPS provides an automated threat mitigation tool, enabling host block activation on an IPS to be enforced directly on the WLAN. This collaboration involves the following key operational elements:

- Cisco WLC and IPS synchronization
- WLC enforcement of a Cisco IPS host block
- Cisco IPS host block retraction

# **Cisco WLC and IPS Synchronization**

A Cisco WLC and IPS synchronize active host block information by the WLC periodically polling the IPS with a shun list request. The Cisco IPS responds with the active host block list (see Figure 8-3).



Figure 8-3 Cisco WLC and IPS Synchronization

Note the following:

- Communication between a Cisco WLC and a IPS is through HTTPS using Transport Layer Security (TLS) 1.0. This ensures that identification of the IPS is authenticated using X.509 certificates and that data is encrypted using the SHA-1 hashing algorithm.
- Only one WLC in a mobility group is required to collaborate with an IPS. Active host block information is automatically passed to all WLCs within a mobility group. For redundancy purposes, multiple WLCs within a mobility group can, however, be configured to collaborate with the same IPS.
- A WLC can collaborate with multiple IPS devices.

## WLC Enforcement of a Cisco IPS Host Block

Automated threat mitigation is provided through collaboration of a Cisco WLC and IPS, enabling a Cisco IPS host block to be passed to and, in the case of a matching WLAN client, enforced by the Cisco WLC.

When anomalous activity in client traffic is detected by an IPS, subsequent investigation may result in a decision to block the client generating these anomalies. This can be initiated on a Cisco IPS and enforced, either directly on the IPS, or through collaboration with another network device, such as a WLC. Enforcement on the Cisco IPS is done through a deny action and enforcement on another network device is activated through a block action.

For more information on the Cisco IPS deny and block actions, refer to Cisco IPS Block versus Deny Actions, page 8-49.



Note

It is critical to ensure that a threat is accurately identified, classified, and traced before action is taken. In addition, ensure that anomalous behavior is not an attempt to perform DoS on a host.

To enable enforcement of a host block on another network device, including a WLC, a host block can be activated on a Cisco IPS by one of the following methods:

- Manual host block creation
- Automatic enforcement through association of a "Request Block Host" action with a signature
- Automatic enforcement through association of a "Request Block Host" action with an event action override based on a certain risk rating (RR) threshold



In accordance with general IPS design guidelines, automatic enforcement of blocking actions should be used with caution. For documents with guidance on IPS deployment and tuning, refer to Reference Documents, page 8-51.

The WLC receives the IPS host block information upon its next poll of the IPS for the shun list. If a WLAN client that matches the host block information is associated with the WLC, the WLC enforces this host block by creating a WLAN client exclusion for that host. The WLAN client is disconnected from the WLAN and blocked from reconnecting as long as the host block action is active.

WLC enforcement of a Cisco IPS host block for a WLAN client is shown in Figure 8-4.



Figure 8-4 WLC Enforcement of a Cisco IPS Host Block

The following are the WLC enforcement steps for a Cisco IPS host block:

- **Step 1** A host block is initiated on a Cisco IPS, defining the source IP address of the client to be blocked.
- **Step 2** The WLC, upon its next poll of the IPS with a shun list request, receives an updated active host block list.
- **Step 3** The WLC updates its shunned client list to reflect the latest IPS active host block information.
- **Step 4** The WLC checks if a client, with a source IP address matching an entry in the shunned client list, is currently associated.
- Step 5 If a WLAN client with a source IP address matching a shunned client is associated, the WLC creates a client exclusion, based on the client's MAC address, to enforce the IPS host block action.
- **Step 6** The blocked WLAN client is disconnected.
- **Step 7** Each time a WLAN client with an excluded MAC address attempts to associate, it is disconnected by the WLC for as long as an IPS host block is in place.
- **Step 8** A host block is active on an IPS until either it expires or it is removed.

- Step 9 A client exclusion is active on a WLC until the client exclusion timeout expires. The client exclusion timeout is defined per WLAN profile on the WLC and is independent of the host block timeout defined on the IPS.
- **Step 10** If the client exclusion expires on the WLC but the host block is still active on the IPS, the WLC creates a new client exclusion if a client with a blocked source IP address is associated or attempting to associate with the WLC.

## **Cisco IPS Host Block Retraction**

Retraction of a Cisco IPS host block occurs based on one of the following events:

- Timeout of a host block
- Manual deletion of a host block

When a Cisco IPS host block is retracted, the WLC receives the updated active host block list on its next poll of the IPS and updates its shunned client list.

The steps performed by a WLC upon retraction of a Cisco IPS host block for a WLAN client are outlined below:

- Step 1The Cisco IPS active host block information is updated to no longer include the source IP address of the<br/>previously-blocked host.
- Step 2 The WLC, upon its next poll of the IPS with a shun list request, receives an updated active host block list.
- **Step 3** The WLC updates its shunned client list to reflect the latest IPS active host block information, removing any hosts no longer being blocked.
- **Step 4** An active WLC client exclusion associated with a previously blocked host will time out based on the client exclusion timeout value for the WLAN profile on which the client connected.
- **Step 5** Upon the client exclusion timeout expiring, a previously blocked host is no longer blocked.

# **Cisco Unified Wireless and IPS Integration**

This section outlines the steps required to integrate a Cisco IPS with a Cisco Unified Wireless Network, along with how to provide a simple, but effective, automated threat mitigation tool by enabling collaboration between a Cisco WLC and a Cisco IPS. This collaboration requires no additional hardware and very simple configuration.

The configuration of a Cisco IPS is illustrated using Cisco IDS Device Manager (IDM). The configuration of the Cisco WLC is illustrated using the GUI of the WLC.

# **IPS Deployment and Integration**

On a Cisco Unified Wireless Network, all WLAN client traffic enters the corporate network through the WLC. This provides the ideal location to perform threat detection and mitigation on this traffic, and a simple integration point for a Cisco IPS. (See Figure 8-5.)





A Cisco IPS can be deployed either as an IDS, employing promiscuous mode passive monitoring, or as an IPS, employing inline mode active monitoring. For the purposes of collaboration with a Cisco WLC, a Cisco IPS can be deployed in either IDS or IPS mode. Enforcement of a host block is done by the WLC, not the IPS; therefore, the sensor is not required to be inline. Consequently, the choice of IPS deployment mode is a general network design choice.

For more information on IPS deployment modes refer to Cisco IPS Deployment Modes, page 8-49.

Note the following:

- The Cisco IPS is performing the same monitoring and anomaly detection on WLAN client traffic as it performs on wired client traffic.
- The specific interfaces, sub-interfaces, and VLANs that a Cisco IPS is deployed to monitor are configurable. Consequently, an IPS can be deployed to monitor all or a subset of the WLC wireless VLANs.
- An IPS does not need to be dedicated to WLAN traffic monitoring. It can be deployed to monitor both wired and wireless traffic.

Detailed IPS design guidance can be found in the documents listed in Reference Documents, page 8-51.

## **Enabling Cisco WLC and Cisco IPS Collaboration**

Collaboration between a Cisco WLC and a Cisco IPS requires completion of the following simple steps:

- Create a user account on Cisco IPS for the WLC
- Define the WLC as an allowed host on the Cisco IPS
- Define the Cisco IPS as a CIDS sensor on the Cisco WLC
- Enable client exclusion in the WLAN profile

Detailed instructions on how to implement each step are outlined below.

The first step in enabling Cisco WLC and Cisco IPS collaboration is to enable the WLC to retrieve active host block information from the IPS.

**Step 1** On the Cisco IPS, create a user account for the WLC.

This enables the WLC to obtain the active host block information from the IPS.

On the IDM, go to **Configuration** -> **Sensor Setup** -> **Users**. Add a new user with the user role **Viewer** and configure a password. (See Figure 8-6.)

Figure 8-6 Create a User Account on Cisco IPS for a WLC

🔀 Cisco IDM 6.1 - 10.20.200.30					- 🗆 ×
File View Help	itoring 🔇 Back 🕥 Forward 🤇	Refresh 🤗 Help			cisco
Sensor Setup 🗇 🕂 ×	Configuration > Sensor Setup > Us Specify the users that have access to allowed.	eers o the sensor. The service role is a special role t	that allows you to bypass the	CLI if needed. Only one	service account is
- 🕑 Time	Username	Role		Status	Add
Users	cisco	Viewer	Active		
	csmars	Viewer	Active		Edit
	User User F	d User name: wic-206-br Role: Viewer  Sessword  Password:  T********  Confirm Password:  Cancel Help	× Active		Delete
Sensor Setup       Interfaces       Policies       Sensor Management		Apply	Reset		
IDM is initialized successfully.				tme-mob adm	ninistrator

Note the following:

- It is recommended that an individual user account is created for each WLC. This facilitates troubleshooting and monitoring.
- A WLC should only be granted view access, as provided by the user role "Viewer". This is all that is required and ensures that only minimum necessary access privileges are granted, as recommended as a security best practice.
- Ensure that a strong password policy is enforced.
- Only one WLC in a mobility group is required to collaborate with an IPS, though multiple WLCs can be configured for redundancy purposes.
- **Step 2** On the Cisco IPS, define the WLC as an allowed host. This allows the WLC host to communicate with the IPS in order to retrieve the active host block list.

On IDM v6.1, go to **Configuration -> Allowed Hosts/Networks**. Add an allowed host with the WLC source IP address and network mask. (See Figure 8-7.)

🔀 Cisco IDM 6.1 - 10.20.200.30				- 🗆 🗙
File View Help	nitoring 💽 Back 💽 Forward 🔍 🚱 Refi	resh 🢡 Help		cisco
Sensor Setup	Configuration > Sensor Setup > Allowed	I Hosts/Networks rks that have permission to access the sensor	sturnet the estimat	
Allowed Hosts/Networks	IP Address	ns that have permission to access the sensor	Network Mask	
-O Time	10.20.30.0	255.255.255.0	Network Mask	Add
- 🕼 Users	10.20.30.34	255,255,255,255		Edit
	10.20.100.150	255.255.255.255		Delete
Sensor Setup         Interfaces         Interfaces <tr< th=""><th>Add Allowed Ho     IP Address:     Network Mask:     OK</th><th>st 10.20.201.2 255.255.255  Cancel Help</th><th>×</th><th></th></tr<>	Add Allowed Ho     IP Address:     Network Mask:     OK	st 10.20.201.2 255.255.255  Cancel Help	×	
×		Apply Res	et	
Refresh completed successfully.			tme-mob	administrator 🔒

Figure 8-7 Define the WLC as an Allowed Host on Cisco IPS

Note the following:

• An individual host IP address or a network IP address range can be defined by using the appropriate network mask. This is typically dictated by the corporate network security policy and is generally a trade-off between ease of management and security risk.

**Step 3** Obtain the TLS fingerprint of the Cisco IPS.

The TLS fingerprint is the server-side X.509 certificate of the IPS. This fingerprint is used in TLS 1.0 to authenticate the server and to secure communication between the WLC and the IPS. On the IDM, go to **Configuration -> Sensor Setup -> Certificates -> Server Certificate**. (See Figure 8-8.)

Figure 8-8 Sample TLS Fingerprint of a Cisco IPS



The TLS fingerprint may also be retrieved on the CLI of a Cisco IPS by entering the following command:

#### show tls fingerprint

A sample TLS fingerprint is as follows:

```
ips-3845-2# show tls fingerprint
MD5: 16:A9:7A:E9:12:38:7A:76:68:EA:F0:47:C8:63:4F:60
SHA1: 5D:F9:29:43:CB:15:EC:60:1B:07:C1:8A:6A:76:20:14:B9:6E:92:AA
```

**Step 4** On each WLC that collaborates with the Cisco IPS, define the IPS as a CIDS sensor.

On the WLC, go to **Security** -> **CIDS** -> **Sensors**. Add a new CIDS sensor with the IP address of the IPS. Enter the username and password of the WLC user account created on the IPS, as completed in Step 1. Check the **State** box to activate the sensor, enter the TLS fingerprint of the IPS and select the **Apply** button. (See Figure 8-9.)

						Sa <u>v</u> e	Configuration	<u>P</u> ing	Logout   <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>V</u>	<u>N</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
Security	CIDS Sens	or Add					< Bac	k	Apply
▼ AAA General ▼ RADIUS	Index	3 💌							
Authentication Accounting Fallback	Server Address	10.20.	200.30						
► TACACS+ LDAP	Port	443							
Local Net Users MAC Filtering Disabled Clients	Username	wic-21	106-br						
User Login Policies AP Policies	Password	****	****						
Local EAP	Confirm Password	****	****						
<ul> <li>Priority Order</li> <li>Access Control Lists</li> </ul>	Query Interval	60	seconds						
Wireless Protection Policies	State								
Web Auth  Advanced  CIDS Sensors Shunned Clients  IPSec Certs	Fingerprint (SHA1 hash)		29:43:CB:15:EC: chars with ev						
CA Certificate ID Certificate									

#### Figure 8-9 Define the IPS as a CIDS Sensor on the WLC

Note the following:

- The query interval determines how frequently the WLC polls the IPS with a shun list request.
- The default query interval is 60 seconds.
- The query interval influences the time between an active host block being activated on a Cisco IPS and enforced on the WLC. The query interval, along with the client exclusion timeout, also influences the time between an active host block being retracted on a Cisco IPS and the block being lifted on the WLC.
- Only one WLC in a mobility group is required to collaborate with an IPS. Active host block information is automatically passed to all WLCs within a mobility group. For redundancy purposes, multiple WLCs within a mobility group can be configured to collaborate with a Cisco IPS.
- A WLC can collaborate with multiple IPS devices.
- IPS deployments often feature multiple sensors, for scale and high availability, as well as to address different logical and geographical locations. A WLC can collaborate with multiple IPS devices in order to fully leverage this network-wide threat detection and mitigation capability.
- **Step 5** For each WLAN on which WLAN client blocking enforcement is to be supported, client exclusion must be enabled in the WLAN profile.

On the WLC, go to **WLANs** to access the WLAN profiles. Select the particular WLAN profile on which client blocking is to be enabled and go to the **Advanced** tab. Next to **Client Exclusion**, ensure that the **Enabled** checkbox is checked. (See Figure 8-10.)

ANs	WLANs > Edit < Back Apply
VLANs	General Security QoS Advanced
VLANs dvanced	Allow AAA Override 🗹 Enabled DHCP
	H-REAP Local Switching <sup>3</sup> Enabled DHCP Server Override
	Enable Session Timeout 😿 1800 Session Timeout (secs) DHCP Addr. Assignment 🗹 Required
	Aironet IE Enabled Management Frame Protection (MFP)
	Diagnostic Channel Enabled Infrastructure MFP 🔽 Override Interface ACL None 💌 Protection (Global MFP Disabled)
	P2P Blocking Action Disabled MFP Client Protection 5 Optional -
	Client Exclusion <sup>£</sup> Enabled 60 Timeout Value (secs) DTIM Period (in beacon intervals)
	802.11a/n (1 - 255) 1
	802.11b/g/n (1 - 255) 1
	Foot Notes
	1 CKIP is not supported by 10xx model APs

#### Figure 8-10 Enable Client Exclusion on each WLAN to Support WLAN Client Blocking Enforcement

Note the following:

- Client exclusion must be enabled on each WLAN profile that is required to support WLAN client blocking.
- If client exclusion is not enabled on a particular WLAN profile, the WLC receives active host block information from the IPS but a host block is not enforced on that WLAN profile.
- When client exclusion is enabled on a WLAN profile, a timeout value must be defined. This timeout is specific to that WLAN profile and applied by the WLC to all client exclusions enforced on that WLAN profile.
- The default client exclusion timeout is 60 seconds.
- Upon a client exclusion being created, the client exclusion timeout determines the time period that a client is blocked by the WLC, based on their MAC address.
- A client exclusion created as a result of a Cisco IPS host block remains active until the client exclusion timeout expires. It is not removed upon retraction of a Cisco IPS host block.

# **Enabling Cisco WLC and IPS Collaboration Monitoring**

Monitoring of network activity is critical to effective network management. This chapter provides details on how to enable monitoring of Cisco WLC and IPS collaboration through:

- WLC local logging
- SNMP traps
- WCS
- CS-MARS

## **Enabling WLC Local Logging of WLAN Client Block Events**

The WLC offers a local message log that can be accessed either through the WLC GUI or on the WLC CLI. The logging of WLAN client block events to this message log requires the WLC log level to be set to a minimum security level of 1, which equates to **Alerts**. A WLC will then generate a local message log entry upon a WLAN client being blocked as a result of an IPS host block, including the IP address received from the IPS and the associated client's MAC address.

If visibility is required into a WLC denying client association due to a client exclusion, the WLC log level must be set to a minimum severity level of 4, which equates to **Warnings**. This entry is generated with a WLAN client block event upon a blocked client subsequently attempting to associate while an active client exclusion exists for its MAC address.

The logging levels required for the different logging options are summarized in Table 8-2.

Event	Minimum Severity Level				
WLC client shun event as a result of an IPS host block being enforced	Alerts	Severity level 1			
Client denied association request due to an active client exclusion	Warnings	Severity level 4			

#### Table 8-2 Logging Levels Required



# The severity log level "Warnings" generates a significant number of events. This log level should be used with caution.

The default buffered and console log level is **Critical**, with a severity level of 2. This default setting will log WLAN client block events enforced as a result of a Cisco IPS host block.

The parameters to define the log level are:

• Buffered Log Level

Defines the log level for the WLC GUI Message log

Console Log Level

Defines the log level for the WLC CLI log

In previous releases of the WLC, the parameter *Message Log Level* defines the log level for both the GUI and the CLI. The setting **Significant System** events enables logging of WLAN client block events.

The following steps describe how to configure the log levels to obtain visibility into WLAN client block events:

**Step 1** Ensure that the *Buffered Log Level* and the *Console Log Level* parameters are set to a severity level 1. The example shown here sets the log level to **Critical** which is a level 2 setting.

On the WLC, go to **Management** -> **Logs** -> **Config**. Set the log level to **Critical** for both the buffered and the console parameters. Enforce any changes by clicking **Apply**. (See Figure 8-11.)

Figure 8-11 WLC Local Logging Level to include WLAN Client Block Events

and in the second					– Sa <u>v</u>	e Configuration	Ping   Logout	<u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Management Summary SNMP HTTP Telnet-SSH Serial Port Local Management Users User Sessions Logs Config Message logs Mgmt Via Wireless Fach Support	Syslog C Syslog Set Syslog Set Syslog Le Syslog Fo Msg Log Buffered I Console L File Info Proc Info Trace Info	erver IP Ad rver evel configu Log Level	ldress Criti Loca		Add	Apply		

### **Enabling SNMP Traps for WLAN Client Block Events**

Enforcement of an IPS host block is enforced by a WLC through automatic creation of a client exclusion. Consequently, in order to generate an SNMP trap upon this event occurring, SNMP traps for client exclusion must be enabled on the WLC.

**Step 1** Ensure that the general WLC parameters are properly defined.

On the WLC, go to **Management** -> **SNMP** -> **General**. Ensure, at a minimum, that the system name and the correct trap port number are defined, and disable any SNMP versions not required. (See Figure 8-12.)

			-		Sa <u>v</u> e Configuration	<u>Ping   Loc</u>	lout   <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Management	SNMP System Sun	nmary					Apply
Summary	Name	wlc-2106-br					
<ul> <li>SNMP</li> <li>General</li> <li>SNMP V3 Users</li> </ul>	Location	SW-Branch					
Communities Trap Receivers Trap Controls	Contact						
Trap Logs	System Description	I Cisco Controlle	er				
HTTP Telnet-SSH	System Object ID	1.3.6.1.4.1.9.1	.828				
Serial Port Local Management	SNMP Port Number	161					
User Sessions	Trap Port Number	162					
Logs Mgmt Via Wireless	SNMP v1 Mode	Disable 💌					
Tech Support	SNMP v2c Mode	Disable 💌					
	SNMP v3 Mode	Enable 💌					

#### Figure 8-12 Verify the General SNMP Parameters on the WLC

Note the following:

- SNMP v1 and SNMP v2c pass all data in clear text, including the community strings, and are thus vulnerable to sniffing.
- If SNMP v1 or v2c are not required, they should be disabled.
- SNMP v3 offers the most secure implementation of SNMP and is recommended where supported.
- If SNMP v1 or v2c are required, ensure that non-default SNMP community strings are used.
- Remove default public and private community definitions.
- If SNMP v1 or v2c are required, only read-only access should be authorized.
- If SNMP v1 or v2c are required, access should be restricted to authorized management platforms through the use of ACLs.

For more information on securing SNMP access, refer to the Network Security Baseline (see Reference Documents, page 8-51).

**Step 2** Enable WLC SNMP traps for client exclusion.

On the WLC, go to **Management** -> **SNMP** -> **Trap Controls**. Under **Client Related Traps**, ensure that the **Exclusion** checkbox is checked. (See Figure 8-13.)



#### Figure 8-13 Enable SNMP Traps for Client Exclusion on the WLC

### Enabling WCS Cross-WLC Monitoring of WLAN Events

WCS offers a consolidated view of cross-WLC events that is invaluable for visibility into activity across the entire Unified Wireless Network. The WCS leverages SNMP traps sent by each WLC to generate these consolidated views. Consequently, each WLC must be configured to send SNMP traps to the WCS.

Enabling WCS monitoring of cross-WLC events requires the following key elements:

- On each WLC:
  - Verify the general SNMP parameters
  - Verify the SNMP trap controls
  - Define the WCS as an SNMP v3 user
  - Define the WCS as an SNMP trap receiver
- On the WCS:
  - Define each WLC along with its SNMP parameters

Detailed instructions on how to configure each of these elements are outlined below. WCS supports SNMP v3; therefore, the configuration is shown for SNMP v3. SNMP v1 and v2c are supported, but SNMP v3 is the most secure implementation of SNMP and is recommended where supported.

Step 1 On each WLC, verify that the general SNMP parameters are correctly defined.

On the WLC, go to **Management** -> **SNMP** -> **General** (see Figure 8-14). For details, refer to Enabling SNMP Traps for WLAN Client Block Events, page 8-16.

a di						Sa <u>v</u> e Configuration	n   <u>P</u> ing   Log	out   <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Management	SNMP Sy	stem Su	mmary					Apply
Summary	Name		wlc-2106-br					
SNMP General SNMP V3 Users	Location		SW-Branch					
Communities Trap Receivers Trap Controls	Contact							
Trap Logs	System D	escriptio	n Cisco Control	ler				
HTTP Telnet-SSH	System O	bject ID	1.3.6.1.4.1.9.	1.828				
Serial Port Local Management	SNMP Port	t Numbei	161					
User Sessions	Trap Port	Number	162					
▶ Logs	SNMP v1	Mode	Disable 💌					
Mgmt Via Wireless Tech Support	SNMP v2c	Mode	Disable 💌					
	SNMP v3 M	Mode	Enable 💌					

#### Figure 8-14 Verify the General SNMP Parameters on the WLC

This example leverages the SNMP v3 support of WCS; therefore, SNMP v3 mode must be enabled.

**Step 2** On each WLC, verify that all the desired SNMP trap controls are enabled.

On the WLC, go to **Management -> SNMP -> Trap Controls** (see Figure 8-15). For an SNMP trap to be generated upon a WLAN client host block event, ensure traps are enabled for exclusion. For details, refer to Enabling SNMP Traps for WLAN Client Block Events, page 8-16.



#### Figure 8-15 Verify the SNMP Trap Controls on the WLC

**Step 3** On each WLC, define the WCS as an SNMP v3 user.

On the WLC, go to **Management** -> **SNMP** -> **SNMP V3 Users**. Select **New** and define a user profile name for the WCS. Set the access mode drop-down box to **Read Write** if the WCS is to be granted the ability to modify the WLC configuration. Define the authentication and privacy passwords then click **Apply**. (See Figure 8-16.)



Figure 8-16 Define the WCS as an SNMPv3 User on the WLC

Note the following:

- If the WCS is not required to configure the WLC, the access mode should be set to read-only.
- The default authentication and privacy protocols are the most secure and recommended settings.
- The authentication and privacy passwords must be at least 12 characters long.
- **Step 4** On each WLC, define the WCS as an SNMP trap receiver.

On the WLC, go to **Management** -> **SNMP** -> **Trap Receivers**. Select **New** and define a name for the WCS, along with its IP address . Set the status drop-down box to **Enable** and click **Apply**. (See Figure 8-17.)

					Sa <u>v</u>	e Configuration	<u>P</u> ing   Lo <u>q</u> out	<u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Management	SNMP Tra	ap Rece	iver > New			< Bac	k App	ly
Summary	Trap Recei	iver Nan	ne wcs					
<ul> <li>SNMP</li> <li>General</li> <li>SNMP V3 Users</li> </ul>	IP Address	5	10.20.30.14					
Communities Trap Receivers Trap Controls Trap Logs	Status		Enable 💌					
НТТР								
Telnet-SSH								
Serial Port								
Local Management Users								
User Sessions								
▶ Logs								
Mgmt Via Wireless								
Tech Support								

Figure 8-17 Define the WCS as an SNMP Trap Receiver on each WLC

**Step 5** On the WCS, define each WLC and its SNMP parameters.

On the WLC, go to **Configure** -> **Controllers**. Either add a controller if it does not exist or click on a controller already defined to modify the SNMP parameters. See Figure 8-18.

ahaha	Wireless Control System Username: tme-mob   Logout   Refresh   Print View
CISCO	🚡 Monitor 🔻 Reports 👻 Configure 👻 Location 👻 Administration 👻 Tools 👻 Help 👻
Quick Search	Add Controllers
<ip, go<="" name,ssi="" th=""><td>Add Format Type Device Info</td></ip,>	Add Format Type Device Info
Search Controllers	IP Addresses 10.20.201.2 (comma-separated IP Addresses)
New Search	Network Mask 255,255,255.0
Saved Searches Edit	SNMP Parameters*
	Version v3
	Retries 3
	Timeout (seconds) 4
	User Name wcs
	Auth. Type HMAC-SHA
	Auth. Password *****
	Privacy Type CFB-AES-128
	Privacy Password ******
	OK Cancel
Alarm Summary <section-header></section-header>	* Please enter SNMP parameters for the write access if you
Malicious AP 0 0 0	have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify
Unclassified AP 0 0 <u>42</u>	configuration
Coverage Hole 0 0 0 Security 5 0 13	
Security <u>5</u> 0 <u>13</u> Controllers <u>727</u>	
Access Points <u>3</u> 00	
Location 0 0	
Mesh Links 0 0 0 WCS 0 0 0	
wcs <u>o o o</u>	

#### Figure 8-18 Define each WLC and its SNMP Parameters on the WCS

Click OK and the WCS will attempt to discover the WLC and retrieve its properties.

Note the following:

• The SNMP parameters must match those defined on the WLC in the SNMP v3 user profile for the WCS.

### **Enabling CS-MARS Monitoring of WLAN Events**

CS-MARS provides cross-network anomaly detection and correlation that is critical to effective threat detection and mitigation. This visibility can be extended to include the WLAN by integrating CS-MARS with a Cisco Unified Wireless Network. For detailed information, refer to Chapter 9, "CS-MARS Integration for Cisco Unified Wireless."

# **Cisco IPS Host Block Activation and WLC Enforcement**

This section illustrates a WLAN client block being activated through a manual host block on a Cisco IPS and automatically enforced on the WLC through a client exclusion. The key steps involved are illustrated in Figure 8-19.



#### Figure 8-19 Cisco IPS Host Block Activation and WLC Enforcement

Before attempting a WLAN client block, verify that the WLC is able to successfully poll the Cisco IPS and receive a response to its shun list request. For details, refer to Verifying Cisco WLC and IPS Communication Status, page 8-29.

**Step 1** On the IPS, add a host block.

On IDM, go to **Monitoring** -> **Time-Based Actions** -> **Host Blocks**. Add a new host block with the source IP address of the WLAN client to be blocked and define the timeout. Click **Apply**. (See Figure 8-20.)

Cisco IDM 6.1 - 10.20.200.30			<u>- 🗆 ×</u>
File View Help	toring 📀 Back 💽 Forward 🗨 Refresh 🦻 Help		cisco
Sensor Monitoring A × Events Events Denied Attackers Denied At	Monitoring > Sensor Monitoring > Time-Based Actions > Host Blocks         Specify the address to block and the duration for that block.         Source IP       Destination IP         Destination IP       Destination Port         Protocol       Minutes         Timeout       (ninutes)         VLAN       Source IP:         I0.20.203.66       0         ID       0         ID       Enable connection blocking         Connection Blocking       Destination Pr:         Destination Pr:       Destination Pr:         VLAN (optional):       Protocol (optional):         VLAN (optional):       VLAN (optional):         VLAN (optional):       Immout         Timeout:       50         No Timeout       Timeout	Connection Block Enabled False	Add Delete
Sensor Monitoring	Apply Cancel Help		
×	Refresh		itor
IDM is initialized successfully.		tme-mob administra	itor 📔 🔂

Figure 8-20 Initiating a Client Block on a Cisco IPS

Note the following:

• The default active host block timeout is 60 minutes.

A blocked client subsequently appears in the list of host blocks on that particular IPS. (See Figure 8-21.)

🎼 Cisco IDM 6.1 - 10.20.200.30									- 🗆 ×
File View Help									abab
🚮 Home 🖓 Configuration 🔯 Mon	itoring 🕜 Back	Forward	💽 Refresh 🢡	Help					cisco
Sensor Monitoring 🗇 🗜 🗙	Monitoring > Ser	nsor Monitorin	g > Time-Based A	ctions > Host B	locks				
Events	Specify the addr	ess to block and	the duration for tha	it block.					
E									
Host Blocks	Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enabled	Add
	10.20.203.66	0	0	0	33	(mindcosy 40		false	Delete
	10.20.203.101	0	0		60	60		false	
The Cogging     The Cogging     The Cogging     The Cogging									
- 🔂 Anomaly Detection									
⊕ Q OS Identifications									
Clear Flow States									
Reset Network Security Heal									
- Support Information									
Diagnostics Report									
System Information									
Sensor Monitoring									
	,	_			Defreeh				
*					Refresh				
IDM is initialized successfully.							tme	e-mob administr	ator 📔

Figure 8-21 Sample List of Host Blocks on a Cisco IPS

Note the following:

- The host blocks list constitutes the client shun list requested by the WLC.
- All active host blocks are passed to the WLC, regardless of whether they are wired or WLAN clients.
- **Step 2** The WLC, upon its next poll of the IPS, receives an updated active host block list and updates its shun list. This is reflected on the WLC under **Security** -> **CIDS** -> **Shunned Clients**. (See Figure 8-22.)

					Sa	<u>v</u> e Configuration	<u>P</u> ing   Lo <u>q</u> ou	ıt   <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Security	CIDS Shu	un List						
* AAA	Re-sync							
General 🔻 RADIUS	IP Addres	is L	ast MAC Address	Expire	Sens	or IP / Index		
Authentication Accounting	10.20.211.	14 0	0:00:00:00:00:00	10	10.20	0.30.33 / 2		
Fallback	10.20.203.0	66 0	0:00:00:00:00:00	19	10.20	0.200.30/1		
TACACS+ LDAP	10.20.203.	101 0	0:18:de:2e:36:71	60	10.20	0.200.30/1		
Local Net Users	10.20.210.	156 0	00:00:00:00:00:00	35	10.20	0.30.55 / 3		
MAC Filtering Disabled Clients User Login Policies AP Policies								
Local EAP								
Priority Order								
Access Control Lists								
Wireless Protection Policies								
🕨 Web Auth								
Advanced     CIDS     Sensors								
Shunned Clients  IPSec Certs  CA Certificate ID Certificate								
TD Continuate								
Done							10.20.	201.2 🙆 //.

#### Figure 8-22 Sample CIDS Shun List on a WLC

Note the following:

- The CIDS shun list contains all host blocks received from all Cisco IPS with which the WLC communicates.
- The expire column indicates the number of minutes remaining before expiry of the host block, as defined by the timeout configured on the Cisco IPS.
- If a WLC is part of a mobility group, the shun list is automatically passed to all WLCs within the mobility group.
- **Step 3** If a WLAN client matching the source IP address of a host block is currently associated to a WLC, the WLC will automatically create a client exclusion for that client, causing it to be disconnected.

To view all client exclusions currently in place on a WLC, along with the reason for the exclusion, go to **Monitor -> Summary** and click on **Detail** next to **Excluded Clients** under the Client Summary section. (See Figure 8-23.)

cisco	MONITOR WLANS	<u>C</u> ONTROLLI	ER W <u>I</u> RELES	S <u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P				
Monitor	Summary										
Summary						6 Access Points	Supported				
Access Points		11111		mmmm	mmmmm		77/17/172				
Statistics		LINKIACT	0/0/0	10/0/		wer 🌑 Status 🌑 Alarm 🔮	AP				
CDP	0.0000000000000000000000000000000000000	100 MBPS	6/6/6			111112 1111111	11111111				
			2 3 4	5 6 7	8						
Rogues		<u> Allanni</u>	unnun ni	<u> 1941/14/16/</u>							
Clients	Controller Summa				Deer	- 0					
					Rugu	e Summary					
	Management IP Addr	ess	10.20.201.2		Activ	e Rogue APs	41	Detail			
	Software Version		5.0.148.2		Activ	e Rogue Clients	3	Detail			
	System Name		wlc-2106-br		Adho	c Rogues	0	Detail			
	Up Time		4 days, 21 hou		Rogu	es on Wired Netw	ork O				
	System Time		Tue Aug 12 14	:22:27 2008							
	Internal Temperature		+50 C		Top V	VLANs					
	802.11a Network Stat		Enabled								
		11b/g Network State Enabled			Profi	e Name	# of	Clients			
	Local Mobility Group		branch		bran	sh	1	Detail			
					bran	sh2	0	Detail			
	Access Point Sum	mary			IPS		0	Detail			
		Total	Up	Down							
	802.11a/n Radios			0 Det	ail Most	Recent Traps					
	802.11b/g/n Radios	2	2	0 Det	ail						
	All APs	2	2	0 Det	ail Clie		Address:00:18:de:2e:				
					ААА		ailure for UserName:/"				
	Client Summary						:93:34:d0 removed fr				
	Gilenc adminiary					Rogue AP : 00:1c:f6:62:83:e1 detected on Base Radio M Rogue AP : 00:1c:f6:62:83:e1 detected on Base Radio M					
	Current Clients	1		<u>Detail</u>	Ro	Jue AP : UU:1c:f6:	62:83:e1 detected on				
	Excluded Clients	1		Detail				View All			
<	Excluded Clients										

Figure 8-23 WLC Monitor Summary screen with Excluded Clients Detail Link

The Excluded Clients list is subsequently displayed. (See Figure 8-24.)

Figure 8-24 Sample Excluded Client List Showing an IPS Host Block

cisco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS <u>S</u> ECU	IRITY M <u>a</u> na	са <u>⊽</u> е са GEMENT С <u>О</u> ММ.		<u>q</u> out   <u>R</u> efres
lonitor	Excluded Clients	- 				Entrie	51-1of1
Summary Access Points Statistics	Search by MAC add	AP Name	AP MAC Addr	WLAN	Protocol	Exclusion Reason	Port
<ul> <li>CDP</li> <li>Roques</li> </ul>	00:18:de:2e:36:71	AP2.3802	00:17:df:a7:50:40	branch	802.11a	UnknownEnum:5	1 🔽
Clients							

Note the following:

- A client exclusion created as a result of an IPS host block is shown with the exclusion reason "UnknownEnum:5".
- Excluded WLAN clients are listed in this summary screen as long as a client exclusion is in place on the WLC.

- A client exclusion will remain active until it expires, based on the client exclusion timeout for that particular WLAN profile.
- A client exclusion is not removed upon retraction of a Cisco IPS host block.
- An excluded client entry indicates that the client was connected to the WLC but that it has been disconnected.

# **Monitoring Cisco WLC and IPS Collaboration**

## **Verifying Cisco WLC and IPS Communication Status**

Successful communication between a Cisco WLC and IPS can be verified through any of the following interfaces:

- WLC GUI
- WLC CLI
- IDM GUI
- IPS CLI

Once successful communication between a Cisco WLC and a Cisco IPS has been verified, the automated threat mitigation tool enabled by this collaboration is available to operational staff.

### WLC GUI

On the WLC GUI, the current status of communication with a particular Cisco IPS can be seen by going to **Security** -> **Advanced** -> **CIDS** -> **Sensors** and clicking on the Index number of the particular sensor. The **Last Query** field will indicate "Success" if the WLC and IPS are able to successfully communicate. (See Figure 8-25.)

								Configuration   <u>P</u> ir	g   Lo <u>q</u> out   <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	CIDS Sen	sor Edit						< Back	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> </ul>	Index Server Address	1 10.20.2	200.30						
Fallback TACACS+ LDAP Local Net Users	Port	443							
MAC Filtering Disabled Clients User Login Policies AP Policies	Username Password								
Local EAP	State	V							
<ul> <li>Priority Order</li> <li>Access Control Lists</li> </ul>	Query Interval	60	seconds						
<ul> <li>Wireless Protection Policies</li> <li>Web Auth</li> </ul>	Fingerprin (SHA1 bach)	40 he	29:43:CB:15:EC: ex chars with e	every 2 char					
Advanced     CIDS     Sensors     Shunned Clients     IPSec Certs     CA Certificate     ID Certificate	Last Quer (count)								

Figure 8-25 Verifying Communication Status between a WLC and a Cisco IPS on the WLC GUI

## WLC CLI

On the WLC CLI, communication with a Cisco IPS can be seen by following these steps:

**Step 1** Login to the CLI of the WLC collaborating with the Cisco IPS.

**Step 2** Enable debugging of the WLC-IPS communication as follows:

debug wps cids enable

Debugs automatically appear on the screen as soon as an event occurs.

The following is a sample of a successful WLC poll of a Cisco IPS with a shun list request:

Tue Aug 12 14:21:43 2008: cidsProcessSdeeQuery: ip=10.20.200.30,port=443 state=1
interval=60
Tue Aug 12 14:21:43 2008: cidsQuerySend:
https://10.20.200.30:443/cgi-bin/transaction-server?command=getShunEntryList
Tue Aug 12 14:21:43 2008: curlHandle is bbd422c
Tue Aug 12 14:21:43 2008: Perform on curlHandle bbd422c ...
Tue Aug 12 14:21:43 2008: Response code is 0
Tue Aug 12 14:21:43 2008: xmlDoc buffer freed
Tue Aug 12 14:21:43 2008: Parser cleaned

**Step 3** After communication is verified, disable debugging:

debug wps cids disable

### IDM GUI

The IDM tool can be used to view events generated by the Cisco IPS during communication with a Cisco WLC.

On the IDM, go to **Monitoring** -> **Events**.

Enable Show status events, define a short timeframe for Show past events (shown in Figure 8-26 for 3 minutes), and select View.

Figure 8-26 Viewing Cisco WLC and IPS Communication Events on the IDM

🎼 Cisco IDM 6.1 - 10.20.200.30		- 🗆 ×
<u>File View H</u> elp		abab
Home 🖓 Configuration 🔯 Mor	nitoring 📀 Back 🕥 Forward 🔍 Refresh 🦻 Help	cisco
Sensor Monitoring R × Sensor Monitoring R × Sensor Monitoring R × Sensor Monitoring Denied Attackers Host Blocks Rate Limits P Logging P Dynamic Data Anomaly Detection Q OS Identifications Properties Clear Flow States Support Information Dignostics Report Statistics System Information	Monitoring > Sensor Monitoring > Events         You can display the events in the sensor Event Store. To filter on event type and/or time, select the appropriate check boxes.         Show Alert Events         Informational       I.ow         Min       Max         Threat Rating (0-100):       0         Show Altextex Response Controller events       Select the number of the rows per page:         Show all events currently stored on the sensor       Show all events currently stored on the sensor         Show all events from the following time range       Start Time (UTC)         From:       January       DI         Informe (UTC)       00       End Time (UTC)         To:       January       DI         View       Reset	
Sensor Monitoring		
IDM is initialized successfully.	t tme-mob administ	rator

In the IDM Event Viewer screen, the related events generated as a result of successful communication will depend upon the IPS software release, as outlined below:

• Prior to IPS Release 6.1

Two related entries generated: one for the event **User logged into HTTP server** and another for the event **getShunEntryList succeeded**.

• IPS Release 6.1 or later

By default, just one entry generated for the event **User logged into HTTP server**. In order to see the **getShunEntryList** event and view the status of a shun-list request, logging of control transactions must be enabled on the IPS CLI. For more information, refer to IPS CLI, page 8-33.

Double-click on an event to see the details, including which WLC logged into the IPS and whether the shun list request was successfully processed. See Figure 8-27 and Figure 8-28.



Figure 8-27 WLC Login to a Cisco IPS Event on the IDM



Figure 8-28 Successful Retrieval of the Shun List by the WLC Event on the IDM

### **IPS CLI**

On the IPS CLI, communication with a particular Cisco WLC can be seen by following these steps:

- **Step 1** Login to the CLI of the IPS collaborating with the Cisco WLC.
- Step 2 Review the recent past events for this WLC, as follows

```
ips-3845-2# show events past 0:03 | include 10.20.201.2
```

The following is a sample of a successful WLC login to the IPS and retrieval of the shun list:

```
evStatus: eventId=1199725892006801610 vendor=Cisco
originator:
    hostId: ips-asa-2
    appName: cidwebserver
    appInstanceId: 320
    time: 2008/08/07 16:50:34 2008/08/07 16:50:34 UTC
    loginAction: action=loggedIn
    description: User logged into HTTP server
    userName: pod1-wism-2-1
    userAddress: port=60597 10.20.100.150
```

```
evStatus: eventId=1199725892006801611 vendor=Cisco
originator:
   hostId: ips-asa-2
   appName: nac
   appInstanceId: 320
time: 2008/08/07 16:50:34 2008/08/07 16:50:34 UTC
controlTransaction: command=getShunEntryList successful=true
   description: Control transaction response.
   requestor:
     user: pod1-wism-2-1
     application:
     hostId: 10.20.100.150
     appName: mainApp
     appInstanceId: 320
```

```
Note
```

IPS Release 6.1 or later does not, by default, generate the event **getShunEntryList succeeded.** In order to see this event and the shun-list request status, logging of control transactions must be enabled on the IPS CLI, as shown below.

```
ips-3845-2(config)# service logger
ips-3845-2(config-log)# event-store
ips-3845-2(config-log-eve)# status-event-logging-categories controlTransaction enabled
true
```

Once successful communication has been verified, this level of logging should be disabled, unless specifically required, as shown below:

```
ips-3845-2(config)# service logger
ips-3845-2(config-log)# event-store
ips-3845-2(config-log-eve)# status-event-logging-categories controlTransaction enabled
false
```

For more information, refer to the IPS documentation (see Cisco IPS, page 8-51).

## Viewing WLAN Client Block Events

### WLC Local Logging of WLAN Client Block Events

If a WLC is configured with local logging set to a minimum security level of 1, a WLC will record WLAN client block events enforced as a result of an IPS host block. For details on configuring local logging, refer to Enabling WLC Local Logging of WLAN Client Block Events, page 8-15.

#### WLC Local Log Format for a WLAN Client Block

The general format of a local message log entry generated by a WLC upon enforcement of a WLAN client block is as follows:

mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:34:ca to exclusion list as a result of an IDS shun event for 10.20.205.51

#### WLC Local Log

The WLC local log can be viewed under Management -> Logs -> Message Logs. (See Figure 8-29.)

Save Configuration | Ping | Logout | Refresh . . . . . . . . CISCO MONITOR <u>W</u>LANs WIRELESS MANAGEMENT COMMANDS HELP Management Message Logs Clear Summary Aug 12 14:22:41.053 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:21:43.474 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client SNMP 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:18:50.533 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client HTTP 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Telnet-SSH Aug 12 14:17:52.953 mm listen.c:4696 MM-1-CLIENT SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Serial Port Aug 12 14:16:55.376 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Local Management Aug 12 14:15:57.792 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 User Sessions Aug 12 14:15:00.214 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 💌 Logs Aug 12 14:14:02.632 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client Config 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:13:05.061 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Message logs Aug 12 14:12:07.583 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Mgmt Via Wireless Tech Support Aug 12 14:11:09.520 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:10:11.938 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:09:14.364 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101 Aug 12 14:08:16.787 mm\_listen.c:4696 MM-1-CLIENT\_SHUNNED: Adding client 00:18:de:2e:36:71 to exclusion list as a result of an IDS shun event for 10.20.203.101

Figure 8-29 WLC Local Log Showing a WLAN Client Block Event

Note the following:

- As long as there is an active IPS host block for a client IP address, upon the WLC client exclusion expiring, the WLC will automatically create a new client exclusion each time the client associates or attempts to associate to the WLAN.
- Consequently, depending on the duration that an IPS host block is in place and the client exclusion timeout, multiple client exclusion events may occur, generating multiple message log entries.

### SNMP Reporting of WLAN Client Block Events

If SNMP traps are enabled for client exclusion, an SNMP trap is generated upon a WLC implementing a WLAN client shun to enforce an IPS host block. These SNMP traps can be used by WLC, WCS, CS-MARS, and general SNMP management station. For details on enabling SNMP, refer Enabling SNMP Traps for WLAN Client Block Events, page 8-16.

The WLC GUI reports SNMP traps in two locations:

- WLC summary screen
- WLC SNMP trap logs

225419

#### **SNMP Trap Format for a WLAN Client Block**

The general format of an SNMP trap generated by a WLC upon enforcement of a WLAN client block is as follows:

Client Excluded: MACAddress:00:18:de:2e:36:71 Base Radio MAC :00:17:df:a7:50:40 Slot: 1 Reason:Unknown ReasonCode: 5

In this example, **Reason:Unknown** and **ReasonCode: 5** indicate that the exclusion event was generated as a result of an IPS host block.

#### **WLC Summary Screen**

The WLC summary screen includes a **Most Recent Traps** section where a WLAN client block event appears as a client exclusion event. On the WLC, go to **Monitor** -> **Summary**. (See Figure 8-30).

cisco	MONITOR WLANS		R WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP		Logout <u>R</u> efre		
nitor	Summary										
ummary						6 Access Poin	ts Supported				
ccess Points		Jan 19	amananan		namenna						
tatistics		LINKIACT				wer 🔵 Status 🔵 Alarm	AP				
DP											
oques		100 MBPS	2 3 4	5 6 7	8						
lients											
	Controller Summa	irv			Roque	Summary					
	Management IP Addre	1.00	10.20.201.2			· · · · · · · · · · · · · · · · · · ·					
	Software Version		5.0.148.2		Active F	Rogue APs	3	8	<u>Detail</u>		
	System Name		wlc-2106-br		Active F	Active Rogue Clients			Detail		
	Up Time		0 days, 23 hours, 10 minutes Fri Aug 8 15:56:23 2008			Adhoc Rogues			<u>Detail</u>		
	System Time					on Wired Netwo	rk 0				
	Internal Temperature		+51 C								
	802.11a Network Stat		Enabled		Top WL	ANs					
	802.11b/g Network St		Enabled								
	Local Mobility Group		branch			Name		# of Cli			
					branch			1	Detail		
	A Delint Our				branch2	2		0	Detail		
	Access Point Sum	mary			IPS			0	Detail		
		Total	Up Do	own							
	802.11a/n Radios	2	2 🔴 0	Detail	Most R	ecent Traps					
	802.11b/g/n Radios	2 🔴	2 🔴 0	Detail	Client	Excluded: MACA	ddrocc 00 18 d	a.2a.26.	71 Bacal		
	All APs	2 🔴	2 🔴 0	Detai		AP:00:1c:f6:6					
	Client Summary					Rogue AP : 00:16:9c:93:34:d1 detected on Base Radio					
	,	ic ourning y			· · ·	tial Honeypot AP					
	Current Clients	1		<u>Detail</u>	Foten	aar noneypot AP	. 00.17.ur.d/14	n.ez det	View All		
	Excluded Clients	1		<u>Detail</u>					VIEW AII		
	Disabled Clients	0	 Detail		This as a	This page refreshes every 30 seconds.					

Figure 8-30 WLC Summary Screen Showing a WLAN Client Block Event

#### WLC SNMP Trap Logs

The WLC SNMP trap logs include all SNMP traps generated by a WLC. An SNMP trap generated upon a WLAN client block event appears in the log as a client exclusion event. To view the SNMP trap log on a WLC, go to **Management -> SNMP -> Trap Logs**. (See Figure 8-31.)
cisco	MONITOR WLANS CONTR	LLER W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Lo <u>g</u> out   <u>R</u> efresh
Management	Trap Logs						Clear Log
Summary	Number of Traps since last i	set 2431					-
SNMP	Number of Traps since log la	st viewed 4					
General SNMP V3 Users	Log System Time Trap						
Communities Trap Receivers		cluded: MACAddre eason:Unknown Re		e:36:71 Base Ra	dio MAC :00:17	:df:a7:50:40	)
Trap Controls Trap Logs		cluded: MACAddre eason:Unknown Re		e:36:71 Base Ra	dio MAC :00:17	:df:a7:50:40	)
НТТР		P : 00:1c:f6:62:83: e no:0(802.11b/g)		rom Base Radio	MAC : 00:17:df:	a7:50:40	
Telnet-SSH		P:00:1c:f6:62:83: e no:0(802.11b/g)		rom Base Radio	MAC : 00:17:df:	a7:4f:e0	
Serial Port	Tue Aug 12 Client E	cluded: MACAddre	ess:00:18:de:2	e:36:71 Base Ra	dio MAC :00:17	:df:a7:50:40	)
Local Management Users	5 Tue Aug 12 Rogue	eason:Unknown Re P : 00:1c:f6:62:83: e no:0(802.11b/g)	e0 removed f	rom Base Radio	MAC : 00:17:df:	a7:4f:e0	
User Sessions	Tue Aug 12 Rogue A	P : 00:1c:f6:62:83: e no:0(802.11b/g)	e0 removed f	rom Base Radio	MAC : 00:17:df:	a7:50:40	
Logs Config		cluded: MACAddre	ss:00:18:de:2	e:36:71 Base Ra	dio MAC :00:17	:df:a7:50:40	)
Message logs	9 Tue Aug 12 Rogue /	P : 00:16:9c:93:34: e no:0(802.11b/g)	d1 removed f	from Base Radio	MAC : 00:17:df	a7:50.19	
Mgmt Via Wireless Tech Support	Tue Aug 12 Client E	cluded: MACAddre eason:Unknown Re	ess:00:18:de:2	2e:36:71 Base Ra	dio MAC :00:17	:df:a7:50:40	$\supset$
P Tech Support	Tuo Aug 12	hentication Failur		ne:/" User Type:	WLAN USER		
	11 Tue Aug 12 Rogue	P : 00:16:9c:93:34: e no:0(802.11b/g)		rom Base Radio	MAC : 00:17:df	a7:50:40	
	12 Tue Aug 12 Rogue	P : 00:1c:f6:62:83: e no:0(802.11b/g)	e1 detected o				fied
	12 Tue Aug 12 Rogue	P:00:1c:f6:62:83: e no:0(802.11b/g)	e1 detected o	n Base Radio MA	C:00:17:df:a7	:4f:e0	

Figure 8-31 WLAN Client Exclusion Trap Generated as a Result of a WLAN Client Block

Note the following:

- As long as there is an active IPS host block for a client IP address, upon the WLC client exclusion expiring, the WLC will automatically create a new client exclusion each time the client associates or attempts to associate to the WLAN.
- Consequently, depending on the duration that an IPS host block is in place and the client exclusion timeout, multiple client exclusion events may occur, generating multiple SNMP traps.

### **IPS Events Related to Host Block Events**

The events generated by a Cisco IPS when a host block is activated can be viewed on IDM.

On IDM, go to **Monitoring** -> **Events**. Enable **Show status events**, define a short timeframe for **Show past events** (shown in Figure 8-32 for 3 minutes) and select **View**.

🕼 Cisco IDM 6.1 - 10.20.200.30		<u>- □ ×</u>
<u>File View H</u> elp		ahaha
Home 🦓 Configuration [ Mor	nitoring 🔇 Back 🚫 Forward 🔍 Refresh 🦻 Help	cisco
Sensor Monitoring	Monitoring > Sensor Monitoring > Events         You can display the events in the sensor Event Store. To filter on event type and/or time, select the appropriate check boxes.         Show Alert Events         If Informational       Low         Min       Max         Threat Rating (0-100):       0         If Threat Rating (0-100):       0         Show status events       Select the number of the rows per page:         Threat Rating (0-100):       0         Show all events torfendy stored on the source         Show past events       Select the number of the rows per page:         Show all events       100         Show past events       100         Show past events       100         Show past events       100         Show all events torfendy stored on the source       100         Show past events       110         Show past events       111         Show	
Sensor Monitoring		
I IDM is initialized successfully.	tme-mob administ	rator

Figure 8-32 Viewing Host I	Block Events on the IDM
----------------------------	-------------------------

The IDM Event Viewer is subsequently displayed. In the IDM Event Viewer screen, a **Block Host** event is generated for each host block activated. Double-click on an event to see the details, including the IP address that was blocked. (See Figure 8-33.)

	lonitoring 🔇 Back	💭 Forward   🔇 Refresh 🧳 Help	cisco
Sensor Monitoring  T		sor Monitoring > Events	
Events     Time-Based Actions	You can display th	events in the sensor Event Store. To filter on event type and/or time, select the appropriate check boxes.	
🖉 Denied Attackers 🛛 👔	Event Viewer		
Host Blocks			
- Kontwork Blocks			
IP Logging	# Type		Sig ID Performed Actions Details
🗆 🦙 Dynamic Data	1 status	Aug 12, 2008 14:19: Aug 12, 2008 14:19: 1217975967077246 User logged into Firm Server	<u> </u>
- 🛃 Anomaly Detection	2 status	Aug 12, 2008 14:20: Aug 12, 2008 14:20: 12179759 7077340 User logged into HTTP serve	
	3 status	Aug 12, 2008 14:21: Aug 12, 2008 14:21: 12179759670, 7240 Block Host	
Properties     Gear Flow States	4 error:error	🕼 Details for 1217975967077340614	×
Reset Network Security	5 status	evStatus: eventId=1217975967077340614 vendor=Cisco	
- Support Information	6 status	evstatus: eventid=121/9/596/0//340614 Vendor=tisco originator:	
Diagnostics Report	7 status	hostId: ips-3845-2	
	8 status	appName: nac	
- System Information	9 status	appInstanceId: 1069	
	10 status	time: Aug 12, 2008 14:21:46 UTC offset=0 timeZone=UTC	
	11 status	shunEntryAdded:	
	12 status	description: Block Host	
	13 status	shunInfo: host:	
	14 status	srcAddr: 10.20.203.101	
	15 status	srcPort: 0	
	16 status 17 status	destAddr: 0	
	17 status 18 status	destPort: 0	
	19 status	protocol: numericType=0	
	20 status	vlan:	
	21 status	interface:	
	22 status	timeoutNinutes: 60	
1	23 status		
Sensor Monitoring	24 status		
4 <u>00</u>	25 status		
	26 status		
and the first of the	27 status		
DM is initialized successfully.	28 status		
	29 status	,	▼ Refresh
		Close	d: 8/12/08 4:49:32 PM

Figure 8-33 Block Host Event on the IDM



If blocking is not enabled or configured on the IPS, an error event is generated indicating that a host block could not be executed (see Figure 8-34). The active host block list is, however, correctly updated with the host block and the WLC-IPS collaboration does successfully enforce the block.

This error message simply indicates that the IPS was not able push the host block policy out to a device. This is normal operation for the WLC-IPS collaboration, because the WLC pulls the active host block list from the IPS rather than the IPS actively pushing the host block out. The error is based on the push nature of the Attack Response Controller (ARC) feature, which expects blocking to be enabled and configured in order for a host block to be enforced. For more information on the ARC feature, refer to the IPS documentation (see Cisco IPS, page 8-51).

Image: Cisco IDM 6.1 - 10.20.200.           Ele         Mew           Help           Home         Configuration		. 💽 Forward 💽 Refr	esh ʔ Help				- 🗆 ×		
Sensor Monitoring 🗗 🕂 🗙	Monitoring > Se	nsor Monitoring > Event:	6						
Events	You can display th	e events in the sensor Even	t Store. To filter on even	t type and/or time, sele	ct the appropriate check boxes.				
Denied Attackers	👩 Event Viewer								×
Host Blocks									
	# Type	Canada LITC Time	Concern Local Time	Europh ID	Cuesta.	G-10	Deufenne of Antion		<u></u>
IP Logging	# Type	Sensor UTC Time	Sensor Local Time	Event ID	Events User logged into HTTP server	Sig ID	Performed Actions		Details
Oynamic Data     Anomaly Detection	2 status				user logged into HTTP server				
OS Identifications	3 status	Aug 12, 2008 14:21:						_	
Properties	4 error:error				Unable to execute a host block [10.2				
- @ Clear Flow States					blocking is disabled				
Reset Network Security	5 status	Provide for 4.24	70750(7077240(4	F			×		
- Support Information	6 status		797596707734061				<u> </u>		
Diagnostics Report     Statistics	7 status	evError: eventId=	12179759670773406	15 vendor=Cisco	severity=error				
System Information	8 status	originator:							
	9 status	hostId: ips-3	845-2						
	10 status	appName: nac appInstanceId	. 1100						
	11 status		: 1122 :008 14:21:46 UTC	offget-0 time7	one-IIIC				
	12 status				.20.203.101] because block	ing is di	sabled name=		
	13 status		mable of checkle	a 1000 broom [10	inclusion in the second	ing it ui			
	14 status 15 status								
	16 status						k	_	
	10 status 17 status								
	18 status							اللاري	
	19 status	1							
	20 status								
	21 status								
	22 status						b		
	23 status								
Sensor Monitoring	24 status								
	25 status								
	26 status						b		
1	27 status								
IDM is initialized successfully.	28 status								
	29 status						E	-	Refresh
	2	•					h (	: 8/12/0	8 4:49:32 PM
				Clos				,, 0	
				Lios					

Figure 8-34 Host Block Error Event on the IDM

### WLC CLI Reporting of WLAN Client Block Events

The WLC CLI can be used to view an active host block list being received from the IPS and the shun list being updated.

To enable debugging for these events, perform the following steps:

- **Step 1** Login to the CLI of the WLC collaborating with the Cisco IPS
- **Step 2** Enable debugging of the WLC-IPS communication as follows:

### debug wps cids enable

Debugs automatically appear on the screen as soon as an event occurs.

The following is a sample of a WLC to Cisco IPS query for the shun list, which in this instance includes a new host block for IP address 10.20.203.101:

```
Tue Aug 12 14:21:43 2008: cidsProcessSdeeQuery: ip=10.20.200.30,port=443 state=1
interval=60
Tue Aug 12 14:21:43 2008: cidsQuerySend:
https://10.20.200.30:443/cgi-bin/transaction-server?command=getShunEntryList
Tue Aug 12 14:21:43 2008: curlHandle is bbd422c
Tue Aug 12 14:21:43 2008: Perform on curlHandle bbd422c ...
Tue Aug 12 14:21:43 2008: Response code is 0
Tue Aug 12 14:21:43 2008: Add 10.20.203.101 from local sensor 10.20.200.30 to shun-list
Tue Aug 12 14:21:43 2008: xmlDoc buffer freed
Tue Aug 12 14:21:43 2008: Parser cleaned
```

**Step 3** After debugging is complete, disable debugging:

debug wps cids disable

### **IPS CLI Reporting of WLAN Client Block Events**

The events generated on the IPS CLI when a host block is passed to a WLC can be seen by performing the following steps:

- **Step 1** Login to the CLI of the IPS collaborating with the Cisco WLC.
- **Step 2** Review the recent past events for this WLC as follows:

ips-3845-2# show events past 0:03 | include block

The following is a sample of a host block being activated on a Cisco IPS and retrieval:

```
evStatus: eventId=1217975967077340614 vendor=Cisco
  originator:
   hostId: ips-3845-2
    appName: nac
    appInstanceId: 1069
  time: 2008/08/12 14:21:46 2008/08/12 14:21:46 UTC
  shunEntryAdded:
    description: Block Host
    shunInfo:
      host:
        srcAddr: 10.20.203.101
        srcPort: 0
        destAddr: 0
        destPort: 0
        protocol: numericType=0
        vlan:
        interface:
      timeoutMinutes: 60
```



If blocking is not enabled or configured on the IPS, an error event is generated indicating that a host block could not be executed (see Figure 8-34). The active host block list is, however, correctly updated with the host block and the WLC-IPS collaboration does successfully enforce the block.

This error message simply indicates that the IPS was not able push the host block policy out to a device. This is normal operation for the WLC-IPS collaboration, because the WLC pulls the active host block list from the IPS rather than the IPS actively pushing the host block out. The error is based on the push nature of the Attack Response Controller (ARC) feature, which expects blocking to be enabled and configured in order for a host block to be enforced. For more information on the ARC feature, refer to the IPS documentation (see Cisco IPS, page 8-51).

```
evError: eventId=1217975967077340615 severity=error vendor=Cisco
originator:
    hostId: ips-3845-2
    appName: nac
    appInstanceId: 1122
    time: 2008/08/12 14:21:46 2008/08/12 14:21:46 UTC
    errorMessage: name=errSystemError Unable to execute a host block [10.20.203.101] because
    blocking is disabled
```

## **Viewing Excluded Clients**

All client exclusions currently in place on a WLC, along with the reason for the exclusion, can be seen on a WLC in the "Excluded Clients" list. This can be viewed by going to **Monitor** -> **Summary** and clicking on **Detail** next to "Excluded Clients" under the Client Summary section. (See Figure 8-35.)

Figure 8-35 WLC Monitor Summary screen with Excluded Clients Detail Link

Summary Access Points Statistics CDP Rogues Clients Clients Control Syste Intern 802.1 802.1 Local Access Control Contro Contro Control Contro Contro Control Control Control	troller Summa agement IP Addr ware Version em Name ime em Time rnal Temperatura	ress	2 3 10.20.2 5.0.148 wlc-210 4 days, Tue Au	8.2 D6-br	29 minutes 27 2008	Rogue S Active R Active R Adhoc R	Access Points S Status Alum A Summary ogue APs ogue Clients ogues on Wired Networ	₽ ₽	41 3 0	<u>Detail</u> Detail
Access Points Statistics CDP Rogues Clients Clients Contri Mana Softwa Syste Up Ti Syste Inter 802.1 802.1 Local Accee	agement IP Addr ware Version em Name ime em Time	100 MBP3	2 3 10.20.2 5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Rogue S Active R Active R Adhoc R	Status Alarm A Summary ogue APs ogue Clients ogues	₽ ₽	3	Detail
Statistics CDP Rogues Clients Clients Conti Mana Softw Syste Up Tit Syste Inter 802.1 802.1 Local Acces	agement IP Addr ware Version em Name ime em Time	100 MBP3	2 3 10.20.2 5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Rogue S Active R Active R Adhoc R	Summary ogue APs ogue Clients ogues		3	Detail
CDP Rogues Clients Conti Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local Acces	agement IP Addr ware Version em Name ime em Time	100 MBP3	2 3 10.20.2 5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Rogue S Active R Active R Adhoc R	Summary ogue APs ogue Clients ogues		3	Detail
Rogues Clients Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local Acce	agement IP Addr ware Version em Name ime em Time	ary ress	5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Active R Adhoc R	ogue APs ogue Clients ogues		3	Detail
Rogues Clients Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local Acce	agement IP Addr ware Version em Name ime em Time	ary ress	5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Active R Adhoc R	ogue APs ogue Clients ogues		3	Detail
Clients Cont Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local Acce	agement IP Addr ware Version em Name ime em Time	ress	5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Active R Adhoc R	ogue APs ogue Clients ogues		3	Detail
Conti Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local	agement IP Addr ware Version em Name ime em Time	ress	5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Active R Adhoc R	ogue APs ogue Clients ogues		3	Detail
Mana Softw Syste Up Ti Syste Inter 802.1 802.1 Local	agement IP Addr ware Version em Name ime em Time	ress	5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Active R Adhoc R	ogue APs ogue Clients ogues		3	Detail
Softw Syste Up Ti Syste Intern 802.1 802.1 Local	ware Version em Name iime em Time		5.0.148 wlc-210 4 days, Tue Au	3.2 D6-br , 21 hours,		Active R Adhoc R	ogue Clients ogues		3	Detail
Syste Up Ti Syste 1ntern 802.1 802.1 Local	em Name îme em Time	e	wic-210 4 days, Tue Au	D6-br , 21 hours,		Adhoc R	ogues		-	
Up Ti Syste 1ntern 802.1 802.1 Local	ime em Time	e	Tue Au				-		0	
Inter 802.1 802.1 Local		e	Tue Au			Rogues				Detail
802.1 802.1 Local	mal Temperature	e						rk	0	
802.1 Local			+50 C							
Local	802.11a Network State		Enabled			Top WL	ANs			
Acce	11b/g Network S	State	Enabled branch			Profile N	lame		# of Cl	liante
	l Mobility Group					branch	vanie		1	Detail
						branch2			0	Detail
	ess Point Sum	nmary				IPS			0	Detail
802.1										
802.1		Total	Up		wn	Most Ps	ecent Traps			
	11a/n Radios	2	• 2	• •	Detail		scent hups			
	11b/g/n Radios	2	• 2 • 2	• 0	Detail	Client E	Excluded: MACA	ddress:00:18:c	de:2e:36:	:71 Base F
All AF	Ps				<u>Detail</u>	AAA Au	thentication Fail	ure for UserNa	me:/" U	ser Type:
						Rogue	AP:00:16:9c:9	93:34:d0 rema	ved from	n Base Rac
Clien	nt Summary					Rogue	AP:00:1c:f6:6	2:83:e1 detect	ed on Ba	se Radio M
Curre	ent Clients	1	1		Detail	Rogue	AP:00:1c:f6:6	2:83:e1 detect	ed on Ba	ase Radio M
Exclu	uded Clients	1	1		Detail	_)				View All
Disab						This page	refreshes ever	x 30 seconds		

The Excluded Clients list is subsequently displayed. (See Figure 8-36.)

Figure 8-36 Excluded Clients List

cisco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS SECU	IRITY M <u>A</u> NAG		onfiguration   <u>P</u> ing   Lo ANDS HE <u>L</u> P	gout   <u>R</u> e	iresh
Monitor Summary Access Points Statistics CDP Rogues Clients	Excluded Clients Search by MAC add Client MAC Addr 00:18:de:2e:36:71	;	AP MAC Addr 00:17:df:a7:50:40		Protocol 802.11a		s 1 - 1 of Port 1	F 1

Note the following:

- A client exclusion created as a result of an IPS host block is shown with the exclusion reason "UnknownEnum:5".
- Excluded WLAN clients are listed in this summary screen, as long as a client exclusion is in place on the WLC.
- A client exclusion will remain active until it expires, based on the client exclusion timeout for that particular WLAN profile.
- A client exclusion is not removed upon retraction of a Cisco IPS host block.
- An excluded client entry indicates that the client was connected to the WLC but that it has been disconnected.

## WCS Cross-WLC Monitoring of WLAN Client Block Events

If WCS cross-WLC monitoring is enabled, the WCS can be consulted for a consolidated view of currently shunned clients and currently excluded clients, as well as historical security events and statistics. For details on enabling WCS cross-WLC monitoring of WLAN events, refer to Enabling WCS Cross-WLC Monitoring of WLAN Events, page 8-18.

### **Consolidated Shunned Clients List**

WCS provides a consolidated shunned clients list, showing all active host blocks passed to all WLCs.

On WCS, go to **Monitor** -> **Security** -> **Shunned Clients**. Select a search option from the drop-down list, which enables a listing of blocked clients to be generated based on all, per-controller, or per-client IP address. (See Figure 8-34.)

ahaha	Wireless Control	System	Username:	tme-mob	Logout	Refresh   Print Viev
CISCO	<u>M</u> onitor ▼ <u>R</u> eports	▼ <u>C</u> onfigure ▼ Location ▼	<u>A</u> dministration $\bullet$	<u>T</u> ools 🔻	<u>H</u> elp 🔻	
ShunnedClients	Shunned Clients					
Search for clients by						
All Shunned Clients 🔍	Client IP Address	Sensor IP Address	Controller			
Search	10.20.211.14	10.20.30.33	10.20.201.2			
Search	10.20.210.156	10.20.30.55	10.20.201.2			
	10.20.203.66	10.20.200.30	10.20.201.2			
	10.20.203.101	10.20.200.30	10.20.201.2			
	10.20.211.14	10.20.30.33	10.20.100.150			
	10.20.210.156	10.20.30.55	10.20.100.150			
	10.20.211.14	10.20.30.33	10.20.100.50			
	10.20.210.156	10.20.30.55	10.20.100.50			
Alarm Summary <sup>®</sup>						
Malicious AP 0 0 0 Coverage Hole 0 0 0						
Coverage Hole 0 0 0 Security <mark>5</mark> 0 <u>13</u>						
Controllers <u>3</u> <u>2</u> <u>7</u>						
Access Points <u>3</u> 00						
Location 0 0 0						
Mesh Links 0 0 0						
wcs o o						

Figure 8-37	WCS Cross-WLC View of Shunned Clients
-------------	---------------------------------------

Note the following:

- This is a consolidated view of the shunned client list present on each WLC, as passed to it by all collaborating Cisco IPS devices.
- This list represents those client IP addresses that will be blocked by a WLC upon a client with a matching IP address connecting to the WLAN.
- This list does not reflect clients currently being excluded by a WLC.
- If multiple WLCs collaborate with the same Cisco IPS, there will be duplicate client IP addresses displayed.

## **Consolidated Excluded Client Events List**

WCS provides a consolidated list of active client exclusions across all WLCs.

On WCS, go to **Monitor** -> **Security** -> **Summary** and click on the **Total Active** field that corresponds to **Excluded Client Events**. (See Figure 8-38.)

Figure 8-38 Sample WCS Security Summary Screen

CISCO	📅 <u>M</u> onitor 🕶	<u>R</u> eport	s 🔻 🤇	onfigure		∖dmin	istration	n <del>v</del> <u>T</u> oo	ols <del>▼</del> <u>H</u> elp <del>▼</del>					
	Security Summ	ary												
nary e APs	Malicious Rogue APs	Las Hou	24 r Hours	Total Active	Signature Attacks		: 24 r Hours	Total Active	AP Threats/Attacks	Last Hour	24 Hours	Total Active		
e Adhocs	Alert	0	0	0	Custom	0	0	0	Fake AP Attack	0	0	<u>0</u>		
e Clients	Contained	0	0	0	NULL probe	0	0	0	AP Missing	0	0	0 0		
	Threat	0	0	0	resp 1	0	0	2	AP Impersonation	0	0	0		
ed Clients	Contained Pending	0	0	Q	Broadcast Probe floo	0	0	0	AP Invalid SSID AP Invalid Preamble	0	0	0		
					EAPOL flood	0	0	0	AP Invalid Encryption	0	0	<u>v</u>		
	802.11a/n5.0	0	0	0	Res mgmt 6 &	0	0	0		0	0	<u>×</u>		
	802.11b/g/n2.4	0	0	0	7	0	0	2	Denial of Service (NAV	0				
	On Network	0	0	0	Reserved mgmt F	0	0	<u>0</u>	related)	0	0	<u>0</u>		
	Off Network	0	0	0	Bcast deauth	0	0		Client Security Related	Last	24	Total		
		Lac	24	Total	Reassoc flood	0	0	6						
	Friendly Rogue APs		r Hours		Disassoc flood	0	0	0		1	2	5		
	Alert	0	0		Res mgmt E &	0	0	Q	WEP Decrypterson	-		2		
	Internal	0	0	0 0	F.				WPA MIC Errors	0	0	0		
	External	0	0	0	Auth flood	0	0	<u>0</u>	Shunned Clients	0	0	0		
	Externer	0	0	<u>~</u>	NetStumbler 3.2.3	0	0	<u>0</u>	IPSEC Failures	0	0	<u>0</u>		
	802.11a/n5.0	0	0	0	NetStumbler	0	0	Q						
	802.11b/g/n2.4	0	0	0	3.3.0									
					Deauth flood	0	0	0 0						
	Unclassified	Last	24 r Hours	Total Active	Wellenreiter	0								
	Rogue APs				NetStumbler generic	0	0	Q						
	Alert	6	21	<u>43</u>	NetStumbler	0	0	٥						
	Contained	0	0	0	3.2.0									
	Contained Pending	0	0	0	Reserved mgmt 7	0	0	<u>0</u>						
	802.11a/n5.0	4	11	23	Assoc flood	0	0	<u>0</u>						
	802.11b/g/n2.4	2	10	20	Res mgmt D	0	0	0						
					NULL probe	0	0	0						
n Summary 🍳	Rogue Adhocs	Last Hour	24 1 Hours /	otal Ictive	resp 2									
age Hole 0 0 0	Alert	0												
V 5 0 13	Contained	0	) <u>(</u>	1										
llers <u>3 2 7</u>	Threat	0	) (	1										
Points 3 0 0	Contained Pending	0	) (	1										
Links 0 0 0	802.11a/n5.0	0	o (	1										
0 0 0	802.11b/g/n2.4	0												

The active client exclusions across all WLCs is subsequently displayed. (See Figure 8-39.)

ahaha	Wireless C	ontrol System			Username: <mark>tme-mob   Logo</mark> u	it   Refresh   Print Vi
cisco	🚡 Monitor 🗸	<u>R</u> eports 🔻 <u>C</u> onfigure 🔻	Location	n 👻 <u>A</u> dministration 👻	v <u>T</u> ools ▼ <u>H</u> elp ▼	
	Alarms (Edit M	<u>ew</u> )			Select a	command 🔹 GO
P, Name,SSI Go					00000	
arch Alarms	Severity	Failure Object	<u>Owner</u>	<u>Date/Time</u> ▼	Message	Acknowledged
	🗌 Minor	Client 00:18:de:2e:36:71		8/12/08 7:10:06 AM	Client '00:18:de:2e:36:71' which was associated	No
ew Search	🗌 Minor	Client 00:18:de:2e:34:ca		8/12/08 6:00:32 AM	Client '00:18:de:2e:34:ca' which was associated	No
	Minor	Client 00:18:de:1d:91:e6		6/23/08 1:08:18 PM	Client '00:18:de:1d:91:e6' which was associated	No
ed Searches Edit Select Search	🗌 Minor	Client 00:18:de:1d:91:97		6/23/08 1:03:55 PM	Client '00:18:de:1d:91:97' which was associated	No
Select Search 💽	🗌 Minor	Client 00:18:de:1d:90:8c		5/14/08 2:05:39 PM	Client '00:18:de:1d:90:8c' which was associated	No
larm Summary 🌻						
Ilicious AP 0 0 0 Iverage Hole 0 0 0 curity <u>5</u> 0 <u>13</u> Introllers <u>3 2 7</u>						
2         0						
cs o o						

Figure 8-39 Sample WCS Active Excluded Client Events Screen

Note the following:

• The WCS performs data aggregation on events. Consequently, identical events are summarized and listed as a single event. This feature is not configurable. All events are, however, logged and can be viewed in the event history of any particular event.

More detailed information on any particular exclusion event can be viewed by clicking the client. (See Figure 8-40.)

ahaha	Wireless Control System	Username: tme-mob   Logout   Refresh   Print View
CISCO	Monitor ▼ Reports ▼ Configure ▼ Location ▼	<u>A</u> dministration ▼ <u>T</u> ools ▼ <u>H</u> elp ▼
Quick Search <ip, go<="" name,ssi="" th=""><th><u>Alarms</u> &gt; Client 00:18:de:2e:36:71</th><th> Select a command 💌 GO</th></ip,>	<u>Alarms</u> > Client 00:18:de:2e:36:71	Select a command 💌 GO
Search Alarms	General	Message
New Search Saved Searches Edit Select Search	Failure Object Client 00:18:de:2e:36:71 Owner Acknowledged No	Client '00:18:de:2e:36:71' which was associated with AP '00:17:df:a7:50:40', interface '1' is excluded. The reason code is '6(Unknown)'.
	Category Security Created Mar 24, 2008 11:14:08 AM Modified Aug 12, 2008 7:10:06 AM Generated By Controller Severity Minor	Help Client '00:18:de:2e:36:71' which was associated with AP '00:17:df:a7:50:40', interface '1' is excluded. The reason code is '6'.
	Previous Severity Minor Annotations Annotations go here.	Event History Annotations
Alarm Summary         Image: Coverage Hole         0         <	Add	

Figure 8-40 WCS Detailed Client Exclusion Event Screen

# General Guidelines for Cisco Wireless and Network IDS/IPS Integration

General guidelines for deploying wireless and network IDS/IPS include the following:

- Leverage the wireless IDS/IPS features of the Cisco WLC for WLAN-specific threat detection and mitigation.
- Deploy Cisco IPS for general WLAN client threat detection and mitigation.
- Enable Cisco WLC and IPS integration to provide operational personnel with a simple, but effective, threat mitigation tool, offering centralized control and enforcement directly on the access edge.
- Leverage distributed IPS deployments to maximize Cisco WLC and IPS collaboration and IPS collaboration for cross-network threat detection and mitigation.
- Ensure that policy violation events are regularly monitored and reviewed.

# **Additional Information**

# **Cisco WLC and IPS Collaboration Operational Details**

General information related to Cisco WLC and IPS integration that should be considered from an operational perspective includes the following:

- A Cisco IPS host block is defined based on a source IP address.
- A Cisco IPS host block is enforced on a WLC as a MAC-based client exclusion.
- The active host block timeout is defined on the Cisco IPS.
- The client exclusion timeout is defined on the WLC for each WLAN profile.
- A blocked WLAN client reassociating with the WLAN continues to be disconnected as long as a Cisco IPS host block is in place.
- Upon a client exclusion expiring, the WLC will create a new client exclusion as long as a Cisco IPS host block remains in place and the client is still attempting to connect to the WLAN.
- A host block can be bypassed by a blocked client changing their IP address.
- If a blocked client attempts to re-connect to the WLAN with a different IP address, the WLC will block the client, based on their MAC address, as long as the client exclusion is in place.
- By default, a blocked WLAN client attempts to re-connect. The exact behavior of a WLAN client upon repeated disconnection from a WLAN varies depending on the particular WLAN client and possible wireless configuration settings. Some clients may stop attempting to reconnect to a particular WLAN after a certain number of unsuccessful connection attempts.
- Active client exclusions being enforced on a WLC can be viewed by browsing to **Monitor**-> **Wireless** -> **Clients**. The listing shows excluded clients with a status of *Excluded*, even if they are not currently connected.
- Upon a host block being retracted, an active client exclusion corresponding to a retracted host block, defined based on the MAC address of the client, remains in place until expiration of the client exclusion timeout configured for that WLAN profile. Consequently, a previously blocked client may continue to be blocked from connection to the WLAN until the client exclusion timeout expires, even though a host block is no longer in place on the Cisco IPS.
- If a WLAN client connects with a fixed IP address, it may take a while for a WLC to learn the client IP address (the client IP address shows 0.0.0.0 in the interim). The WLC is only able to enforce a host block once the client IP address is known.
- There is a risk of a blocked IP address being reassigned to a different client.
- Source IP spoofing protection must be in place on the network in order for the Cisco IPS to Cisco WLC automated threat mitigation technique to be effective.

**Cisco IPS Deployment Modes** 

One of the key design choices when deploying this functionality is between IDS or IPS mode:

• IDS Mode

Promiscuous mode passive monitoring, whereby traffic is passed to an IDS for analysis through a monitoring port. Upon detection of anomalous behavior, management systems are informed of an event. Operational staff subsequently decide what action, if any, to take in response to the incident.

IPS Mode

Inline mode active monitoring, whereby an IPS is in the data path. The detection capabilities are the same as for an IDS, but an inline configuration provides operational staff with the option to filter malicious traffic on the IPS device itself.

S.

**Note** Since IPS mode is in the data path, it is critical to ensure that a deployment is well designed and architected to ensure that it does not have a negative impact on network performance.

An IPS sensor can generally only be configured to operate in either IDS or IPS mode. A design may, however, require both modes to be deployed; for instance, to provide passive monitoring on some flows and active monitoring on other flows, perhaps on a per-VLAN basis. To enable this scenario to be achieved, a design may use the following:

- Multiple physical platforms, with each individual platform deployed in either IDS or IPS mode.
- A single platform supporting multiple virtual sensors, enabling both IDS and IPS modes on the same platform. This is achieved by configuring some sensors in IDS mode and others in IPS mode. Note that each individual virtual sensor can only be configured to operate in either IDS or IPS mode.

See the product pages for detailed information on the products, platforms and features, as well as deployment options and considerations. For details, refer to Reference Documents, page 8-51.

## **Cisco IPS Block versus Deny Actions**

A Cisco IPS block action, although activated on the IPS, is enforced on a collaborating device. The Cisco IPS relies on this collaborating device to enforce threat mitigation through a localized technique. On a Cisco Unified Wireless Network, the collaborating device in this scenario is the Cisco WLC and the local threat mitigation technique is client exclusion.

In contrast, a Cisco IPS deny action is both created and enforced on the IPS. The IPS itself filters the traffic to mitigate the attack. A deny action does not trigger a WLAN client block on a WLC.

If desired, activation of both a block action and a deny action can be used to enforce threat mitigation both directly on the IPS and through collaboration with another network device, such as a Cisco WLC.



A Cisco IPS must be deployed in inline mode in order for it to be able to directly perform threat mitigation on traffic passing through it.

Γ

## **Cisco IPS and WLC Integration Dependencies**

Collaboration between a Cisco IPS and WLC is dependent upon the software and hardware platforms identified in Table 8-3.

Table 8-3	Cisco IPS and WLC Integration Dependencies

Component	Minimum Software	Hardware
IPS	IPS sensor software release v5.x or later	Cisco IPS 4200 Series Appliances
		Catalyst 6500 Series Intrusion Detection System     Services Module (IDSM-2)
		ASA IPS module (AIP-SSM)
		ISR AIM IPS module (AIM-IPS)
WLC	Cisco Unified Wireless Network v4.0 or later	All Cisco Unified Wireless Network WLAN controllers
LWAPP AP		and access points

Note that Cisco IOS IPS for routing platforms, including the Cisco Integrated Services Routers (ISRs), does not currently support integration with a Cisco WLC for threat mitigation.

## **Test Bed Hardware and Software**

Integration testing was performed and verified between all the IPS and WLC platforms and software releases shown in Table 8-4.

Component	Hardware	Software
IPS	AIM-IPS in ISR 3845	6.1(1)E2
		ISR running IOS v12.4(20)T
	AIP-SSM-20 in ASA 5520	6.0(3)E1
		ASA running 8.0(3)
	IPS 4255	5.1(1)S205.0
WLC	WLC 2106	5.0.148.2
	Wireless Services Module (WiSM) in Cisco Catalyst 6500 Series	5.0.148.2
WCS		5.0.72.0

### Table 8-4 Test Bed Hardware and Software

- Alternative platforms and modes are supported and should provide similar functionality.
- IPS devices were configured in promiscuous mode.
- Cisco WLC and IPS collaboration has previously been validated with WLC version 4.0.206.0 and WCS versions 4.0.96.0 and 5.0.56.0, along with WLC version 4.1.171.0 on a Cisco Catalyst 6500 Series Wireless Services Module (WiSM) with a Cisco IPS 4255 version 5.1(1).

## **Reference Documents**

## **Cisco IPS**

Cisco IPS Portfolio

http://www.cisco.com/go/ips

- Cisco IPS 4200 Series Configuration Examples and TechNotes http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod\_configuration\_examples\_list.htm
- Cisco IPS 4200 Series Configuration Guides http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products\_installation\_and\_configuratio n\_guides\_list.html
- Cisco IPS Tuning Overview (CCO Login required) http://www.cisco.com/en/US/partner/prod/collateral/vpndevc/ps5729/ps5713/ps4077/overview\_c1 7-464691.html

## **Cisco Security Portfolio**

Cisco Security Portfolio

http://www.cisco.com/en/US/products/hw/vpndevc/index.html

## **Cisco Unified Wireless**

- Cisco Wireless Network Security http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking\_solutions\_package.htm 1
- Cisco Wireless Portfolio

http://www.cisco.com/en/US/products/hw/wireless/index.html

• Cisco Wireless LAN Controller and IPS Integration Guide

http://www.cisco.com/en/US/tech/tk722/tk809/technologies\_configuration\_example09186a008073 60fc.shtml

### **General Network Security**

• Network Security Baseline

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline\_Security/securebasebook.html

