CHAPTER 9

CS-MARS Integration for Cisco Unified Wireless

A secure unified network, featuring both wired and wireless access, requires an integrated, defense-in-depth approach to security, including cross-network anomaly detection and correlation that is critical to effective threat detection and mitigation.

This chapter outlines how CS-MARS can be integrated with a Cisco Unified Wireless Network to extend cross-network anomaly detection and correlation to the WLAN, providing network security staff with visibility across all elements of the network.

Software implementation, screenshots, and behavior referenced in this chapter are based on the releases listed in Test Bed Hardware and Software, page 9-24. It is assumed that the reader is already familiar with both CS-MARS and the Cisco Unified Wireless Network.

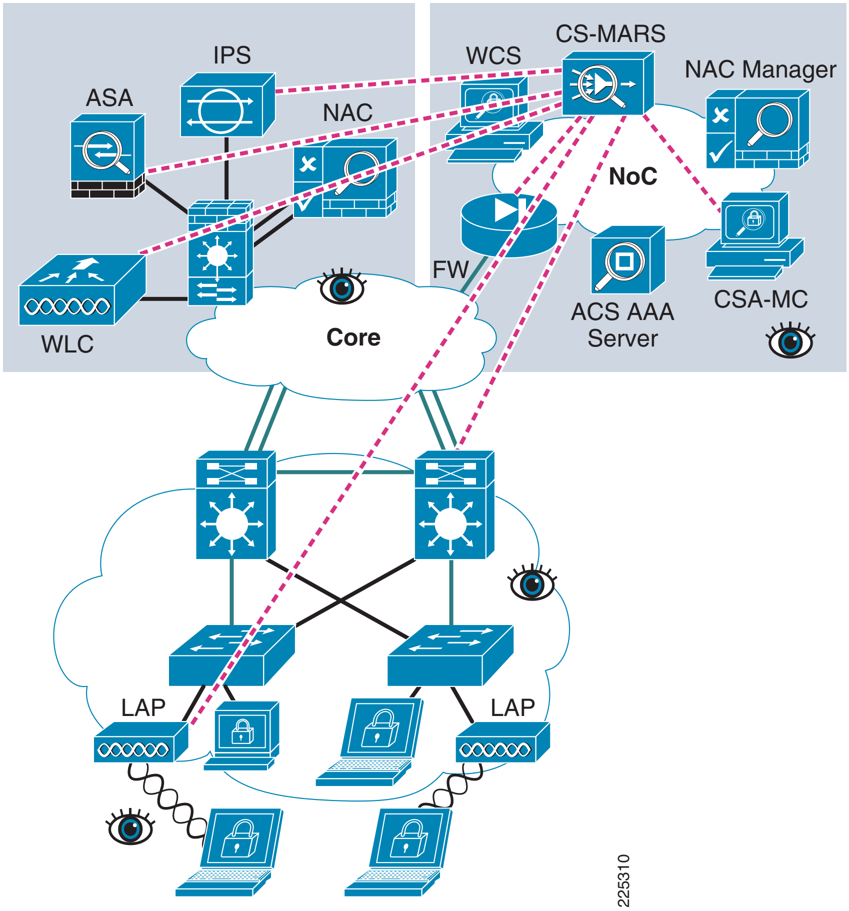
Note This guide addresses only CS-MARS features specific to Cisco Unified Wireless integration.

CS-MARS Cross-Network Security Monitoring

CS-MARS security monitoring combines cross-network intelligence, sophisticated event correlation, and threat validation to effectively identify potential network and application threats.

Network intelligence is gained through the efficient aggregation and correlation of massive amounts of network and security data from devices across the network, including network devices and host applications from Cisco and other vendors. This extensive monitoring enables critical visibility into overall network status, traffic flows, and events. For more information on CS-MARS, refer to Reference Documents, page 9-25.

Figure 9-1 CS-MARS Cross-Network Anomaly Detection and Correlation



Extending CS-MARS Visibility to Cisco Unified Wireless

CS-MARS Release 5.3.2 introduced native support for Cisco Unified Wireless Network devices that extends visibility to the WLAN, integrating WLAN events into its threat detection, investigation, mitigation, and reporting capabilities.

This includes visibility into WLAN events such as:

- WLAN DoS attacks
- Rogue APs
- 802.11 probes
- Ad hoc networks
- Client exclusions and blacklisting
- WLAN operational status

For more information, refer to CS-MARS for Cisco Unified Wireless Features, page 9-13.

CS-MARS is complementary to the WLAN-specific anomaly detection and correlation features offered by the Cisco WLC and Wireless Control System (WCS), offering network security staff an integrated view of the entire network that is critical to cross-network anomaly detection and correlation.

For more information on WCS, refer to Reference Documents, page 9-25.

Implementing CS-MARS and Cisco WLC Integration

Configuring the Cisco WLC

In order for CS-MARS to obtain visibility into events on a Cisco Unified Wireless Network, each Cisco WLC must be configured to send SNMP traps to CS-MARS.

In addition, if CS-MARS discovery of each WLC and its connected LWAPP APs is required, a read-only community string must also be configured on each WLC. This enables CS-MARS to query the WLC and obtain this information.

The configuration steps required to enable CS-MARS and WLC integration are:

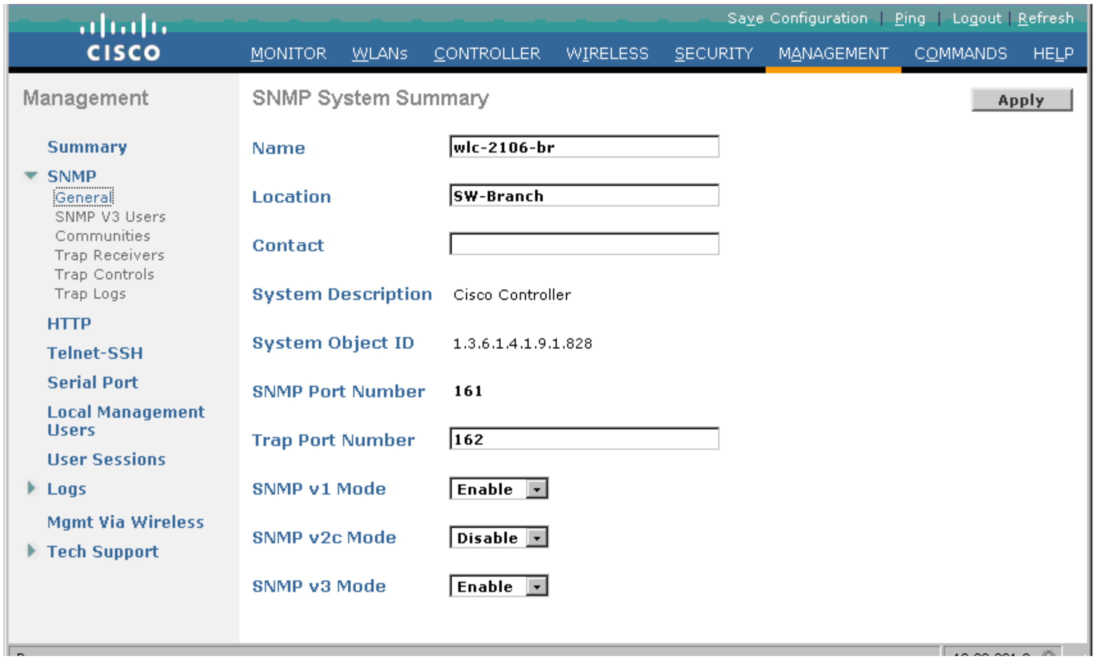
1. Enable SNMP v1 (CS-MARS currently only supports SNMP v1).
2. Define the community settings for use with CS-MARS.
3. Verify that the required SNMP traps are enabled.
4. Define CS-MARS as an SNMP trap receiver.

The following are detailed instructions on how to implement each of these steps:

Step 1 Enable SNMP v1.

On the WLC, go to **Management** -> **SNMP** -> **General**. Verify the general SNMP parameters, set the state box next to SNMP v1 Mode to **Enable** and click **Apply** (see Figure 9-2).

Figure 9-2 Enabling SNMP v1 on a Cisco WLC



SNMP System Summary

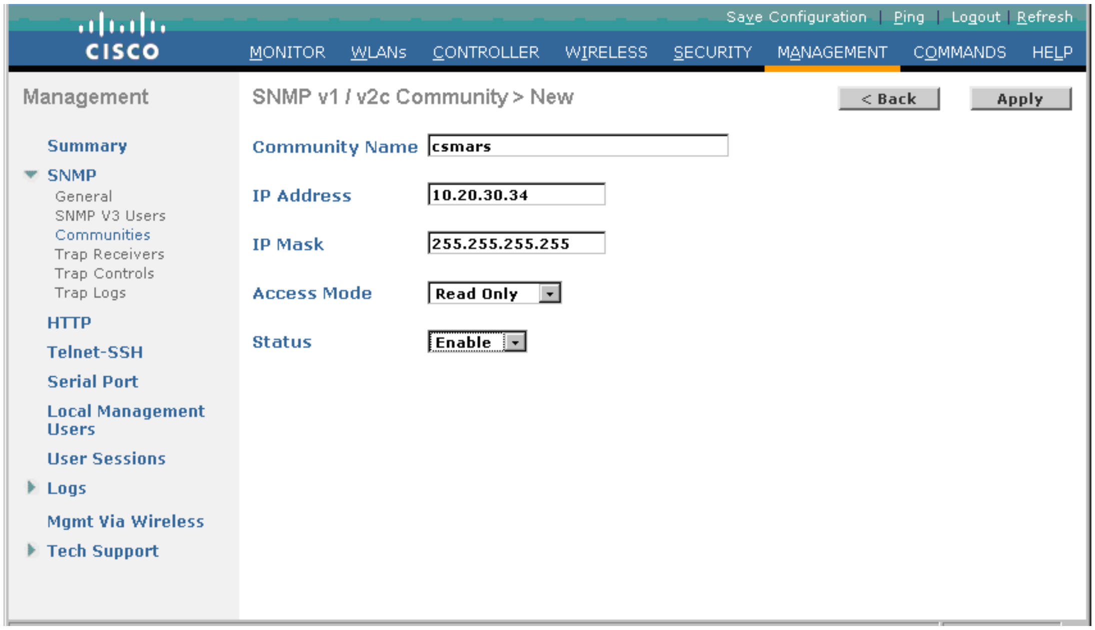
Name	wlc-2106-br
Location	SW-Branch
Contact	
System Description	Cisco Controller
System Object ID	1.3.6.1.4.1.9.1.828
SNMP Port Number	161
Trap Port Number	162
SNMP v1 Mode	Enable
SNMP v2c Mode	Disable
SNMP v3 Mode	Enable

Note SNMP v1 is disabled by default on the WLC.

Step 2 Define the community settings for use with CS-MARS.

On the WLC, go to **Management** -> **SNMP** -> **Communities**. Define a read-only community string for use with CS-MARS and the source IP address and mask of the CS-MARS management station. Set the access mode to **Read Only**, the status to **Enable**, and then click **Apply** (see Figure 9-3).

Figure 9-3 Defining the Community Settings for Use with CS-MARS



SNMP v1 / v2c Community > New

Community Name: csmars

IP Address: 10.20.30.34

IP Mask: 255.255.255.255

Access Mode: Read Only

Status: Enable

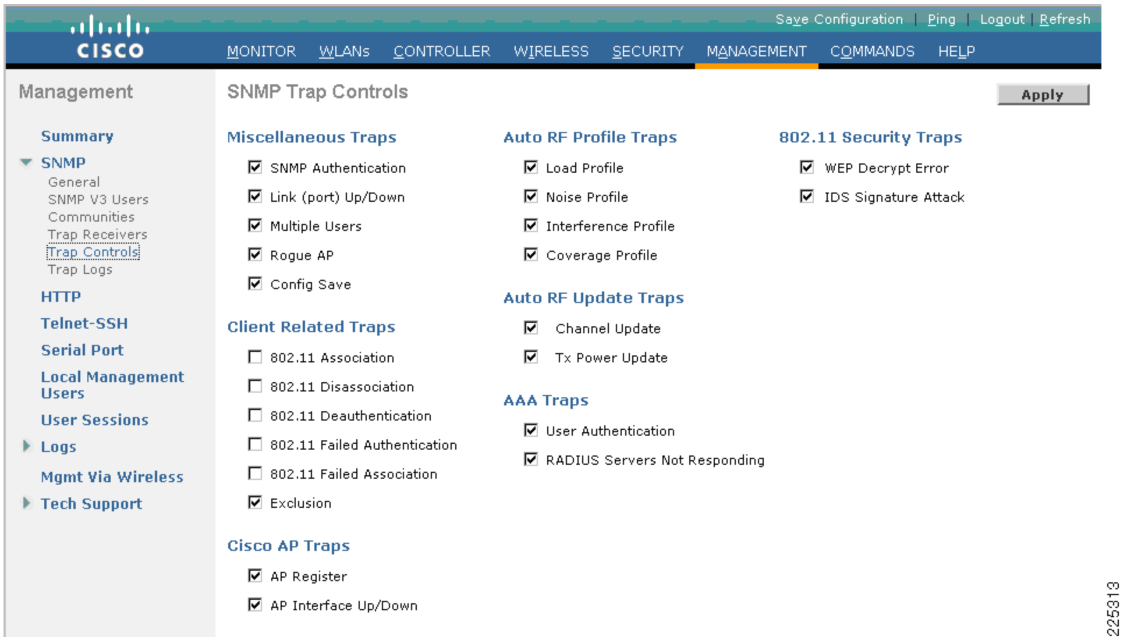
Note the following:

- If the IP address and IP Mask fields are left blank, they default to 0.0.0.0/0.0.0.0, permitting read-only access with this community string to any source IP address.
- It is recommended that access with any particular community string is restricted to only authorized source IP addresses.
- SNMP v1 passes all data in clear text, including the community strings, and is thus vulnerable to sniffing. Customers should review their security policy to determine if additional security techniques, such as IPSec or an out-of-band (OOB) management network, are required to protect SNMP v1 transactions.
- CS-MARS should only be granted read-only access. This is all that is required and ensures that only minimum necessary access privileges are granted, as recommended as a security best practice.

Step 3 Verify that the required SNMP traps are enabled.

On the WLC, go to **Management** -> **SNMP** -> **Trap Controls**. SNMP traps are sent for all events that have their associated checkbox checked. Set the trap controls required for monitoring and click **Apply** (see Figure 9-4).

Figure 9-4 Verifying WLC SNMP Trap Controls



SNMP Trap Controls

Miscellaneous Traps

- ☑ SNMP Authentication
- ☑ Link (port) Up/Down
- ☑ Multiple Users
- ☑ Rogue AP
- ☑ Config Save

Client Related Traps

- □ 802.11 Association
- □ 802.11 Disassociation
- □ 802.11 Deauthentication
- □ 802.11 Failed Authentication
- □ 802.11 Failed Association
- ☑ Exclusion

Cisco AP Traps

- ☑ AP Register
- ☑ AP Interface Up/Down

Auto RF Profile Traps

- ☑ Load Profile
- ☑ Noise Profile
- ☑ Interference Profile
- ☑ Coverage Profile

Auto RF Update Traps

- ☑ Channel Update
- ☑ Tx Power Update

AAA Traps

- ☑ User Authentication
- ☑ RADIUS Servers Not Responding

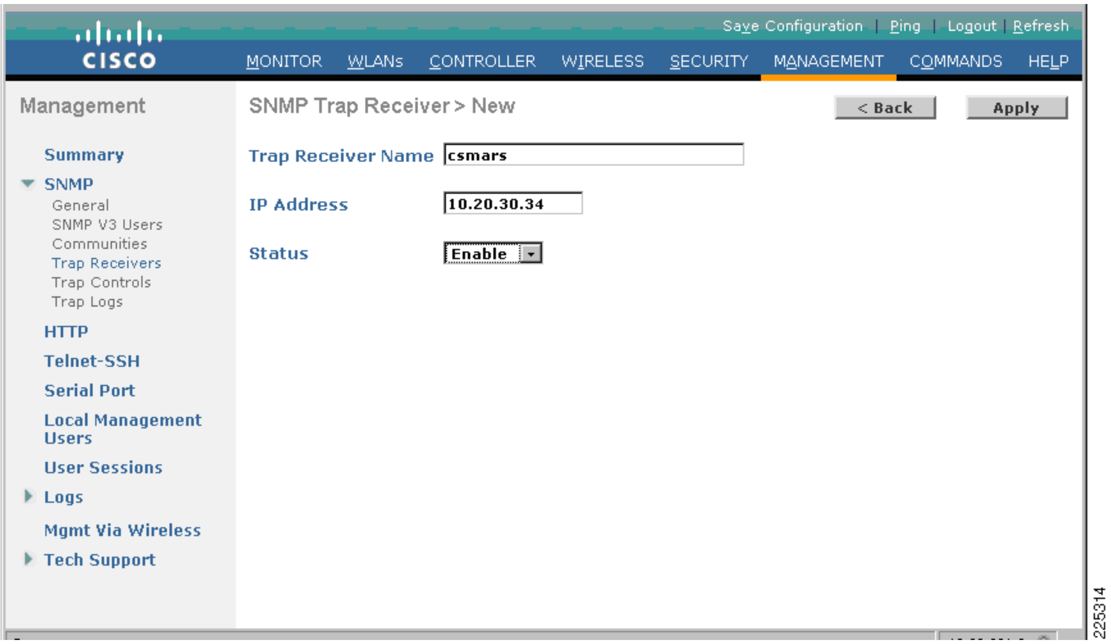
802.11 Security Traps

- ☑ WEP Decrypt Error
- ☑ IDS Signature Attack

Step 4 Define CS-MARS as an SNMP trap receiver.

On the WLC, go to **Management** -> **SNMP** -> **Trap Receivers**. Add a new SNMP trap receiver with the name and IP address of CS-MARS. Set the status to **Enable** and click **Apply** (see Figure 9-5).

Figure 9-5 Defining CS-MARS as an SNMP Trap Receiver



SNMP Trap Receiver > New

Trap Receiver Name: csmars

IP Address: 10.20.30.34

Status: Enable

Configuring CS-MARS

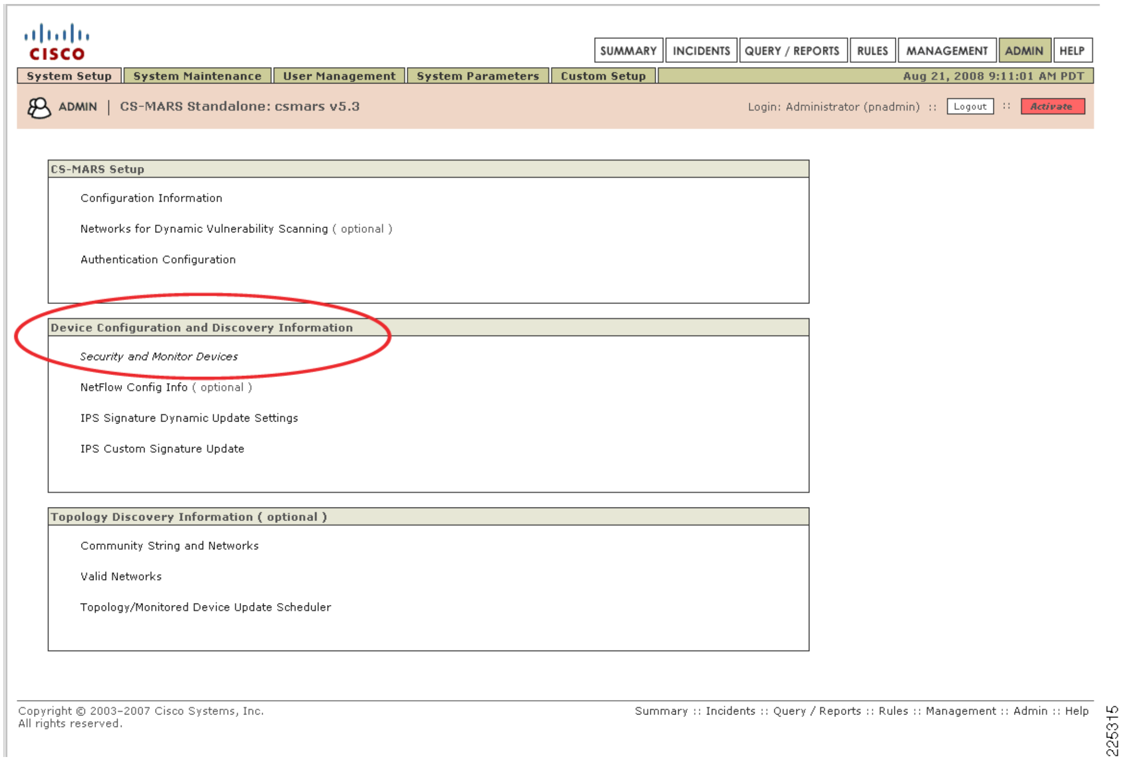
In order for CS-MARS to discover each Cisco WLC and its connected LWAPP APs, each WLC must be defined on CS-MARS. This provides CS-MARS with SNMP read-only access to the device so that it can obtain this and other device-specific information. This is the only configuration required on CS-MARS.

Manually Adding a Cisco WLC

To manually add a Cisco WLC to CS-MARS, complete the following steps:

Step 1 On the CS-MARS GUI, navigate to **ADMIN** -> **System Setup**. In the middle section titled **Device Configuration and Discovery Information**, select **Security and Monitor Devices** (see Figure 9-6).

Figure 9-6 CS-MARS System Setup Screen



Aug 21, 2008 9:11:01 AM PDT

ADMIN | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) ::

CS-MARS Setup

- Configuration Information
- Networks for Dynamic Vulnerability Scanning (optional)
- Authentication Configuration

Device Configuration and Discovery Information

- *Security and Monitor Devices*
- NetFlow Config Info (optional)
- IPS Signature Dynamic Update Settings
- IPS Custom Signature Update

Topology Discovery Information (optional)

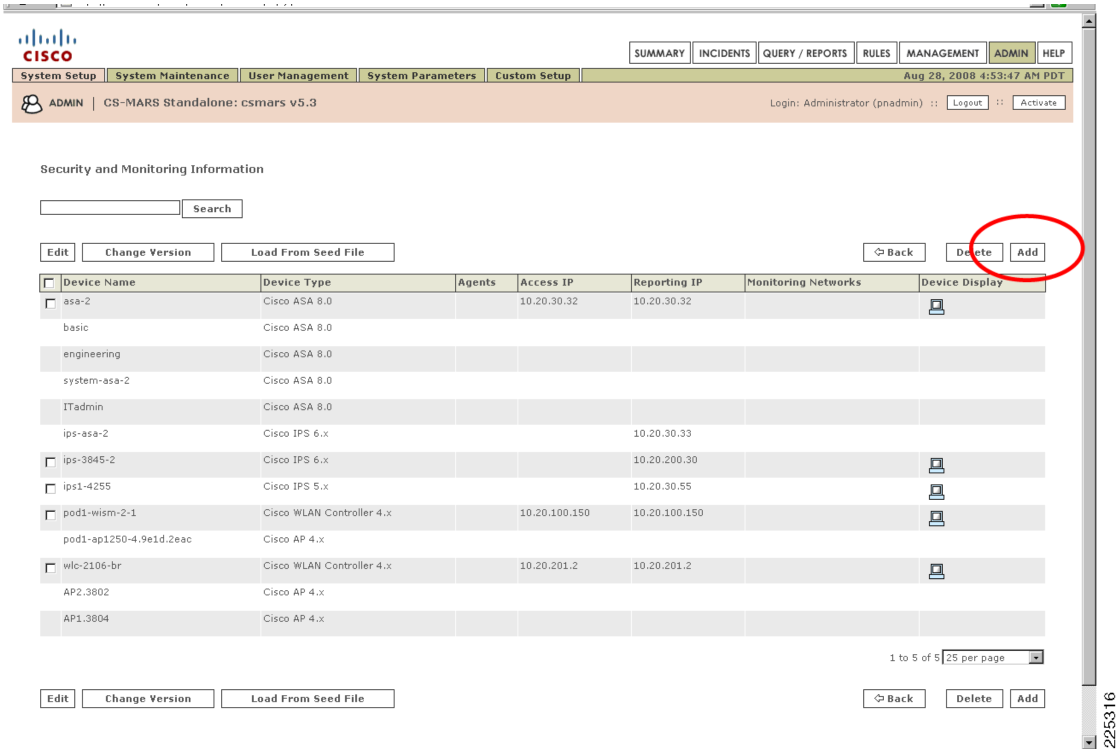
- Community String and Networks
- Valid Networks
- Topology/Monitored Device Update Scheduler

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Step 2 On the Security and Monitoring Information screen, as shown in Figure 9-7, click **Add**.

Figure 9-7 CS-MARS Screen to Add a New Device

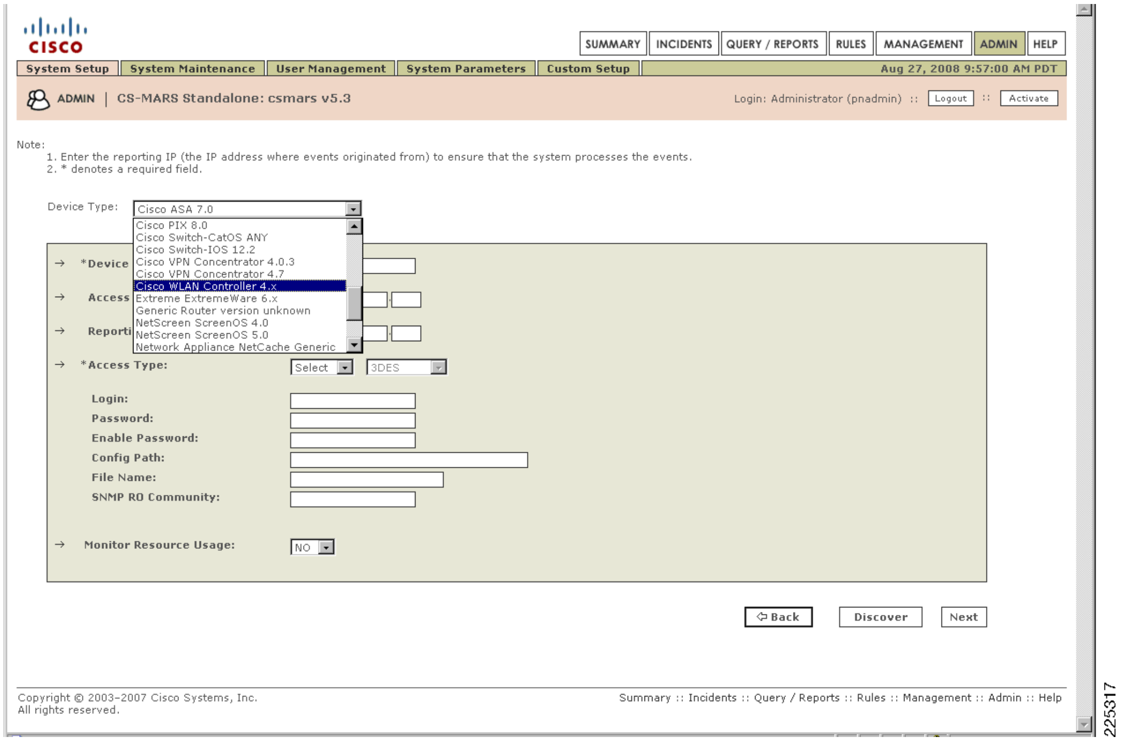


□	Device Name	Device Type	Agents	Access IP	Reporting IP	Monitoring Networks	Device Display
□	asa-2	Cisco ASA 8.0		10.20.30.32	10.20.30.32		💻
	basic	Cisco ASA 8.0					
	engineering	Cisco ASA 8.0					
	system-asa-2	Cisco ASA 8.0					
	ITadmin	Cisco ASA 8.0					
	ips-asa-2	Cisco IPS 6.x			10.20.30.33		
□	ips-3845-2	Cisco IPS 6.x			10.20.200.30		💻
□	ips1-4255	Cisco IPS 5.x			10.20.30.55		💻
□	pod1-wism-2-1	Cisco WLAN Controller 4.x		10.20.100.150	10.20.100.150		💻
	pod1-ap1250-4.9e1d.2eac	Cisco AP 4.x					
□	wlc-2106-br	Cisco WLAN Controller 4.x		10.20.201.2	10.20.201.2		💻
	AP2.3802	Cisco AP 4.x					
	AP1.3804	Cisco AP 4.x					

Step 3 Add a Cisco WLC from the device type drop-down box by scrolling down to and selecting Cisco WLAN Controller 4.x.

Note WLCs running Cisco Unified Wireless Network Software Release 5.x are supported and can be configured as a Cisco WLAN Controller 4.x (see Figure 9-8).

Figure 9-8 Adding a Cisco WLC on CS-MARS



cisco
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
ADMIN
HELP
System Setup
System Maintenance
User Management
System Parameters
Custom Setup
Aug 27, 2008 9:57:00 AM PDT
ADMIN | CS-MARS Standalone: csmars v5.3
Login: Administrator (pnadmin) :: Logout :: Activate
Back
Discover
Next
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help
225317

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco ASA 7.0

Cisco PIX 8.0
Cisco Switch-CatOS ANY
Cisco Switch-IOS 12.2
Cisco VPN Concentrator 4.0.3
Cisco VPN Concentrator 4.7
Cisco WLAN Controller 4.x
Extreme ExtremeWare 6.x
Generic Router version unknown
NetScreen ScreenOS 4.0
NetScreen ScreenOS 5.0
Network Appliance NetCache Generic

*Device
Access
Reporti
*Access Type: Select 3DES
Login:
Password:
Enable Password:
Config Path:
File Name:
SNMP RO Community:
Monitor Resource Usage: NO

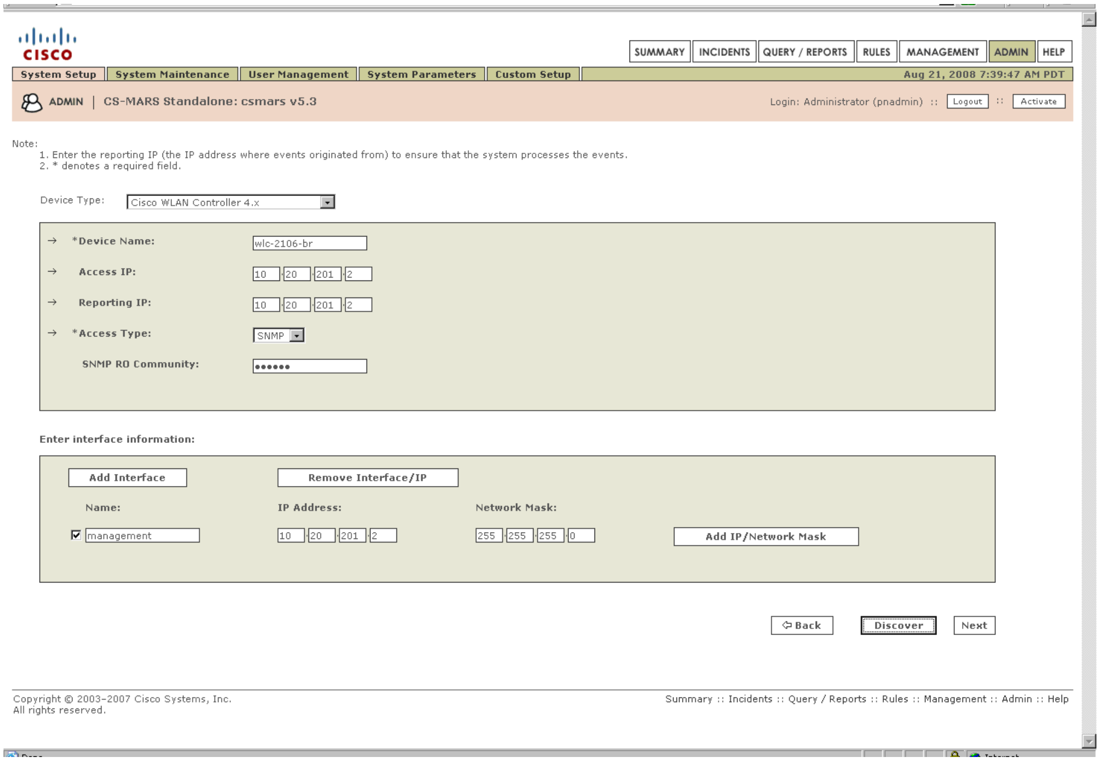
Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

The device entry fields change to reflect this device type and the WLC can be defined by entering this information:

- Device Name—WLC name
- Access IP—WLC IP address to be used for SNMP read-only access
- Reporting IP—WLC management interface IP address used as the source IP address for SNMP traps
- Access Type—Select SNMP (the only option available in the drop-down box)
- SNMP RO Community—SNMP community name defined on the WLC for use with CS-MARS
- Interface Information—WLC management interface IP address and network mask

Step 4 Once all the WLC information has been defined, click **Discover** (see Figure 9-9).

Figure 9-9 Defining a Cisco WLC on CS-MARS



Aug 21, 2008 7:39:47 AM PDT

ADMIN | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin)

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco WLAN Controller 4.x

*Device Name: wlc-2106-br
Access IP: 10.20.201.2
Reporting IP: 10.20.201.2
*Access Type: SNMP
SNMP RO Community: ●●●●●●

Enter interface information:

Name:	IP Address:	Network Mask:
☑ management	10.20.201.2	255.255.255.0

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

Note the following:

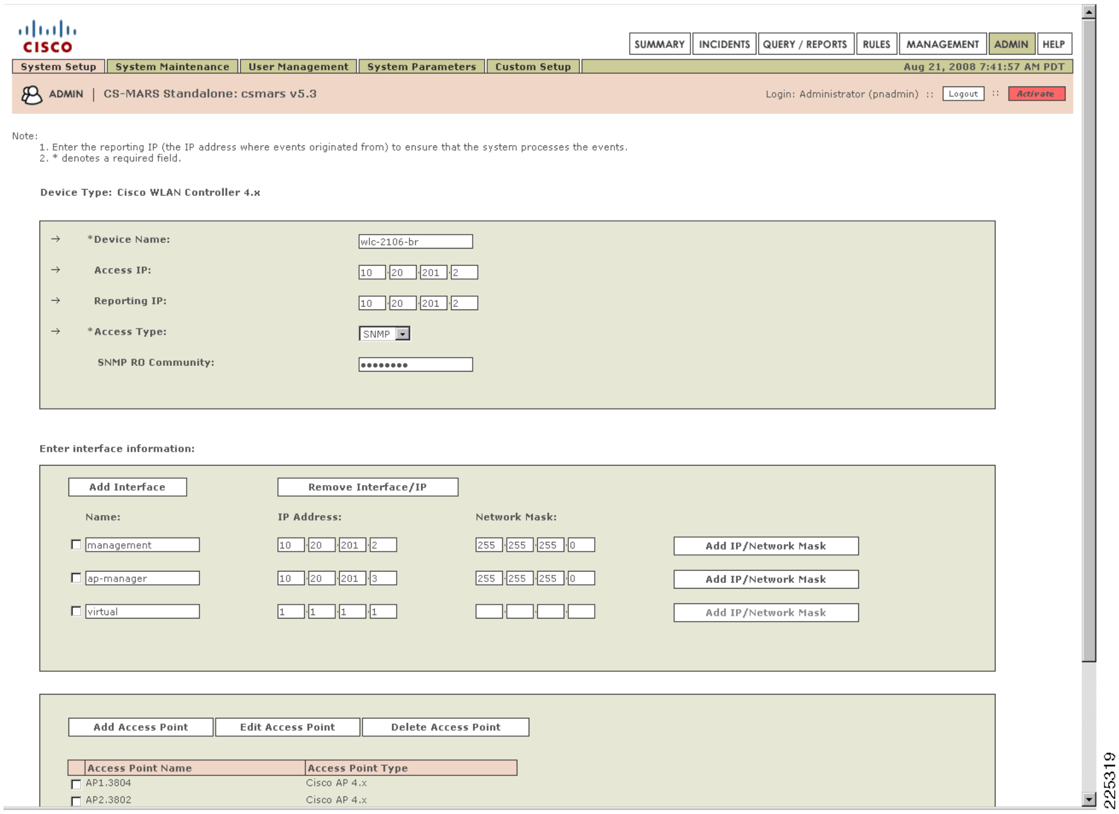
- The WLC management interface must be defined. Other interfaces will automatically be added upon successful discovery of the device.
- SNMP v1 access must already be enabled on the WLC for discovery to be successful (see Configuring the Cisco WLC, page 9-3).

Upon successful discovery of the WLC, any other interfaces and any currently associated access points are discovered and populated on the CS-MARS interface (see Figure 9-10).

If discovery is not successful, verify that:

- CS-MARS can ping the WLC.
- SNMP v1 is enabled on the WLC.
- SNMP community string defined on CS-MARS matches that defined on the WLC for CS-MARS.
- SNMP community string for CS-MARS is enabled on the WLC.
- CS-MARS source IP address matches that defined on the WLC.

Figure 9-10 Successful Cisco WLC Discovery on CS-MARS



Aug 21, 2008 7:41:57 AM PDT

ADMIN | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin)

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco WLAN Controller 4.x

→ *Device Name:	wlc-2106-br
→ Access IP:	10.20.201.2
→ Reporting IP:	10.20.201.2
→ *Access Type:	SNMP
SNMP RO Community:	••••••••

Enter interface information:

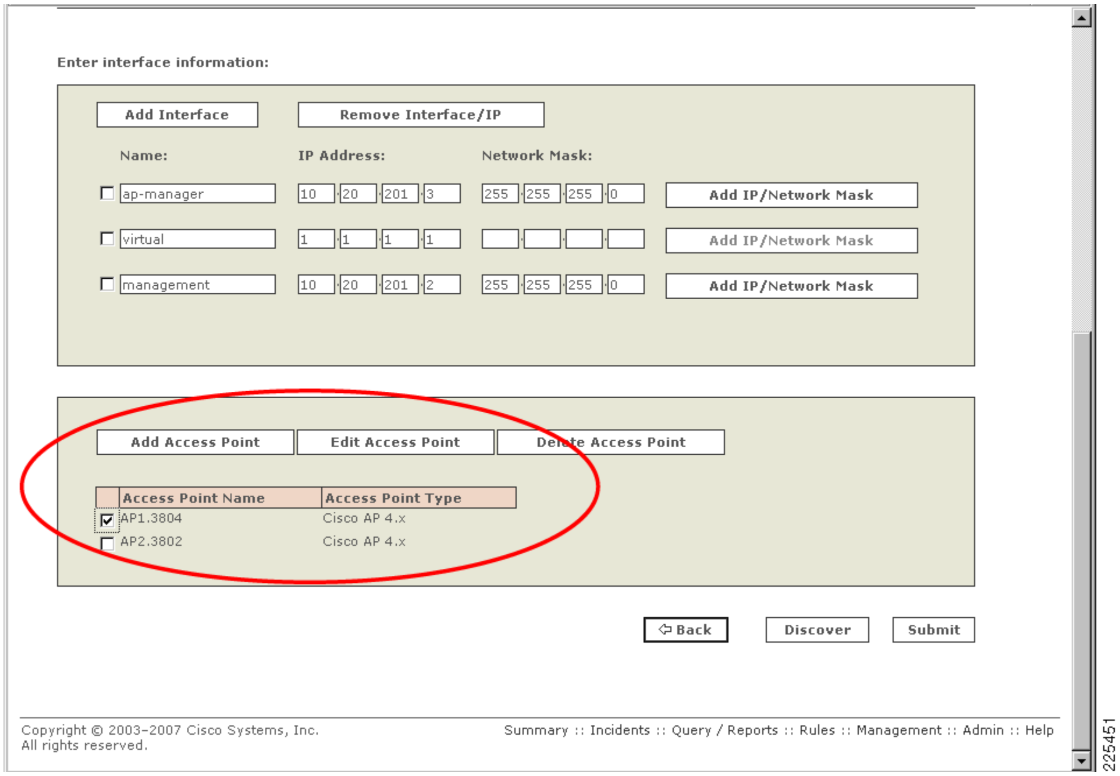
Name:	IP Address:	Network Mask:
□ management	10.20.201.2	255.255.255.0
□ ap-manager	10.20.201.3	255.255.255.0
□ virtual	1.1.1.1	...

	Access Point Name	Access Point Type
□	AP1.3804	Cisco AP 4.x
□	AP2.3802	Cisco AP 4.x

Step 5 Select **Submit** and then **Activate** the configuration.

Note that CS-MARS identifies an access point (AP) based on its MAC address rather than the typical Access IP/Reporting IP. To view the MAC address of a particular AP, scroll to the bottom of the WLC device page, check the box next to the name of an AP and click **Edit Access Point** (see Figure 9-12).

Figure 9-11 Viewing a Cisco LWAPP Access Point on CS-MARS



Enter interface information:

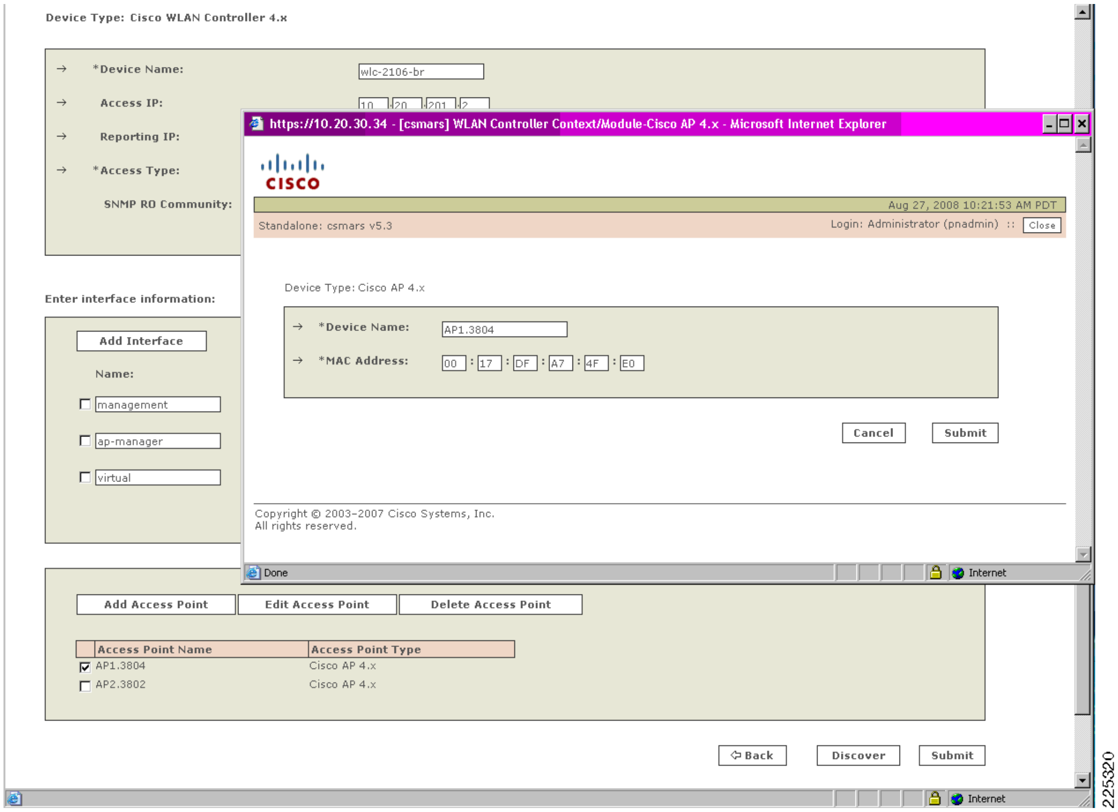
	Name:	IP Address:	Network Mask:
□	ap-manager	10 . 20 . 201 . 3	255 . 255 . 255 . 0
□	virtual	1 . 1 . 1 . 1	. . .
□	management	10 . 20 . 201 . 2	255 . 255 . 255 . 0

	Access Point Name	Access Point Type
☑	AP1.3804	Cisco AP 4.x
□	AP2.3802	Cisco AP 4.x

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

The AP device name and MAC address is subsequently displayed (see Figure 9-12).

Figure 9-12 Cisco LWAPP Access Point as a Device on CS-MARS



Device Type: Cisco WLAN Controller 4.x

→ *Device Name: wlc-2106-br

→ Access IP: 10 . 20 . 201 . 2

→ Reporting IP:

→ *Access Type:

SNMP RO Community:

Enter interface information:

Name:

☐ management

☐ ap-manager

☐ virtual

	Access Point Name	Access Point Type
☑	AP1.3804	Cisco AP 4.x
☐	AP2.3802	Cisco AP 4.x

https://10.20.30.34 - [csmars] WLAN Controller Context/Module-Cisco AP 4.x - Microsoft Internet Explorer

Aug 27, 2008 10:21:53 AM PDT

Standalone: csmars v5.3 Login: Administrator (pnadmin) :: Close

Device Type: Cisco AP 4.x

→ *Device Name: AP1.3804

→ *MAC Address: 00 : 17 : DF : A7 : 4F : E0

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Note The MAC address of access points must be unique to enable accurate event logging.

For more information on how CS-MARS parses events from Cisco LWAPP APs, refer to CS-MARS WLAN AP Event Parsing, page 9-23.

CS-MARS for Cisco Unified Wireless Features

This section provides a brief overview of the CS-MARS features to support Cisco Unified Wireless.

More information on the CS-MARS wireless LAN features is available in the *CS-MARS User Guide* (see Reference Documents, page 9-25).

WLAN Events

CS-MARS support for Cisco Unified Wireless devices includes visibility into WLAN events such as:

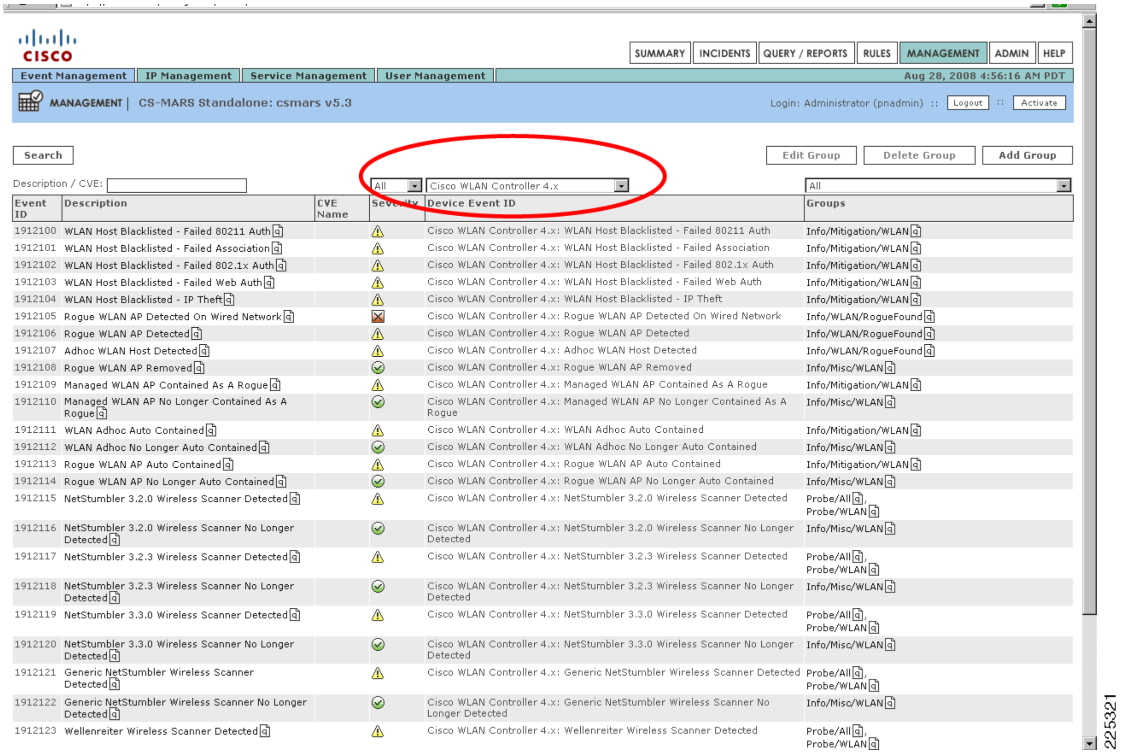
- WLAN DoS attacks
- Rogue APs
- 802.11 probes
- Ad hoc networks
- Client exclusions/blacklisting
- WLAN operational status

To view all the WLAN events parsed by CS-MARS:

Step 1 Navigate to **MANAGEMENT** -> **Event Management**.

Step 2 Select Cisco WLAN Controller 4.x from the pull down menu to review all the WLC events (see Figure 9-13).

Figure 9-13 Sample Subset of CS-MARS WLAN Events



Description / CVE:

All | Cisco WLAN Controller 4.x | All

Event ID	Description	CVE Name	Severity	Device Event ID	Groups
1912100	WLAN Host Blacklisted - Failed 80211 Auth		⚠	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed 80211 Auth	Info/Mitigation/WLAN
1912101	WLAN Host Blacklisted - Failed Association		⚠	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed Association	Info/Mitigation/WLAN
1912102	WLAN Host Blacklisted - Failed 802.1x Auth		⚠	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed 802.1x Auth	Info/Mitigation/WLAN
1912103	WLAN Host Blacklisted - Failed Web Auth		⚠	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed Web Auth	Info/Mitigation/WLAN
1912104	WLAN Host Blacklisted - IP Theft		⚠	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - IP Theft	Info/Mitigation/WLAN
1912105	Rogue WLAN AP Detected On Wired Network		☒	Cisco WLAN Controller 4.x: Rogue WLAN AP Detected On Wired Network	Info/WLAN/RogueFound
1912106	Rogue WLAN AP Detected		⚠	Cisco WLAN Controller 4.x: Rogue WLAN AP Detected	Info/WLAN/RogueFound
1912107	Adhoc WLAN Host Detected		⚠	Cisco WLAN Controller 4.x: Adhoc WLAN Host Detected	Info/WLAN/RogueFound
1912108	Rogue WLAN AP Removed		✓	Cisco WLAN Controller 4.x: Rogue WLAN AP Removed	Info/Misc/WLAN
1912109	Managed WLAN AP Contained As A Rogue		⚠	Cisco WLAN Controller 4.x: Managed WLAN AP Contained As A Rogue	Info/Mitigation/WLAN
1912110	Managed WLAN AP No Longer Contained As A Rogue		✓	Cisco WLAN Controller 4.x: Managed WLAN AP No Longer Contained As A Rogue	Info/Misc/WLAN
1912111	WLAN Adhoc Auto Contained		⚠	Cisco WLAN Controller 4.x: WLAN Adhoc Auto Contained	Info/Mitigation/WLAN
1912112	WLAN Adhoc No Longer Auto Contained		✓	Cisco WLAN Controller 4.x: WLAN Adhoc No Longer Auto Contained	Info/Misc/WLAN
1912113	Rogue WLAN AP Auto Contained		⚠	Cisco WLAN Controller 4.x: Rogue WLAN AP Auto Contained	Info/Mitigation/WLAN
1912114	Rogue WLAN AP No Longer Auto Contained		✓	Cisco WLAN Controller 4.x: Rogue WLAN AP No Longer Auto Contained	Info/Misc/WLAN
1912115	NetStumbler 3.2.0 Wireless Scanner Detected		⚠	Cisco WLAN Controller 4.x: NetStumbler 3.2.0 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912116	NetStumbler 3.2.0 Wireless Scanner No Longer Detected		✓	Cisco WLAN Controller 4.x: NetStumbler 3.2.0 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912117	NetStumbler 3.2.3 Wireless Scanner Detected		⚠	Cisco WLAN Controller 4.x: NetStumbler 3.2.3 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912118	NetStumbler 3.2.3 Wireless Scanner No Longer Detected		✓	Cisco WLAN Controller 4.x: NetStumbler 3.2.3 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912119	NetStumbler 3.3.0 Wireless Scanner Detected		⚠	Cisco WLAN Controller 4.x: NetStumbler 3.3.0 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912120	NetStumbler 3.3.0 Wireless Scanner No Longer Detected		✓	Cisco WLAN Controller 4.x: NetStumbler 3.3.0 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912121	Generic NetStumbler Wireless Scanner Detected		⚠	Cisco WLAN Controller 4.x: Generic NetStumbler Wireless Scanner Detected	Probe/All, Probe/WLAN
1912122	Generic NetStumbler Wireless Scanner No Longer Detected		✓	Cisco WLAN Controller 4.x: Generic NetStumbler Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912123	Wellenreiter Wireless Scanner Detected		⚠	Cisco WLAN Controller 4.x: Wellenreiter Wireless Scanner Detected	Probe/All, Probe/WLAN

This screen presents all the events related to Cisco WLAN controllers that CS-MARS natively supports.

Event Groups Featuring WLAN Events

CS-MARS correlates WLAN events into WLAN-specific and general event groups, as outlined in Table 9-1.

Table 9-1 Event Groups

Event Group Type	Event Group
DoS	DoS/All DoS/Network/WLAN
Informational	Info/High Usage/Network Device Info/Misc/WLAN Info/Mitigation/WLAN Info/WLAN/RogueFound
Operational	OperationalError/WLAN OperationalStatusChange/WLAN
Penetration	Penetrate/All Penetrate/GuessPassword/All Penetrate/GuessPassword/System/Non-root Penetrate/SpoofIdentity/Misc

In CS-MARS queries and reports, the Event Group is represented as “Event Type”.

Rules Based on WLAN Events

CS-MARS features the WLAN-specific inspection rules shown in Table 9-2.

Table 9-2 Rules Based on WLAN Events

CS-MARS Rule	CS-MARS Rule Group
System Rule: Operational Issue: WLAN	System: Operational Issue
System Rule: Rogue WLAN AP Detected	System: Operational Issue
System Rule: WLAN DoS Attack Detected	System: Network Attacks and DoS

These rules are enabled by default and integrated into existing rule groups.

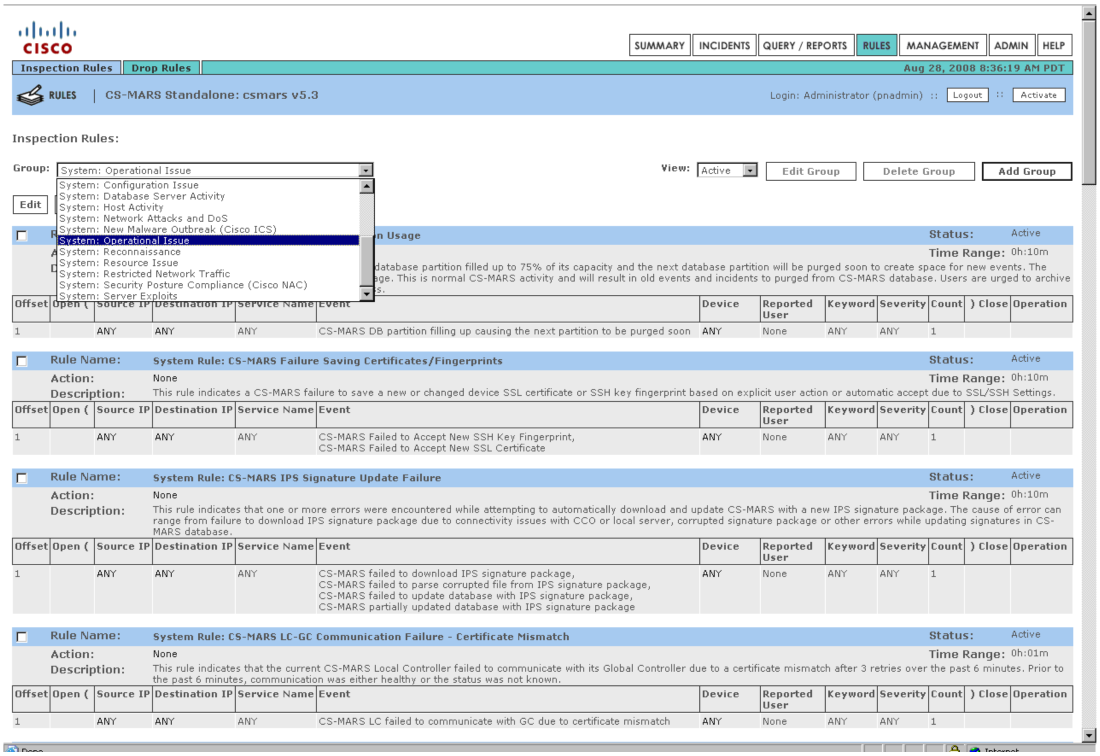
To view the details of a CS-MARS rule:

Step 1 Navigate to **RULES**.

Step 2 Scroll down the list to find the rule.

If you know which Rule Group a rule belongs to, you can filter the list by selecting the appropriate Rule Group in the drop-down box next to **Group** (see Figure 9-14).

Figure 9-14 Viewing CS-MARS Rules by Rule Group



Aug 28, 2008 8:36:19 AM PDT

RULES | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) ::

Inspection Rules:

Group: System: Operational Issue

System: Configuration Issue
System: Database Server Activity
System: Host Activity
System: Network Attacks and DoS
System: New Malware Outbreak (Cisco ICS)
System: Operational Issue
System: Reconnaissance
System: Resource Issue
System: Restricted Network Traffic
System: Security Posture Compliance (Cisco NAC)
System: Server Exploits

View: Active

☐ R… …n Usage Status: Active
A… Time Range: 0h:10m
D… …database partition filled up to 75% of its capacity and the next database partition will be purged soon to create space for new events. The …age. This is normal CS-MARS activity and will result in old events and incidents to purged from CS-MARS database. Users are urged to archive …s.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	CS-MARS DB partition filling up causing the next partition to be purged soon	ANY	None	ANY	ANY	1		

☐ Rule Name: System Rule: CS-MARS Failure Saving Certificates/Fingerprints Status: Active
Action: None Time Range: 0h:10m
Description: This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS Failed to Accept New SSL Certificate	ANY	None	ANY	ANY	1		

☐ Rule Name: System Rule: CS-MARS IPS Signature Update Failure Status: Active
Action: None Time Range: 0h:10m
Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	CS-MARS failed to download IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS partially updated database with IPS signature package	ANY	None	ANY	ANY	1		

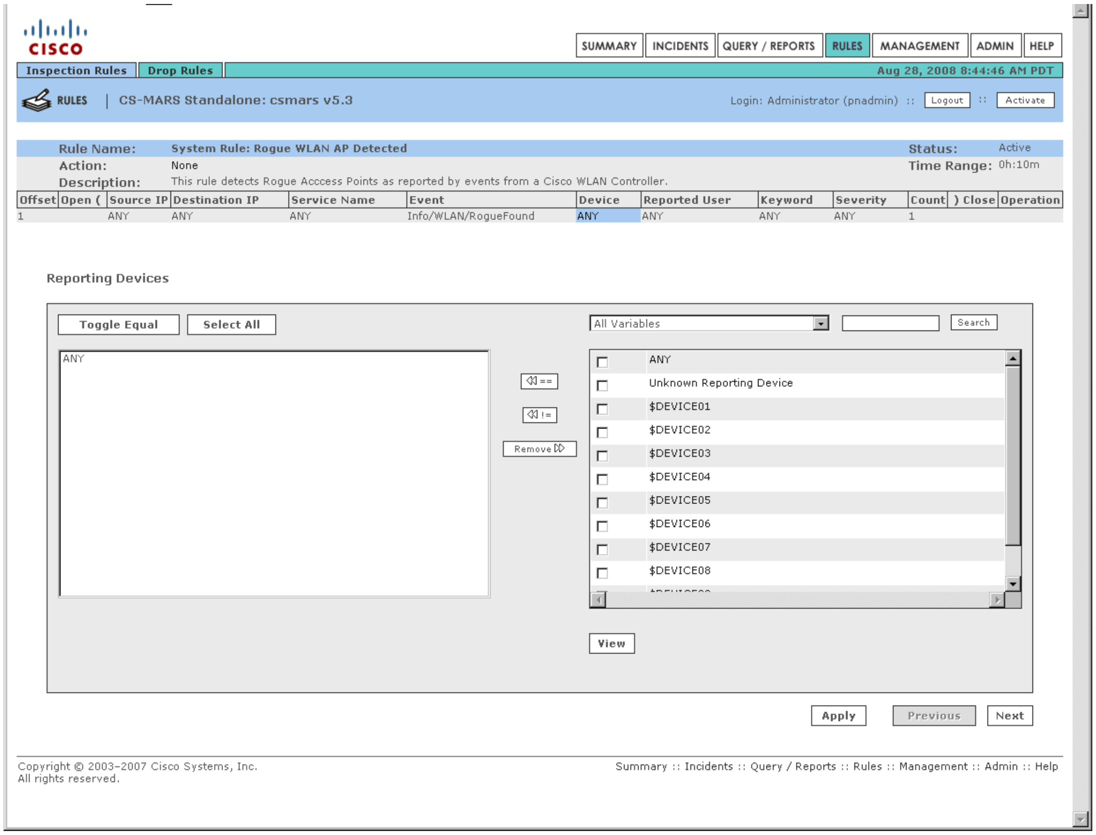
☐ Rule Name: System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch Status: Active
Action: None Time Range: 0h:01m
Description: This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	CS-MARS LC failed to communicate with GC due to certificate mismatch	ANY	None	ANY	ANY	1		

The details of a particular rule can be viewed by selecting that rule and then clicking **Edit**.

As an example, the default details of the rule **System Rule: Rogue WLAN AP Detected** are shown in Figure 9-15.

Figure 9-15 CS-MARS Rule Rogue WLAN AP Detected



Aug 28, 2008 8:44:46 AM PDT

RULES | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) ::

Rule Name: System Rule: Rogue WLAN AP Detected

Status: Active

Action: None

Time Range: 0h:10m

Description: This rule detects Rogue Acccess Points as reported by events from a Cisco WLAN Controller.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	ANY	1		

Reporting Devices

ANY

□ ANY
□ Unknown Reporting Device
□ $DEVICE01
□ $DEVICE02
□ $DEVICE03
□ $DEVICE04
□ $DEVICE05
□ $DEVICE06
□ $DEVICE07
□ $DEVICE08

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Queries and Reports Featuring WLAN Events

CS-MARS features WLAN-specific queries and reports, including:

- WLAN DoS Attacks Detected
- WLAN Probes Detected
- WLAN Rogue AP or Adhoc Hosts Detected
- WLAN Successful Mitigations

WLAN events are also integrated into existing queries and reports, as appropriate, for example:

- Network Attacks and DoS
- Reconnaissance
- Operational Issue

Running a Query on WLAN Events

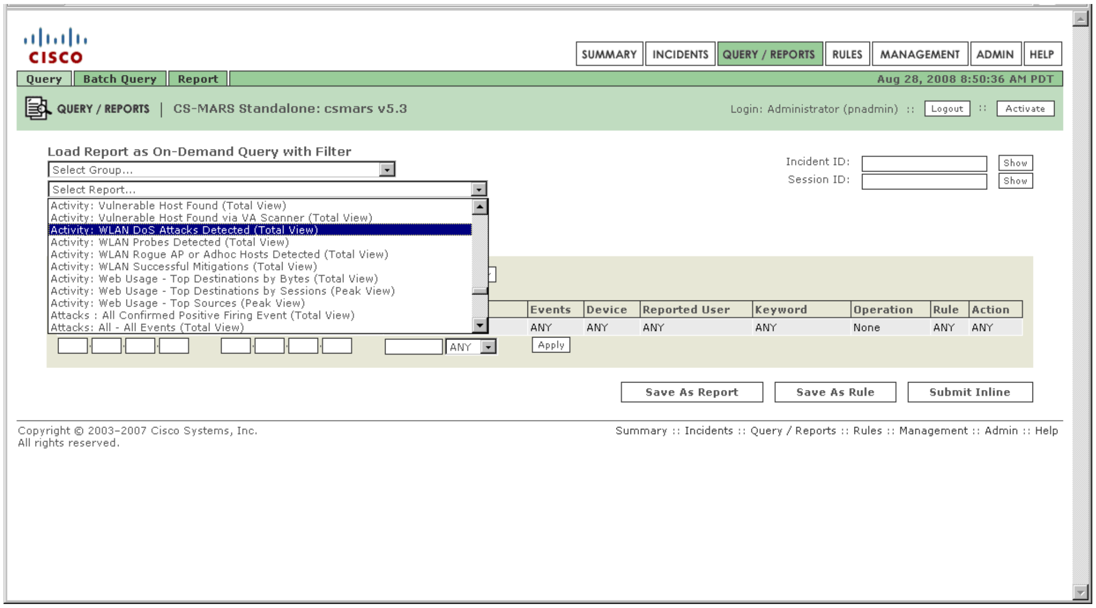
To run a query on particular WLAN-specific events:

Step 1 Navigate to **QUERY/REPORTS**.

Step 2 From the drop-down box **Select Report…**, select the desired WLAN-specific report.

If you know which Report Group a report belongs to, you can filter the list by selecting the appropriate Report Group in the drop-down box **Select Group…** (see Figure 9-16).

Figure 9-16 CS-MARS WLAN-Specific Reports



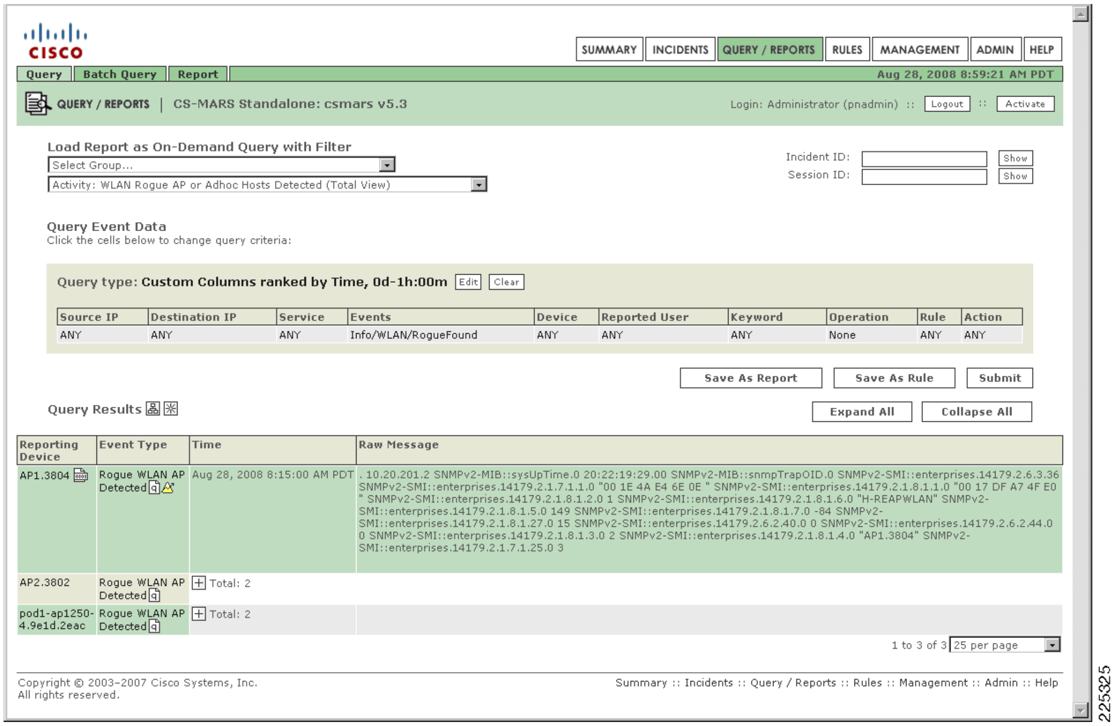
Activity: Vulnerable Host Found (Total View)
Activity: Vulnerable Host Found via VA Scanner (Total View)
Activity: WLAN DoS Attacks Detected (Total View)
Activity: WLAN Probes Detected (Total View)
Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View)
Activity: WLAN Successful Mitigations (Total View)
Activity: Web Usage - Top Destinations by Bytes (Total View)
Activity: Web Usage - Top Destinations by Sessions (Peak View)
Activity: Web Usage - Top Sources (Peak View)
Attacks : All Confirmed Positive Firing Event (Total View)
Attacks: All - All Events (Total View)

Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	None	ANY	ANY

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

Ensure the query timeframe is as required (shown here for the last one hour interval) and click **Submit Inline** (see Figure 9-17).

Figure 9-17 Sample CS-MARS Rogue WLAN AP Report



Aug 28, 2008 8:59:21 AM PDT

QUERY / REPORTS | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) ::

Load Report as On-Demand Query with Filter

Select Group...

Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View)

Incident ID:

Session ID:

Query Event Data

Click the cells below to change query criteria:

Query type: Custom Columns ranked by Time, 0d-1h:00m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	None	ANY	ANY

Query Results

Reporting Device	Event Type	Time	Raw Message
AP1.3804	Rogue WLAN AP Detected	Aug 28, 2008 8:15:00 AM PDT	. 10.20.201.2 SNMPv2-MIB::sysUpTime.0 20:22:19:29.00 SNMPv2-MIB::snmpTrapOID.0 SNMPv2-SMI::enterprises.14179.2.6.3.36 SNMPv2-SMI::enterprises.14179.2.1.7.1.1.0 "00 1E 4A E4 6E 0E " SNMPv2-SMI::enterprises.14179.2.1.8.1.1.0 "00 17 DF A7 4F E0 " SNMPv2-SMI::enterprises.14179.2.1.8.1.2.0 1 SNMPv2-SMI::enterprises.14179.2.1.8.1.6.0 "H-REAPWLAN" SNMPv2-SMI::enterprises.14179.2.1.8.1.5.0 149 SNMPv2-SMI::enterprises.14179.2.1.8.1.7.0 -84 SNMPv2-SMI::enterprises.14179.2.1.8.1.27.0 15 SNMPv2-SMI::enterprises.14179.2.6.2.40.0 0 SNMPv2-SMI::enterprises.14179.2.6.2.44.0 0 SNMPv2-SMI::enterprises.14179.2.1.8.1.3.0 2 SNMPv2-SMI::enterprises.14179.2.1.8.1.4.0 "AP1.3804" SNMPv2-SMI::enterprises.14179.2.1.7.1.25.0 3
AP2.3802	Rogue WLAN AP Detected	⊞ Total: 2	
pod1-ap1250-4.9e1d.2eac	Rogue WLAN AP Detected	⊞ Total: 2	

1 to 3 of 3 25 per page

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Generating a Report on WLAN Events

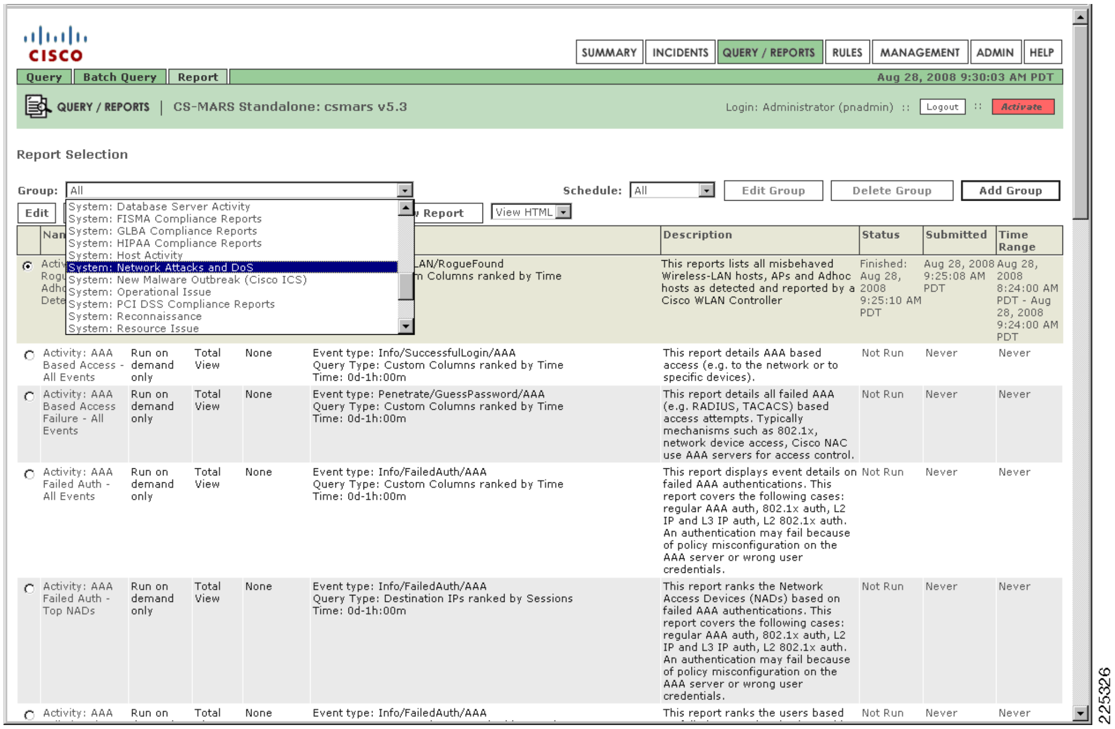
Events that have been correlated into event sets can be expanded to view the individual events and their associated raw message.

To generate a report on particular WLAN-specific events:

Step 1 Navigate to **QUERY/REPORTS** -> **Report**.

Step 2 From the drop-down box **Group --Report Groups -**, select, the desired Report Group (see Figure 9-18).

Figure 9-18 Selecting a CS-MARS Report by Report Group


SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
ADMIN
HELP
Query
Batch Query
Report
QUERY / REPORTS
Logout
Activate
Edit
Report
Edit Group
Delete Group
Add Group
System: Database Server Activity
System: FISMA Compliance Reports
System: GLBA Compliance Reports
System: HIPAA Compliance Reports
System: Host Activity
System: Network Attacks and DoS
System: New Malware Outbreak (Cisco ICS)
System: Operational Issue
System: PCI DSS Compliance Reports
System: Reconnaissance
System: Resource Issue
225326

Aug 28, 2008 9:30:03 AM PDT

CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) ::

Report Selection

Group: All

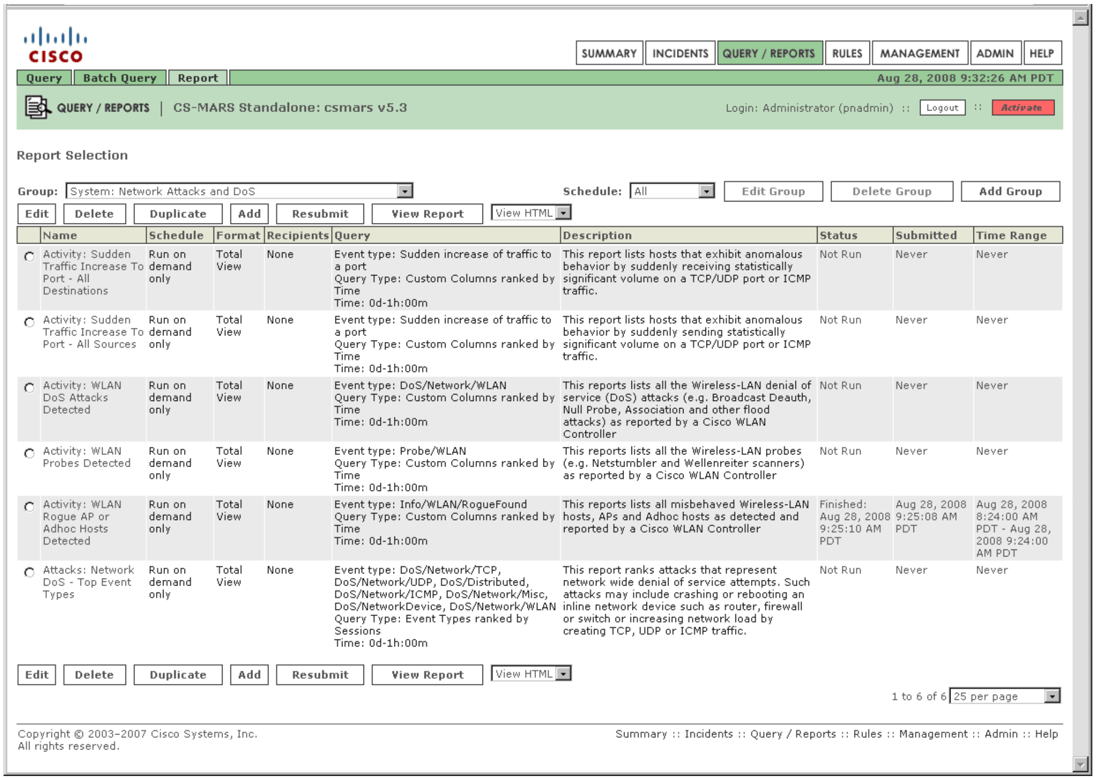
Schedule: All

View HTML

	Nam					Description	Status	Submitted	Time Range
●	Acti Rogu Adhc Dete				LAN/RogueFound m Columns ranked by Time	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT
○	Activity: AAA Based Access - All Events	Run on demand only	Total View	None	Event type: Info/SuccessfulLogin/AAA Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report details AAA based access (e.g. to the network or to specific devices).	Not Run	Never	Never
○	Activity: AAA Based Access Failure - All Events	Run on demand only	Total View	None	Event type: Penetrate/GuessPassword/AAA Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.	Not Run	Never	Never
○	Activity: AAA Failed Auth - All Events	Run on demand only	Total View	None	Event type: Info/FailedAuth/AAA Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.	Not Run	Never	Never
○	Activity: AAA Failed Auth - Top NADs	Run on demand only	Total View	None	Event type: Info/FailedAuth/AAA Query Type: Destination IPs ranked by Sessions Time: 0d-1h:00m	This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.	Not Run	Never	Never
○	Activity: AAA	Run on	Total	None	Event type: Info/FailedAuth/AAA	This report ranks the users based	Not Run	Never	Never

The reports available within that Report Group are then displayed (see Figure 9-19).

Figure 9-19 CS-MARS Network Attacks and DoS Report Group


CISCO
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
ADMIN
HELP
Query
Batch Query
Report
Aug 28, 2008 9:32:26 AM PDT
QUERY / REPORTS | CS-MARS Standalone: csmars v5.3
Login: Administrator (pnadmin) :: Logout :: Activate

Report Selection

Group: System: Network Attacks and DoS   Schedule: All

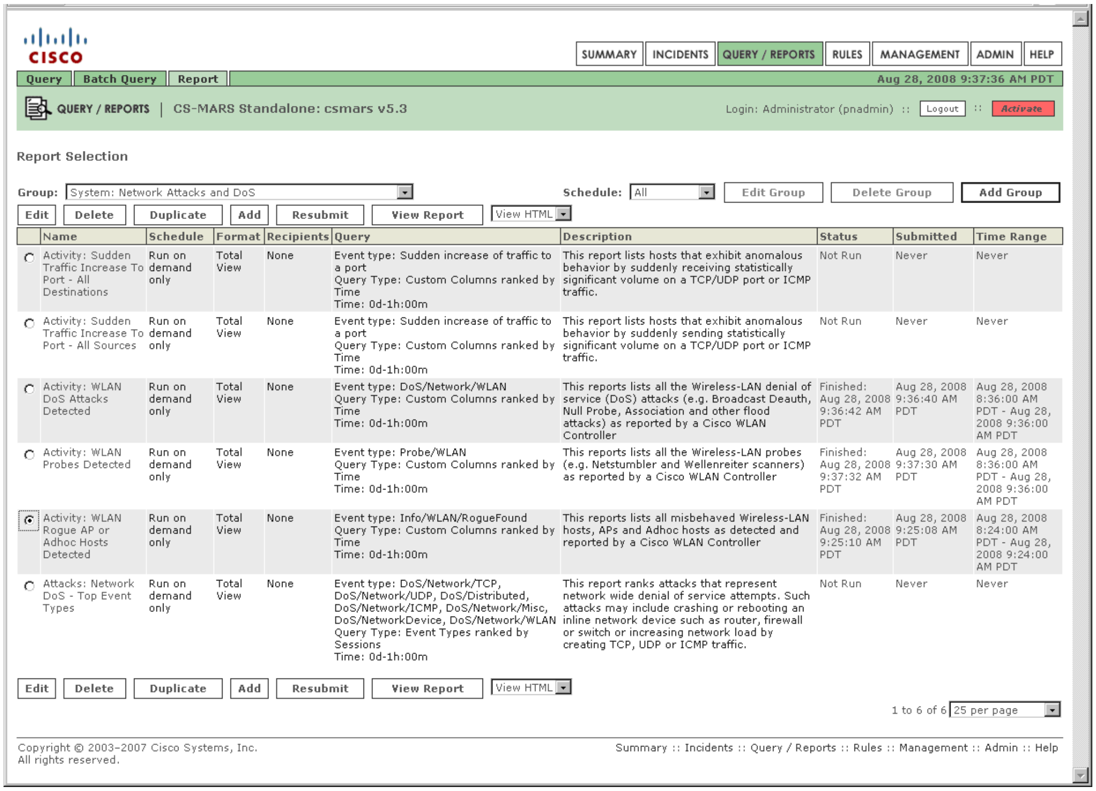
	Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
○	Activity: Sudden Traffic Increase To Port - All Destinations	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
○	Activity: Sudden Traffic Increase To Port - All Sources	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
○	Activity: WLAN DoS Attacks Detected	Run on demand only	Total View	None	Event type: DoS/Network/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller	Not Run	Never	Never
○	Activity: WLAN Probes Detected	Run on demand only	Total View	None	Event type: Probe/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller	Not Run	Never	Never
○	Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT
○	Attacks: Network DoS - Top Event Types	Run on demand only	Total View	None	Event type: DoS/Network/TCP, DoS/Network/UDP, DoS/Distributed, DoS/Network/ICMP, DoS/Network/Misc, DoS/NetworkDevice, DoS/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m	This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.	Not Run	Never	Never

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help
225327

Step 3 Select the report of interest and, unless the report was recently generated, click **Resubmit**.

To view the newly generated report, click **View Report** (see Figure 9-20).

Figure 9-20 Generating and Viewing a CS-MARS Report



Aug 28, 2008 9:37:36 AM PDT

QUERY / REPORTS | CS-MARS Standalone: csmars v5.3

Login: Administrator (pnadmin) :: Logout :: Activate

Report Selection

Group: System: Network Attacks and DoS

Schedule: All

	Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
○	Activity: Sudden Traffic Increase To Port - All Destinations	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
○	Activity: Sudden Traffic Increase To Port - All Sources	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
○	Activity: WLAN DoS Attacks Detected	Run on demand only	Total View	None	Event type: DoS/Network/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:36:42 AM PDT	Aug 28, 2008 9:36:40 AM PDT	Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT
○	Activity: WLAN Probes Detected	Run on demand only	Total View	None	Event type: Probe/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:37:32 AM PDT	Aug 28, 2008 9:37:30 AM PDT	Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT
●	Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT
○	Attacks: Network DoS - Top Event Types	Run on demand only	Total View	None	Event type: DoS/Network/TCP, DoS/Network/UDP, DoS/Distributed, DoS/Network/ICMP, DoS/Network/Misc, DoS/NetworkDevice, DoS/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m	This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.	Not Run	Never	Never

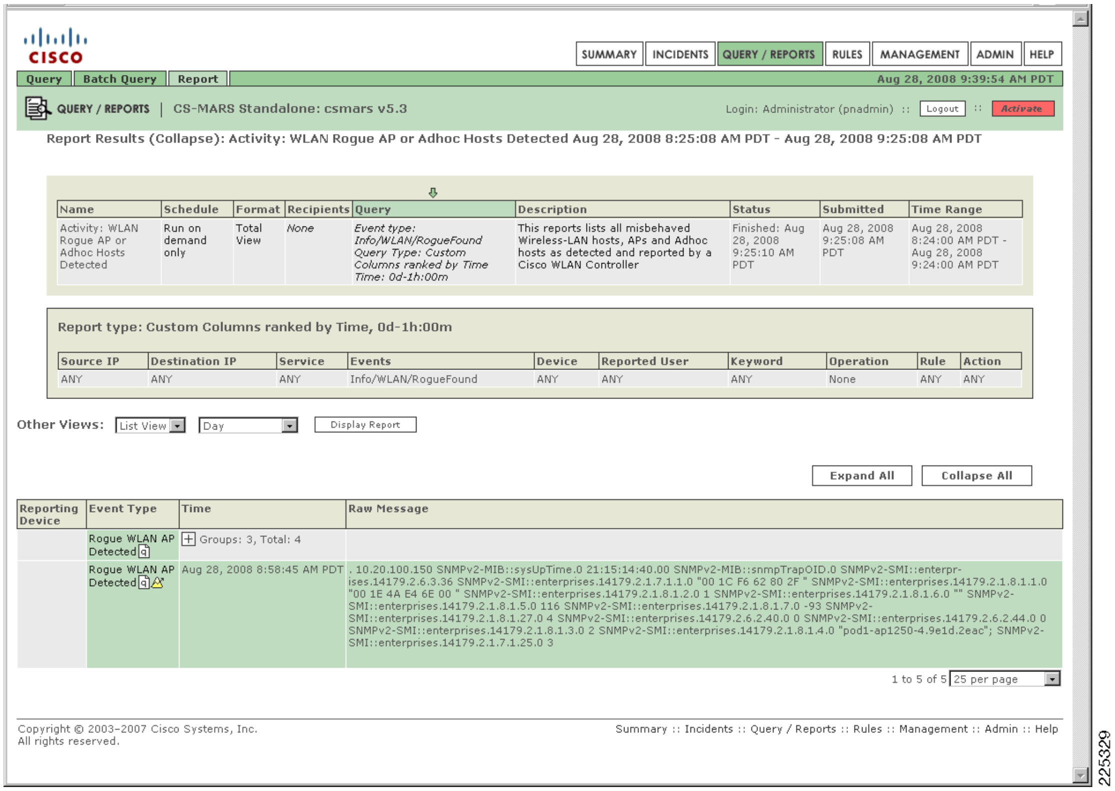
1 to 6 of 6 25 per page

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help
225328

The report is then displayed (see Figure 9-21).

Figure 9-21 Sample CS-MARS WLAN Rogue AP Report



Report Results (Collapse): Activity: WLAN Rogue AP or Adhoc Hosts Detected Aug 28, 2008 8:25:08 AM PDT - Aug 28, 2008 9:25:08 AM PDT

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	*None*	*Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m*	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT

Report type: Custom Columns ranked by Time, 0d-1h:00m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	None	ANY	ANY

Reporting Device	Event Type	Time	Raw Message
	Rogue WLAN AP Detected	⊞ Groups: 3, Total: 4	
	Rogue WLAN AP Detected	Aug 28, 2008 8:58:45 AM PDT	. 10.20.100.150 SNMPv2-MIB::sysUpTime.0 21:15:14:40.00 SNMPv2-MIB::snmpTrapOID.0 SNMPv2-SMI::enterprises.14179.2.6.3.36 SNMPv2-SMI::enterprises.14179.2.1.7.1.1.0 "00 1C F6 62 80 2F " SNMPv2-SMI::enterprises.14179.2.1.8.1.1.0 "00 1E 4A E4 6E 00 " SNMPv2-SMI::enterprises.14179.2.1.8.1.2.0 1 SNMPv2-SMI::enterprises.14179.2.1.8.1.6.0 "" SNMPv2-SMI::enterprises.14179.2.1.8.1.5.0 116 SNMPv2-SMI::enterprises.14179.2.1.8.1.7.0 -93 SNMPv2-SMI::enterprises.14179.2.1.8.1.27.0 4 SNMPv2-SMI::enterprises.14179.2.6.2.40.0 0 SNMPv2-SMI::enterprises.14179.2.6.2.44.0 0 SNMPv2-SMI::enterprises.14179.2.1.8.1.3.0 2 SNMPv2-SMI::enterprises.14179.2.1.8.1.4.0 "pod1-ap1250-4.9e1d.2eac"; SNMPv2-SMI::enterprises.14179.2.1.7.1.25.0 3

1 to 5 of 5

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

General Guidelines for CS-MARS Integration for Cisco Unified Wireless

General guidelines for extending CS-MARS monitoring to the Cisco Unified Wireless Network include the following:

- Enable CS-MARS monitoring of the Cisco Unified Wireless Network to provide cross-network visibility
- Ensure access point MAC addresses are unique
- Consider developing custom rules that use the rich set of WLAN events to further extend CS-MARS capabilities
- Use WCS for detailed analysis and investigation of WLAN events

Additional Information

CS-MARS for Cisco Unified Wireless Operational Considerations

This section outlines some operational considerations when extending CS-MARS cross-network anomaly detection and correlation to the Cisco Unified Wireless Network.

- The reporting device for Cisco Unified Wireless events is the name of the WLC or AP that generated the event.
- The WLC and AP often only identify and report WLAN anomalies based on the MAC address of the device generating the anomaly. Related information, such as source and destination IP address, port, or protocol are typically not reported. If this is the case, CS-MARS displays the WLAN event with a source and destination IP address of 0.0.0.0, a source and destination port of 0, and a protocol of N/A. The MAC address of the device identified as the source of the anomaly is available in the raw message.
- CS-MARS does not currently perform event classification or correlation based on the MAC address of the device generating a WLAN anomaly. For detailed WLAN-specific event anomaly detection and correlation, the Cisco WLC and Wireless Control System (WCS) can be leveraged to enable further investigation of anomalies identified by CS-MARS.
- CS-MARS false positive tuning is performed based on source or destination IP address. Since many WLAN anomalies, such as rogue AP reporting, do not have a client source or destination IP address, this is not currently possible. However, extensive rogue device classification capabilities were introduced in Cisco Unified Wireless Release 5.0 and these should be leveraged to aid incident investigation. For more details on this feature, refer to Reference Documents, page 9-25.
- A custom parser can be used to extend CS-MARS native parsing of WLAN events, for example, to use the WLAN anomaly source MAC address. For more details on this CS-MARS capability, refer to Reference Documents, page 9-25.
- CS-MARS currently only supports SNMP v1, which passes all data in clear text, including the community strings, and is thus vulnerable to sniffing. It is recommended that customers review their security policy to determine if additional security techniques, such as IPSec or an out-of-band (OOB) management network, are required to protect SNMP v1 transactions. General best practices include the use of strong, non-trivial community strings, removing default community strings, restricting access to authorized originators only, and granting only read-only access. For more information on securing SNMP access, refer to the *Network Security Baseline* document in General Network Security, page 9-25.

CS-MARS WLAN AP Event Parsing

In order for CS-MARS to discover and parse events from Cisco LWAPP access points, the Cisco WLC must first be defined as a reporting device in CS-MARS. The steps required to define a Cisco WLC as a reporting device in CS-MARS are outlined in detail earlier in this chapter.

The WLC receives events from the APs that it monitors and then forwards these events as SNMP traps. The source IP address of the trap is always the WLC. However, if an AP generated the original event, the MAC address of the AP is embedded in the SNMP trap as an OID (object identifier).

CS-MARS parses these SNMP traps in order to accurately identify the reporting device.

When CS-MARS receives an SNMP trap from a WLC that includes the MAC address of an AP as the event originator, the manner in which the event is parsed depends upon whether CS-MARS has an AP with a matching MAC address already defined or not:

- If the AP MAC address is known, CS-MARS presents the AP device name as the reporting device
- If the AP MAC address is unknown, CS-MARS presents this first event with the WLC device name as the reporting device and also, automatically, defines the AP as a child agent of the WLC sending the trap. Subsequent events are thus accurately attributed to the AP as the reporting device, since it is defined as a device and identifiable based on its MAC address.

This progressive, automatic discovery of new, undefined, or previously undiscovered APs eliminates the need for manual definition.

Note Progressive auto-discovery of the access points requires SNMPv1 read access to be enabled on the WLC. For information on configuring the WLC, refer to Configuring the Cisco WLC, page 9-3.

If an AP MAC address is unknown and automatic discovery fails, the event is attributed to the WLC.

WLC SNMP traps that do not include AP MAC address information are attributed to the WLC as the reporting device.

CS-MARS Integration for Cisco Unified Wireless Dependencies

CS-MARS and Cisco WLC integration is dependent upon the software and hardware platforms shown in Table 9-3.

Table 9-3 CS-MARS and Cisco WLC Integration Dependencies

Component	Minimum Software	Additional Information
CS-MARS	Release 5.3.2 or later	Release 6.0 supports both Gen1 and Gen2 hardware Release 5.3.2 supports Gen2 hardware (110 and 210) only
Cisco WLC	Cisco Unified Wireless Release 4.x or later	LWAPP APs only
LWAPP AP		

Test Bed Hardware and Software

Integration testing was performed and verified using the CS-MARS and WLC platforms and software releases shown in Table 9-4.

Table 9-4 Test Bed Hardware and Software

Component	Hardware	Software
CS-MARS	MARS 210	5.3.5 (2934)
WLC	WLC 2106	5.0.148.2
	Wireless Services Module (WiSM) in Cisco Catalyst 6500 Series	5.0.148.2

Reference Documents

Cisco Unified Wireless

- Cisco Wireless

  http://www.cisco.com/en/US/products/hw/wireless/index.html
- Cisco Wireless Control System (WCS)

  http://www.cisco.com/en/US/products/ps6305/index.html
- Managing Rogue Devices

  Cisco Wireless LAN Controller Configuration Guide, Release 5.0
  http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/c5sol.html#wp1345692

CS-MARS

- CS-MARS

  http://www.cisco.com/en/US/products/ps6241/tsd_products_support_series_home.html
- Configuring Wireless LAN Devices

  User Guide for Cisco Security MARS Local Controller, Release 5.3.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgwlan.html
- Configuring Custom Devices

  User Guide for Cisco Security MARS Local Controller, Release 5.3.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgcustm.html

  User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/cfgCustm.html

General Network Security

- Network Security Baseline

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html