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 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

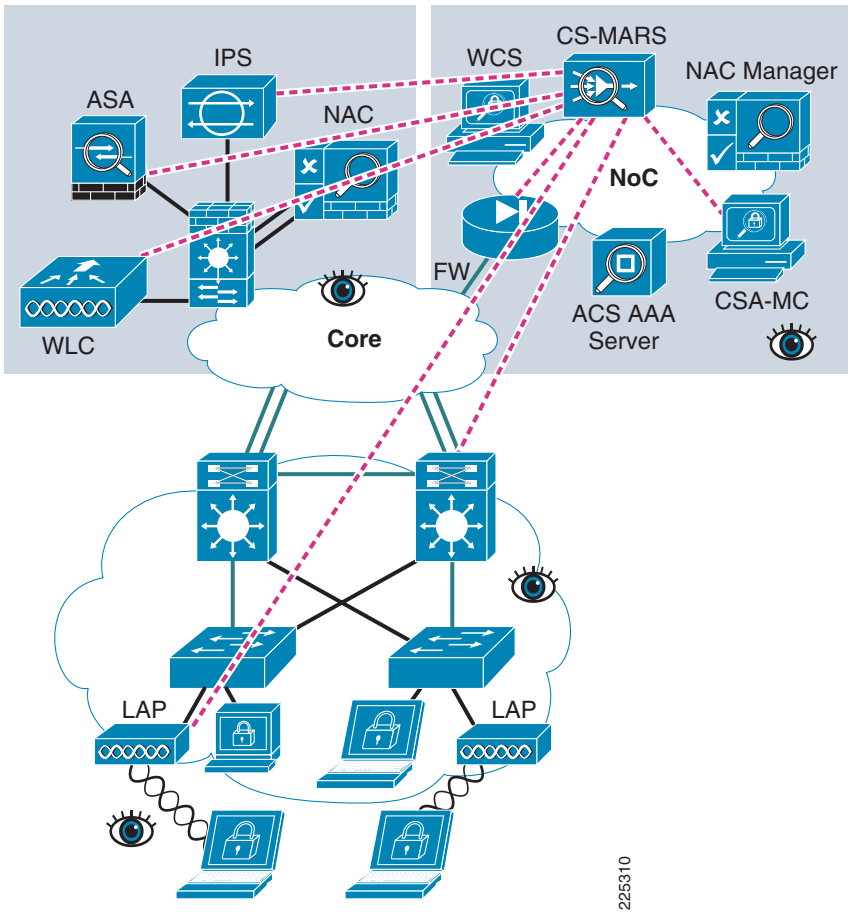
CS-MARS security monitoring combines cross-network intelligence, sophisticated event correlation, and threat validation to effectively identify potential network and application threats.

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 25.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

Figure 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 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 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:

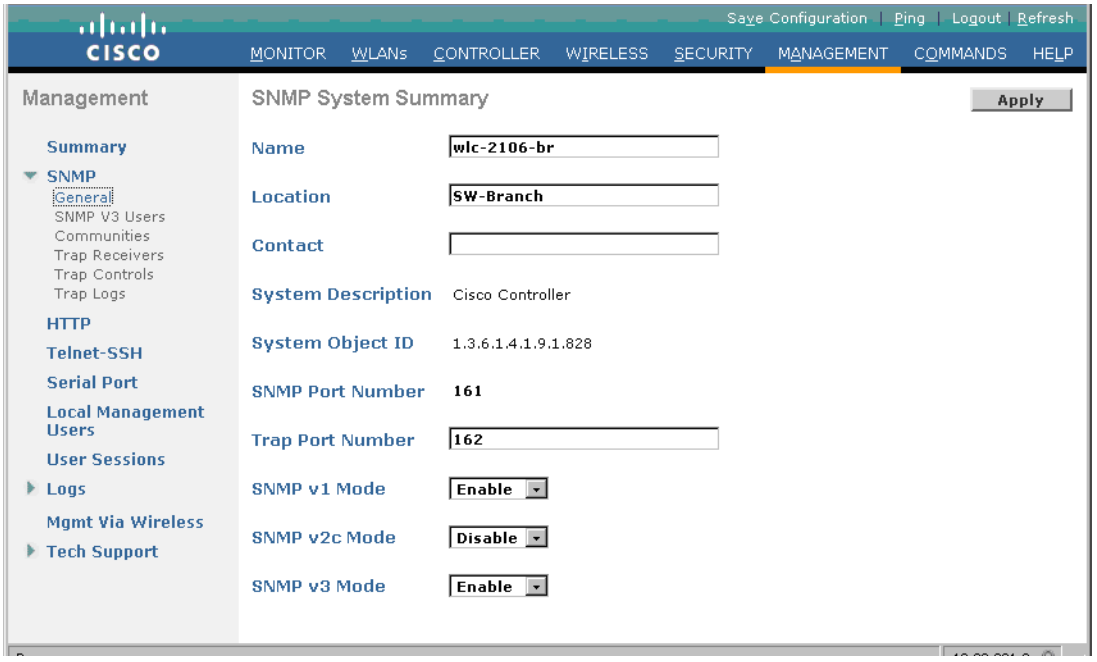
1. Enable SNMP v1 (CS-MARS currently only supports SNMP v1).
2. Define the community settings for use with CS-MARS.
3. Verify that the required SNMP traps are enabled.
4. Define CS-MARS as an SNMP trap receiver.

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 2).

Figure 2 Enabling SNMP v1 on a Cisco WLC

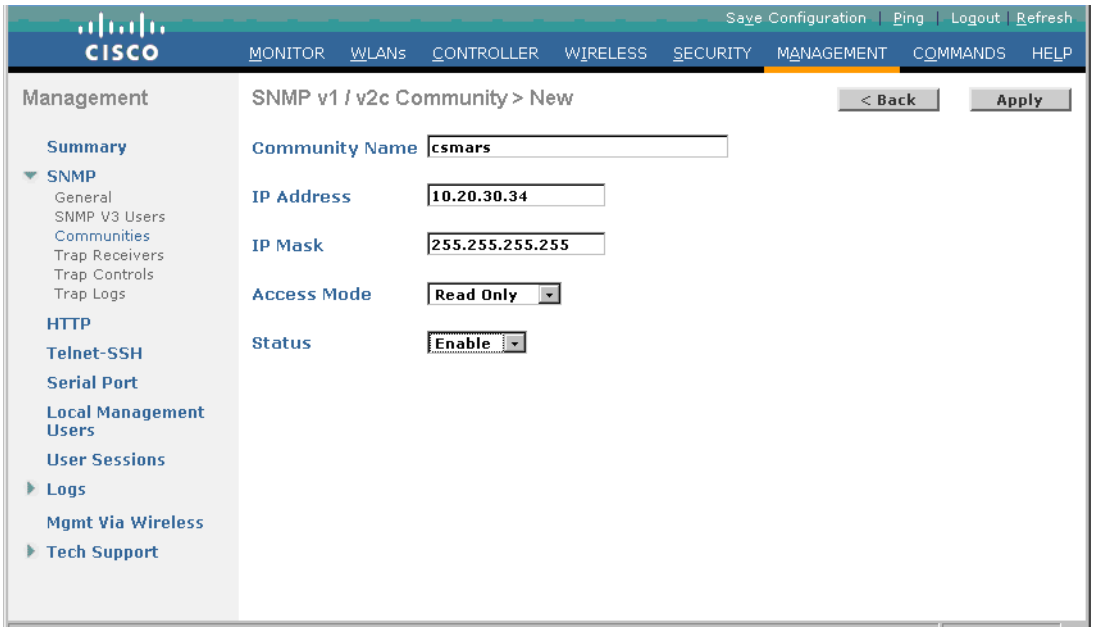


Note SNMP v1 is disabled by default on the WLC.

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 3).

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



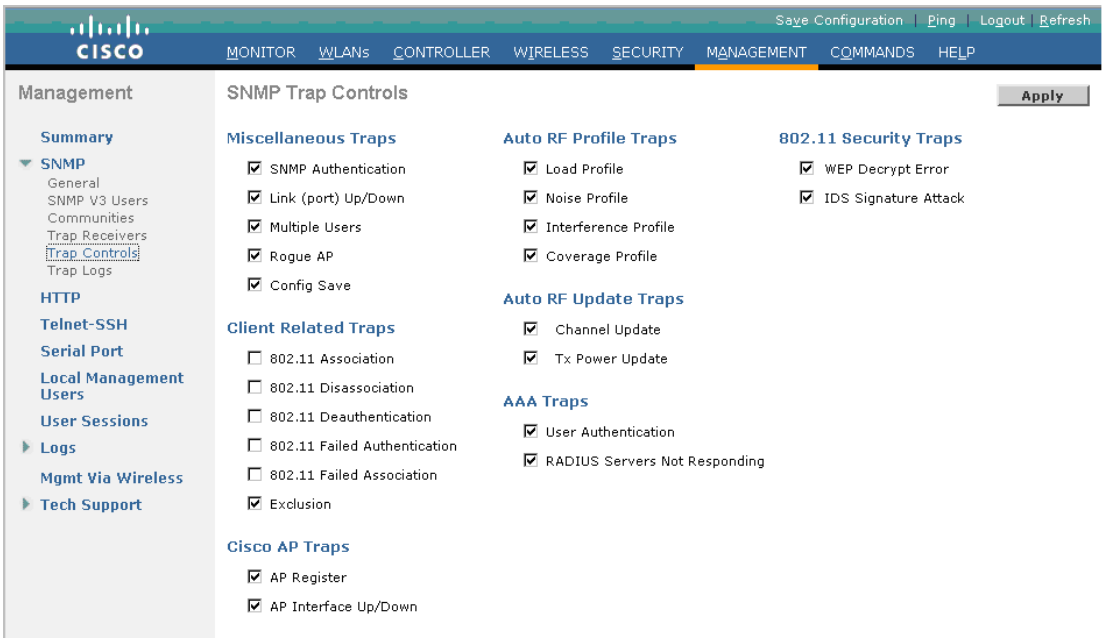
Note the following:

- 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 4).

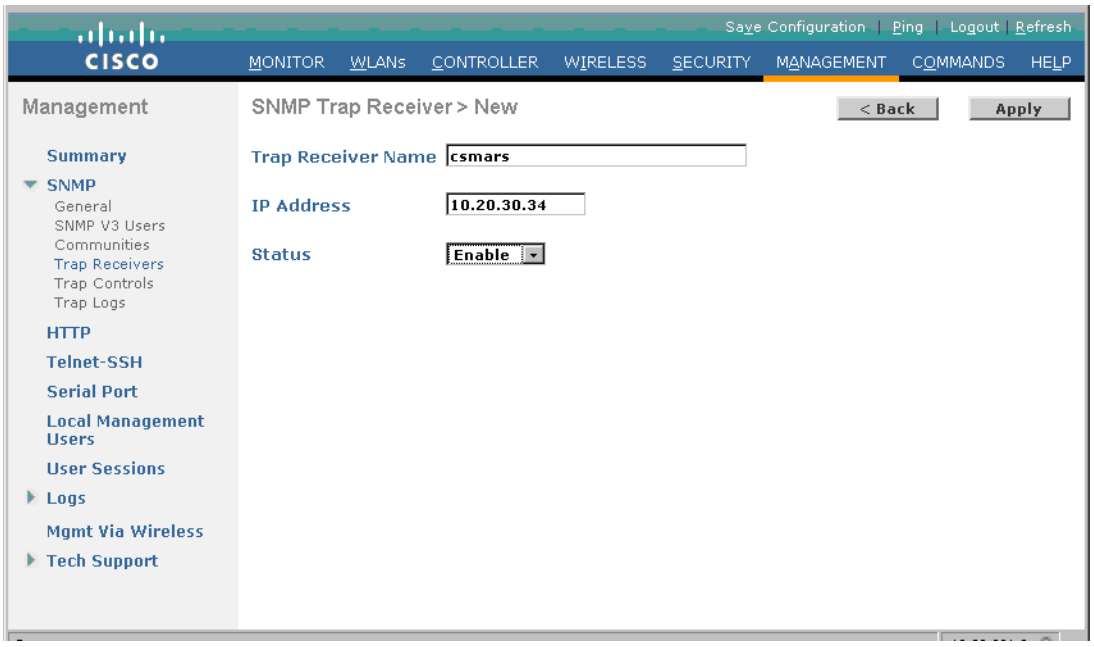
Figure 4 Verifying WLC SNMP Trap Controls



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 5).

Figure 5 Defining CS-MARS as an SNMP Trap Receiver



Configuring CS-MARS

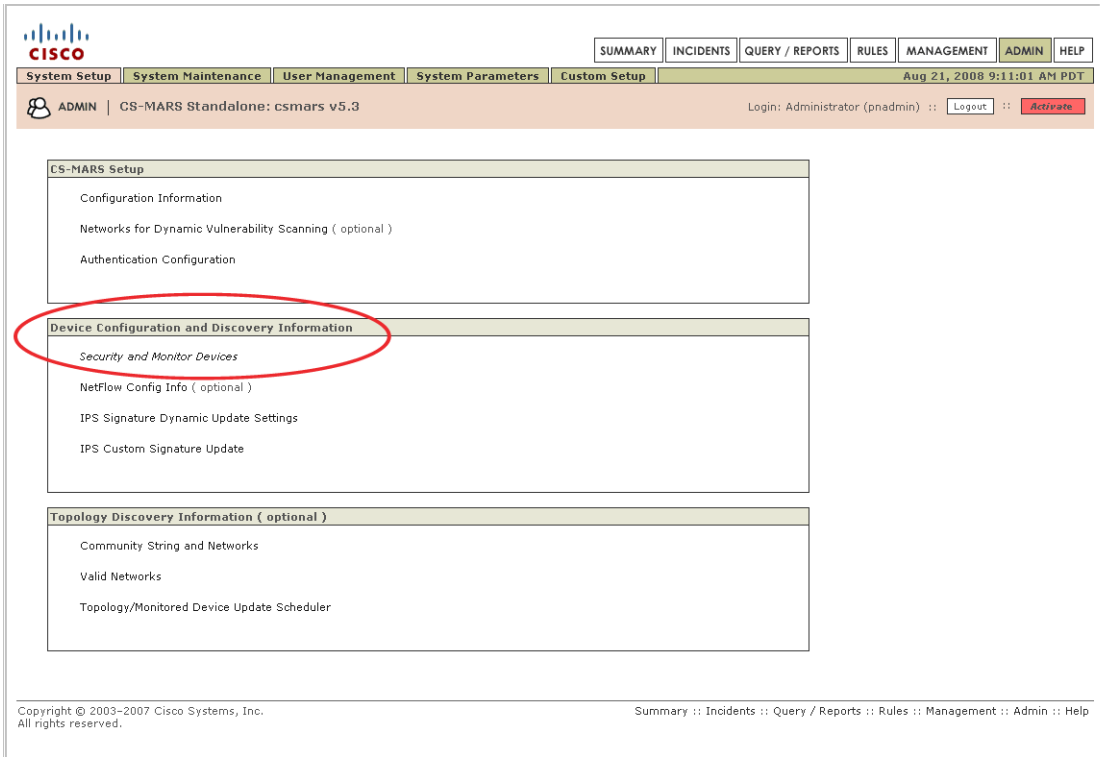
In order for CS-MARS to discover each Cisco WLC and its connected LWAPP APs, each WLC must be defined on CS-MARS. This provides CS-MARS with SNMP read-only access to the device so that it can obtain this and other device-specific information. This is the only configuration required on CS-MARS.

Manually Adding a Cisco WLC

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

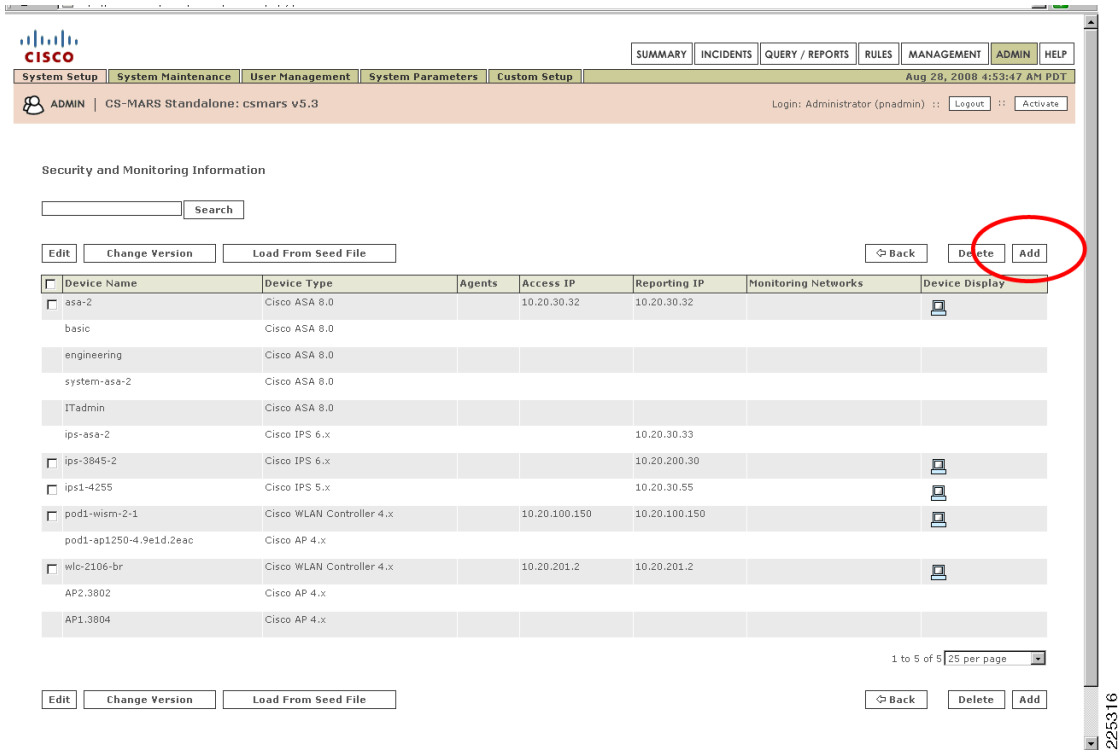
Step 1 On the CS-MARS GUI, navigate to **ADMIN -> System Setup**. In the middle section titled **Device Configuration and Discovery Information**, select **Security and Monitor Devices** (see Figure 6).

Figure 6 CS-MARS System Setup Screen



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

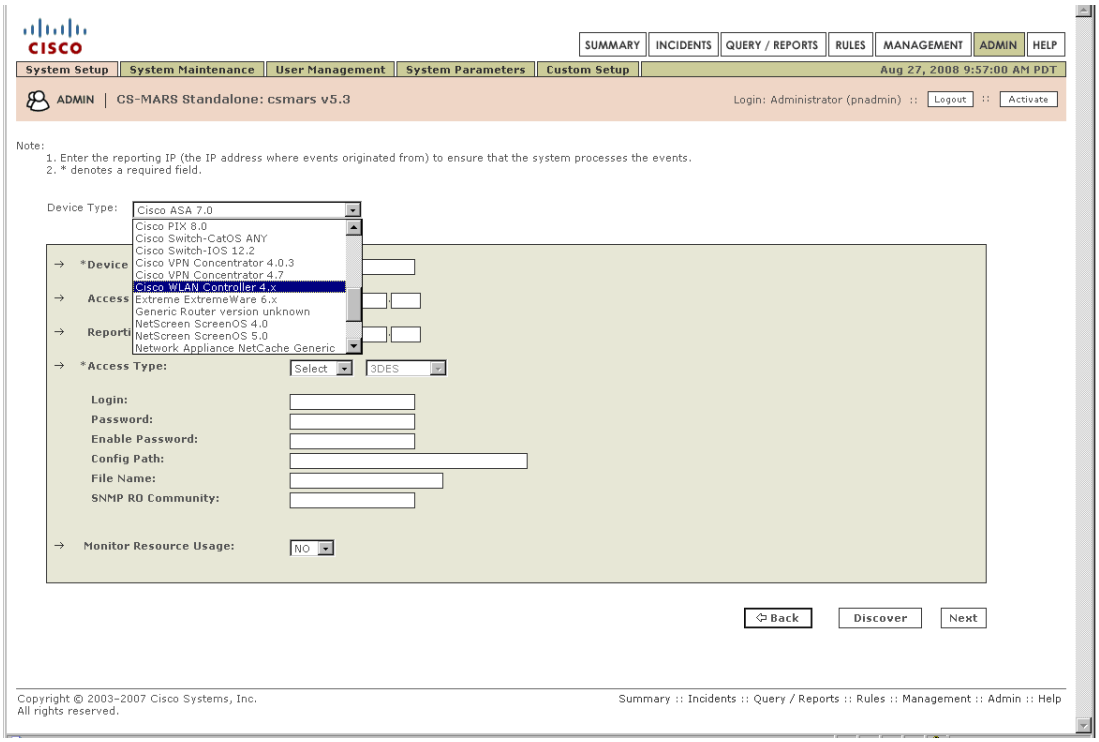
Figure 7 CS-MARS Screen to Add a New Device



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 8).

Figure 8 Adding a Cisco WLC on CS-MARS

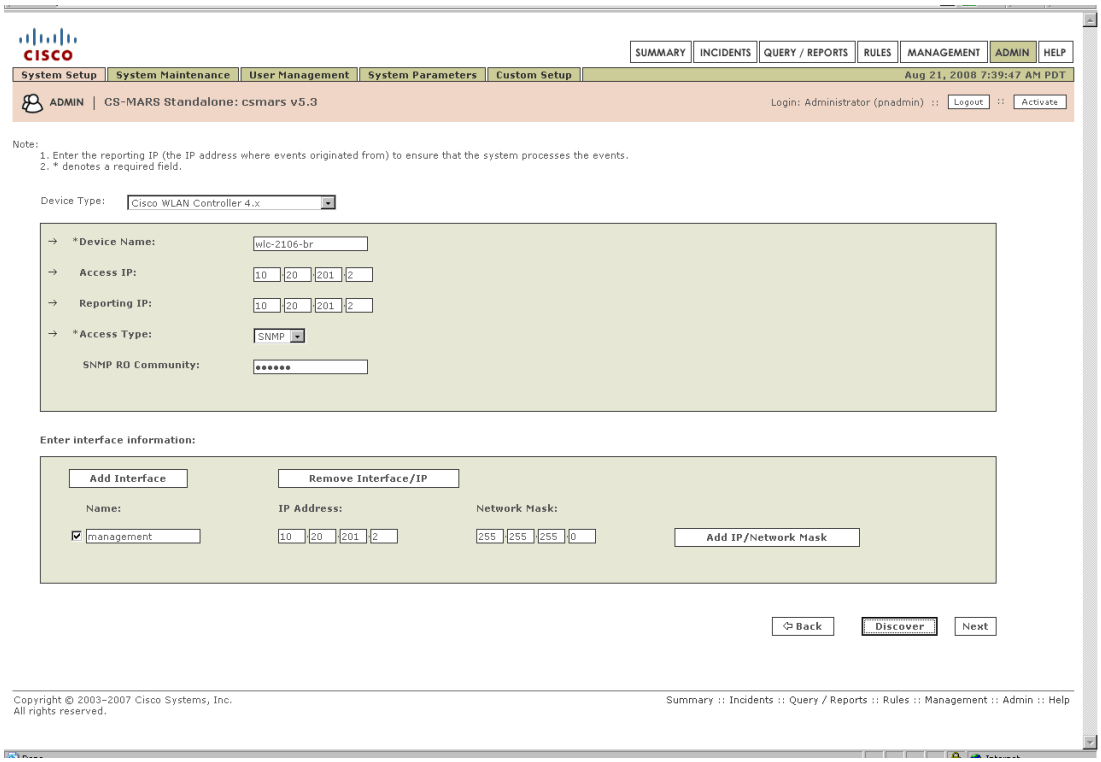


The device entry fields change to reflect this device type and the WLC can be defined by entering this information:

- 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).

Figure 9 Defining a Cisco WLC on CS-MARS



Note the following:

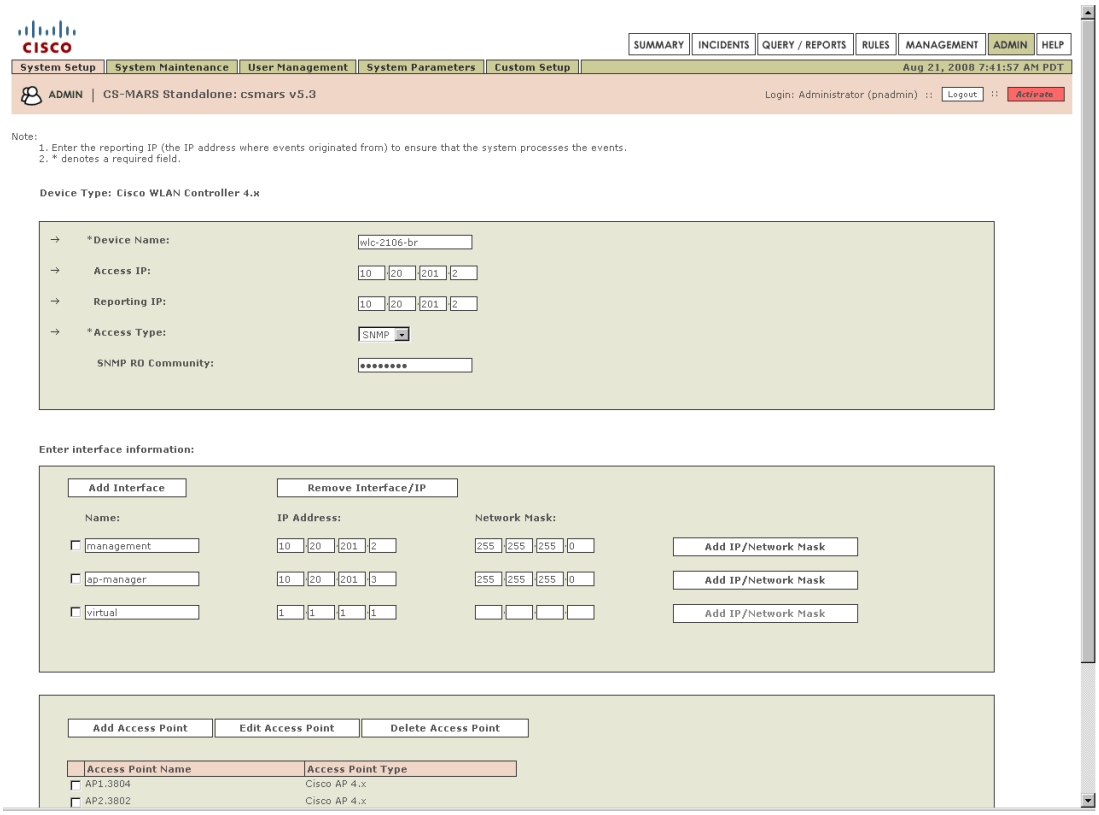
- The WLC management interface must be defined. Other interfaces will automatically be added upon successful discovery of the device.
- SNMP v1 access must already be enabled on the WLC for discovery to be successful (see Configuring the Cisco WLC, page 3).

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 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.

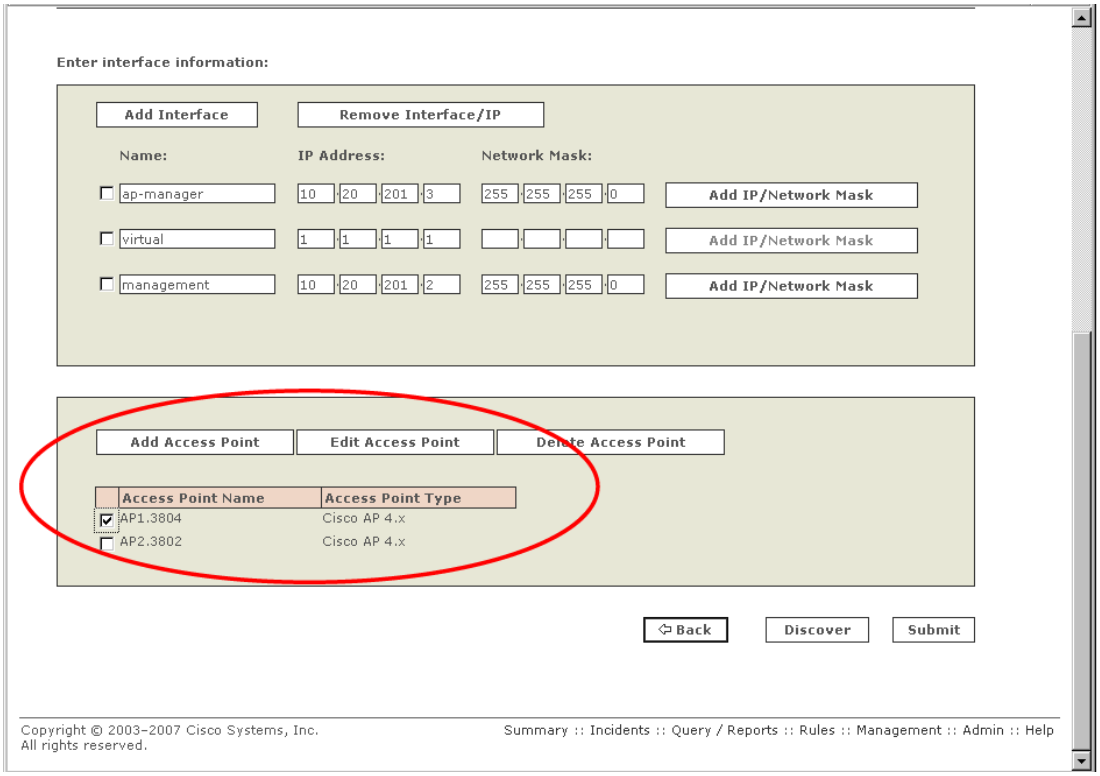
Figure 10 Successful Cisco WLC Discovery on CS-MARS



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

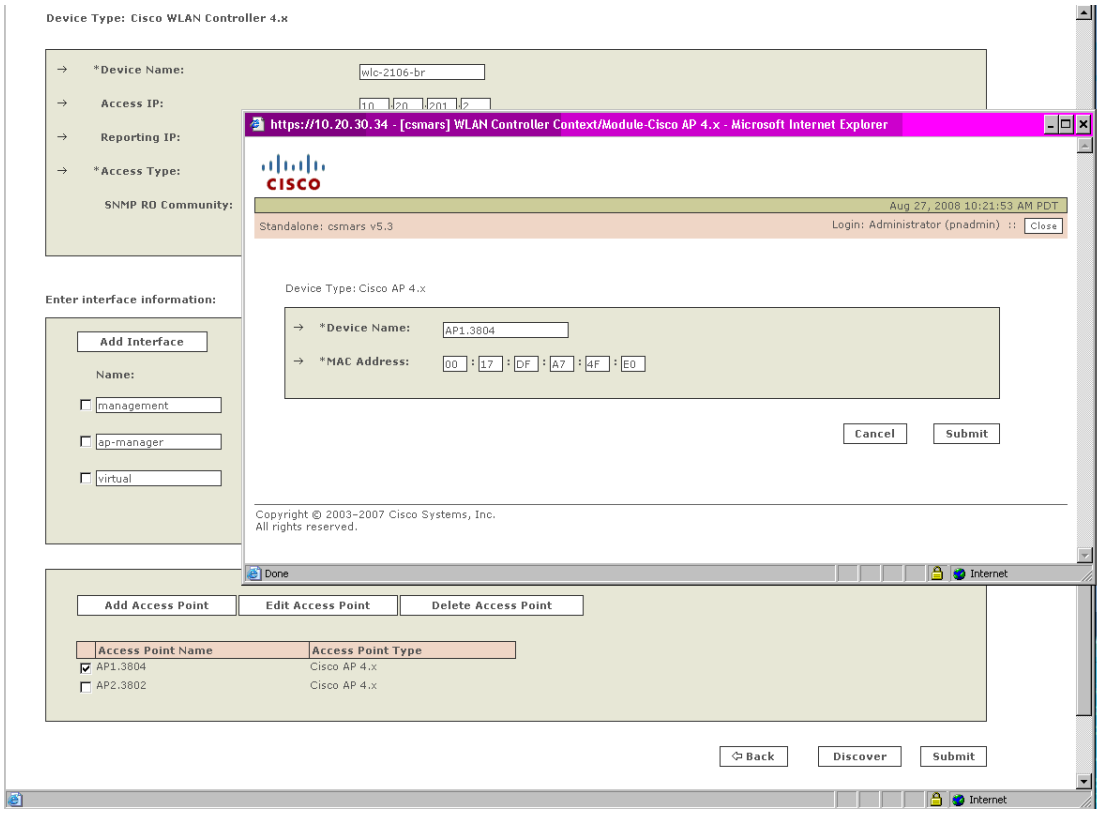
Note that CS-MARS identifies an access point (AP) based on its MAC address rather than the typical Access IP/Reporting IP. To view the MAC address of a particular AP, scroll to the bottom of the WLC device page, check the box next to the name of an AP and click **Edit Access Point** (see Figure 12).

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



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

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



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 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 25).

WLAN Events

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

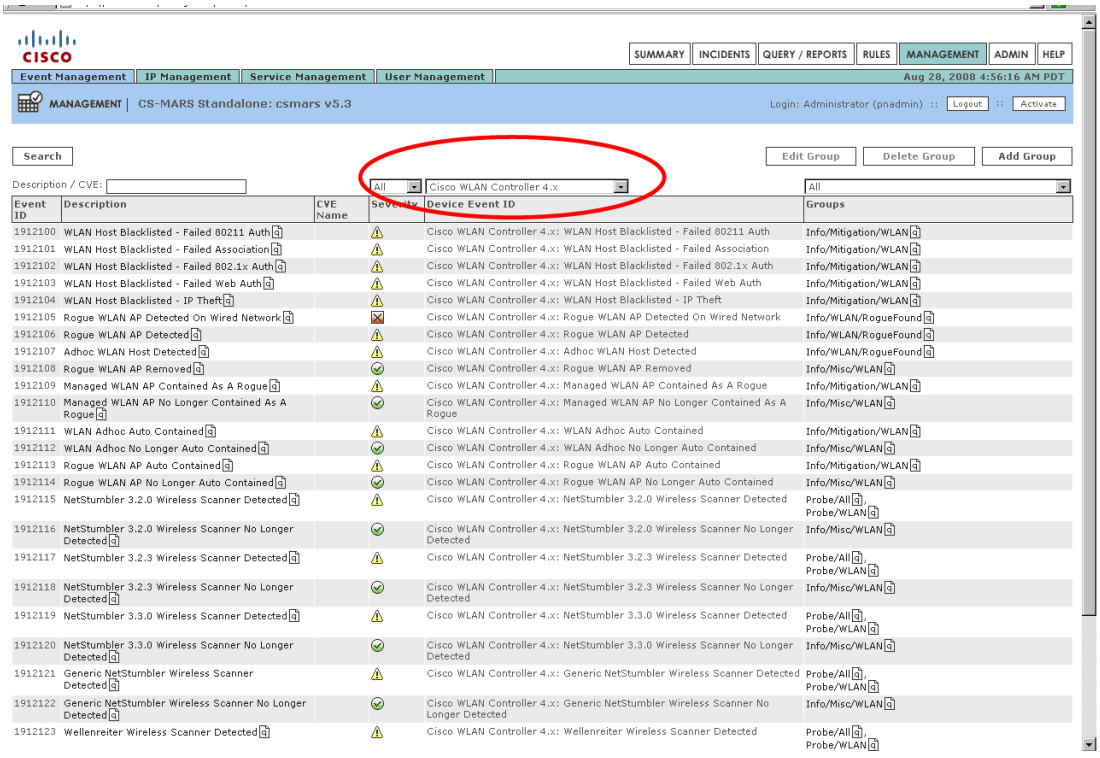
- WLAN DoS attacks
- Rogue APs
- 802.11 probes
- Ad hoc networks
- Client exclusions/blacklisting
- WLAN operational status

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 13).

Figure 13 Sample Subset of CS-MARS WLAN Events



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 1.

Table 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 2.

Table 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.

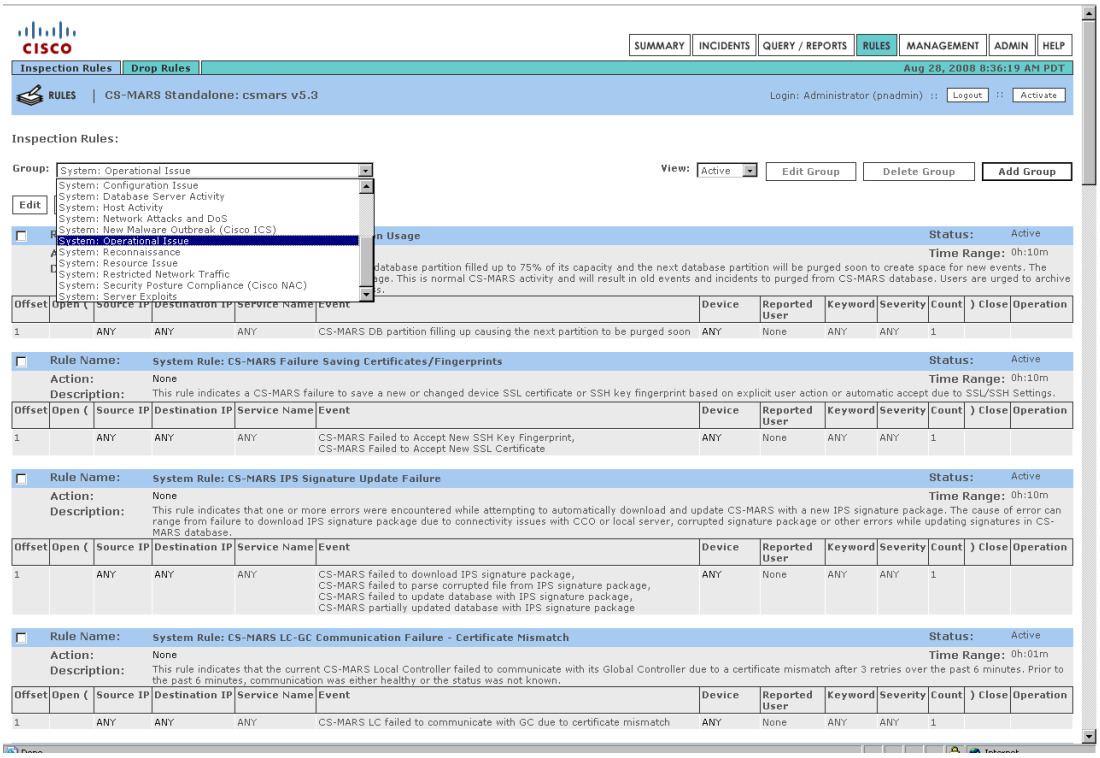
To view the details of a CS-MARS rule:

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 14).

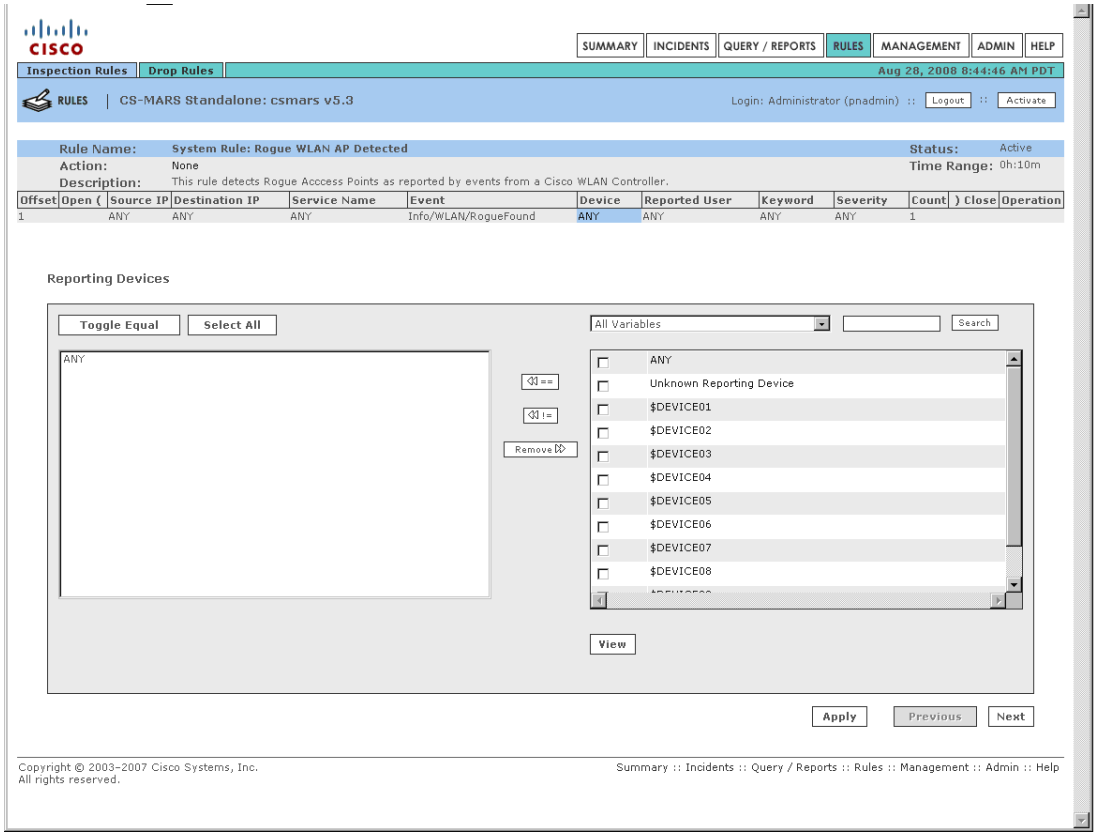
Figure 14 Viewing CS-MARS Rules by Rule Group



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 15.

Figure 15 CS-MARS Rule Rogue WLAN AP Detected



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

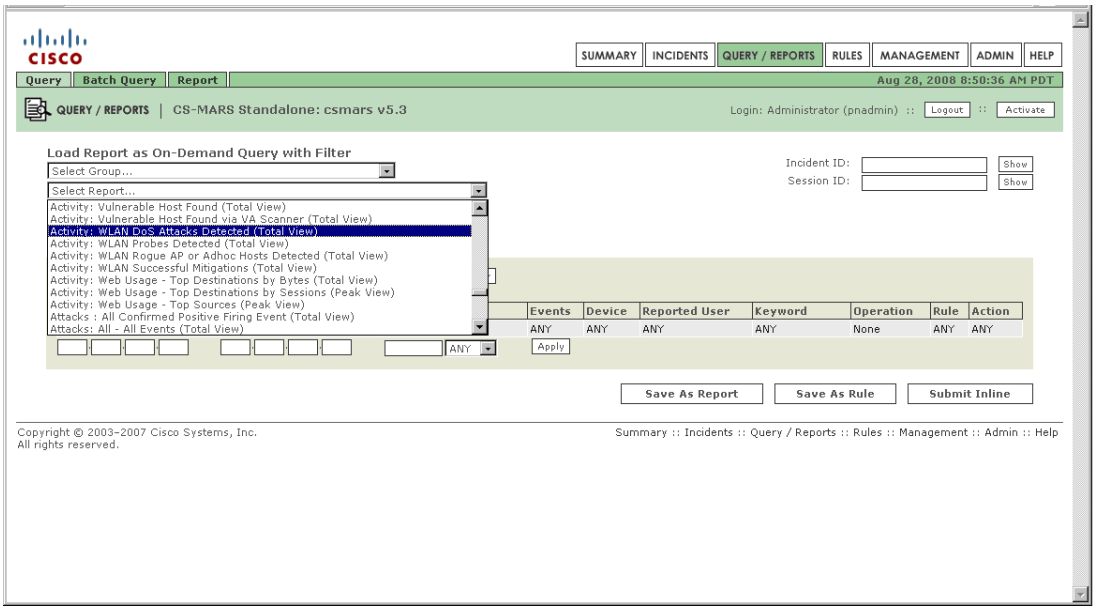
To run a query on particular WLAN-specific events:

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

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

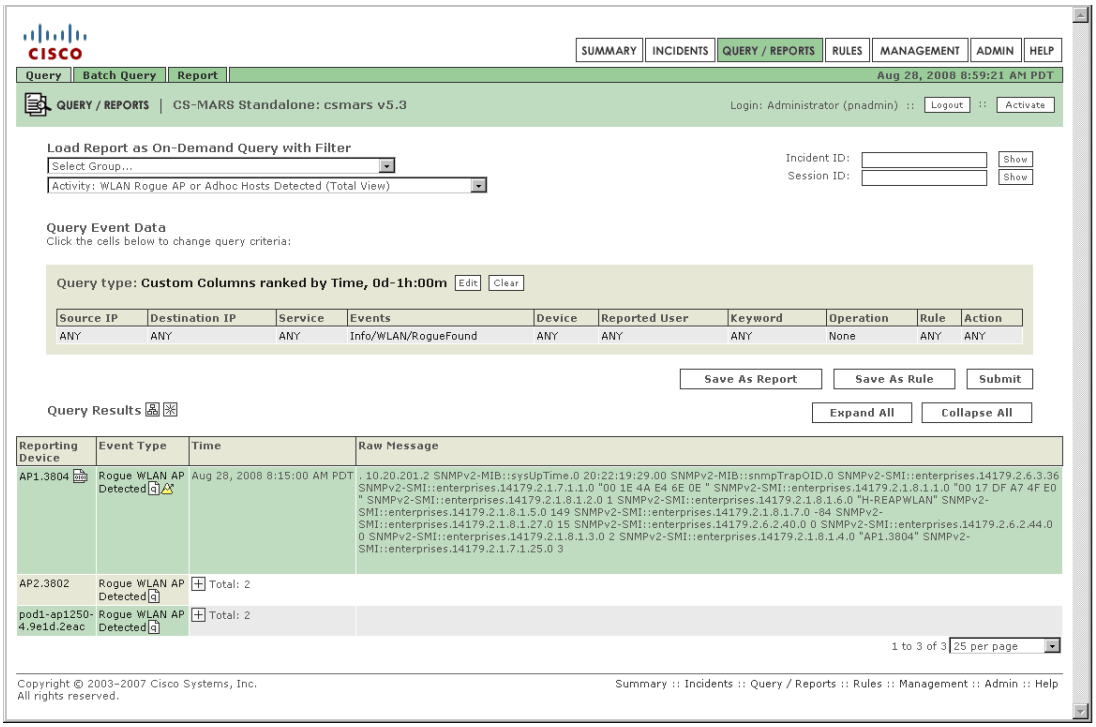
If you know which Report Group a report belongs to, you can filter the list by selecting the appropriate Report Group in the drop-down box **Select Group…** (see Figure 16).

Figure 16 CS-MARS WLAN-Specific Reports



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

Figure 17 Sample CS-MARS Rogue WLAN AP Report



Generating a Report on WLAN Events

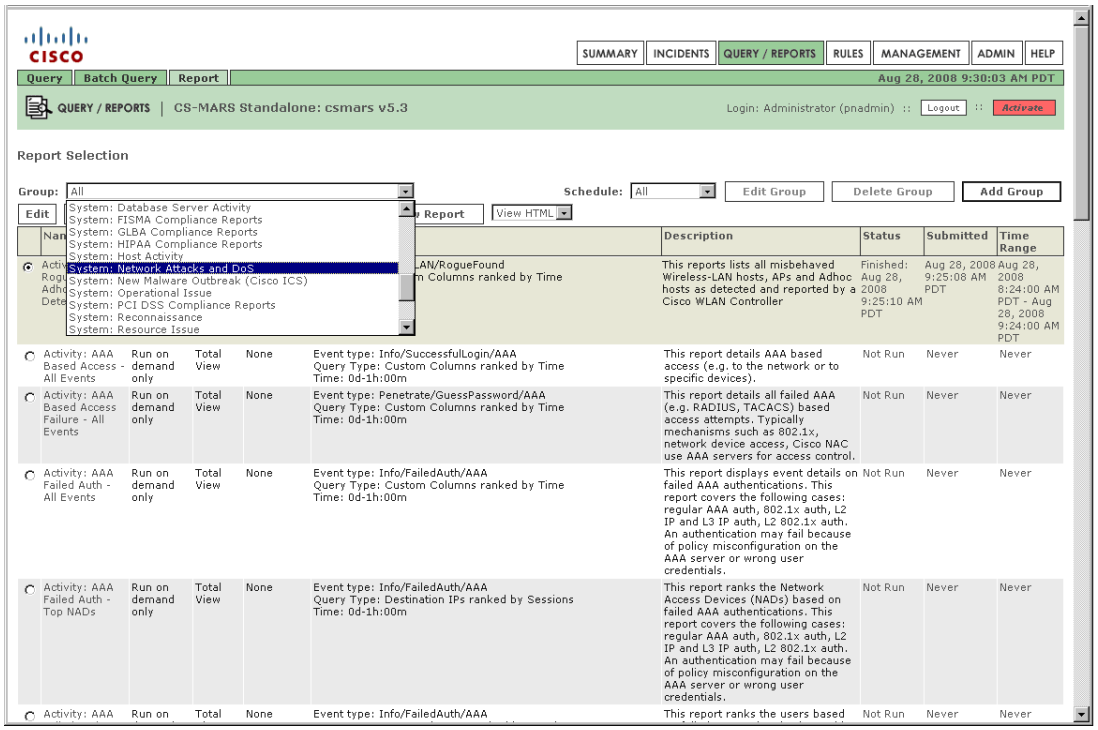
Events that have been correlated into event sets can be expanded to view the individual events and their associated raw message.

To generate a report on particular WLAN-specific events:

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

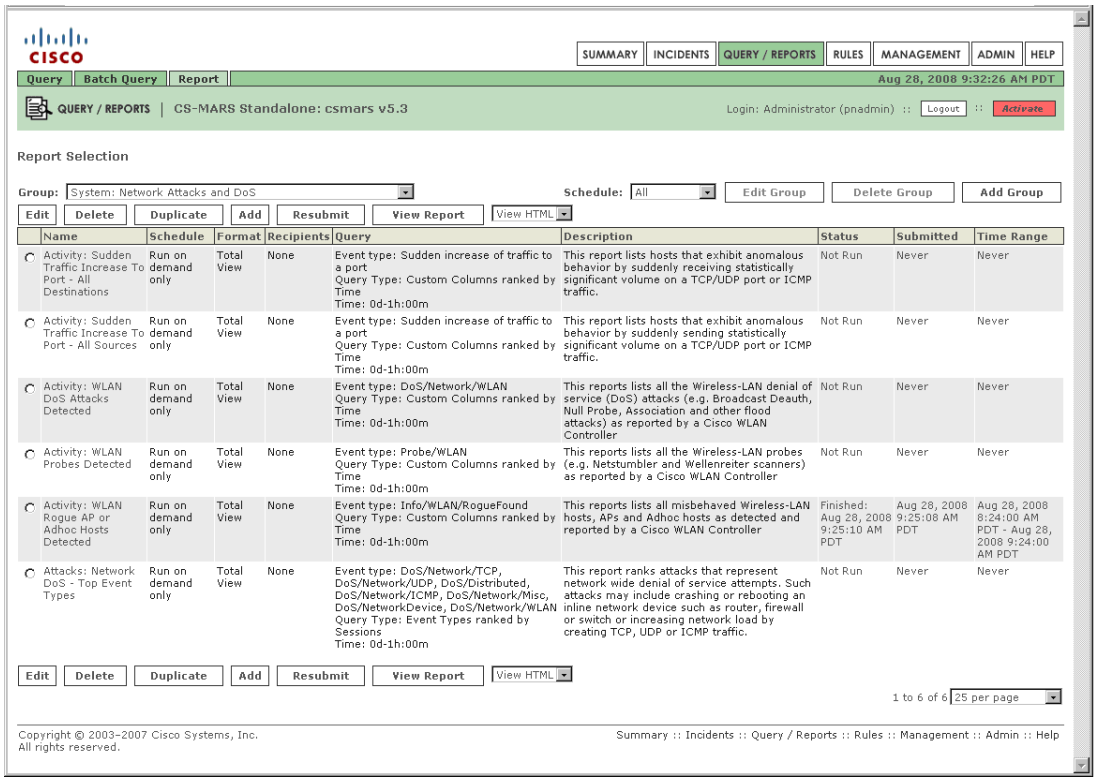
Step 2 From the drop-down box **Group --Report Groups -**, select, the desired Report Group (see Figure 18).

Figure 18 Selecting a CS-MARS Report by Report Group



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

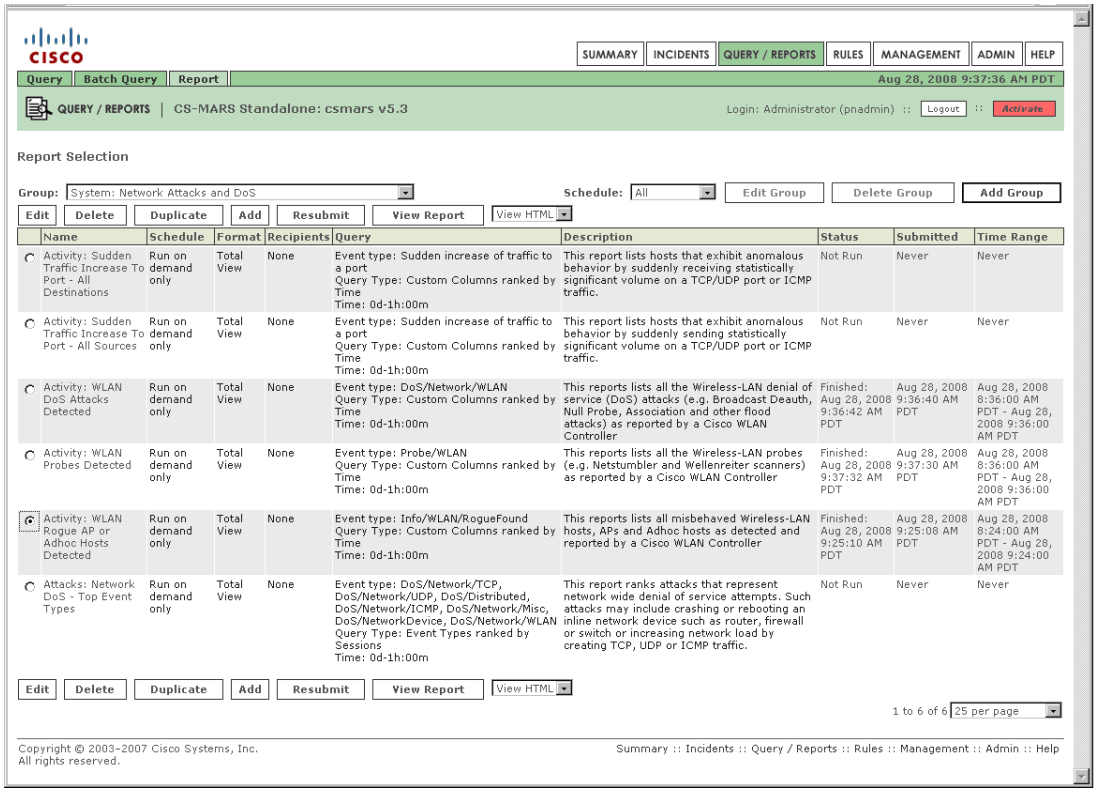
Figure 19 CS-MARS Network Attacks and DoS Report Group



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

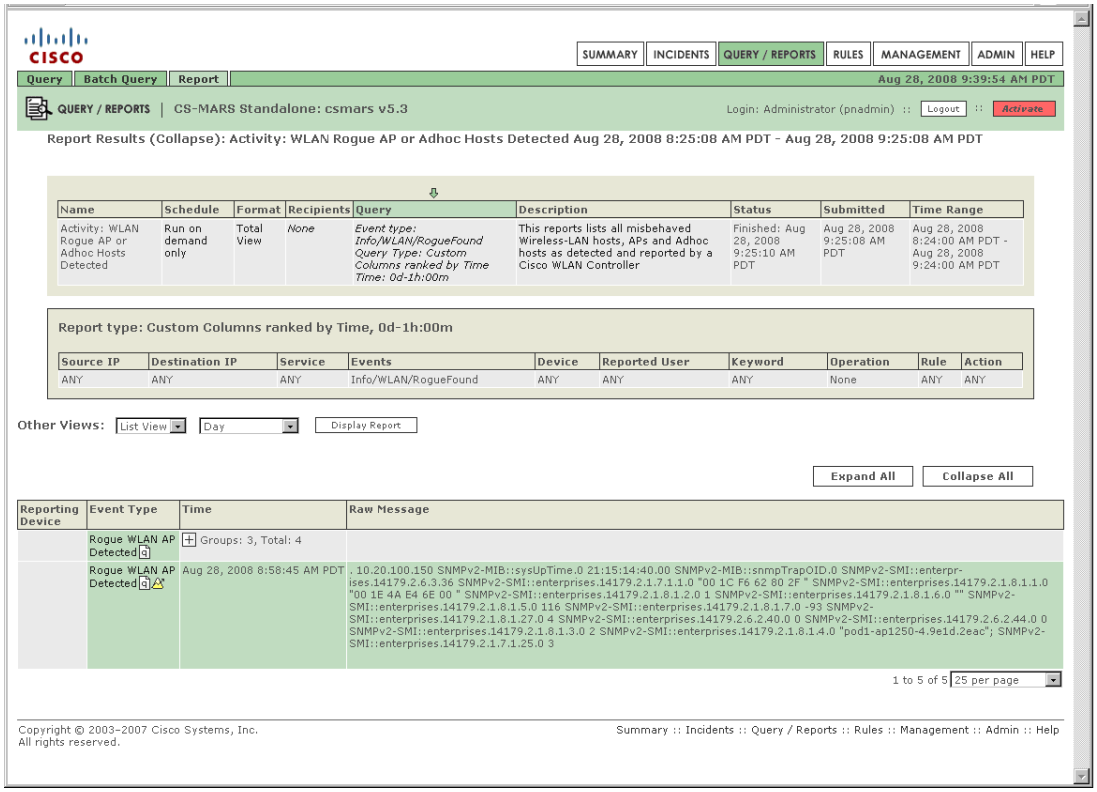
To view the newly generated report, click **View Report** (see Figure 20).

Figure 20 Generating and Viewing a CS-MARS Report



The report is then displayed (see Figure 21).

Figure 21 Sample CS-MARS WLAN Rogue AP Report



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 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 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 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 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 3.

Table 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 4.

Table 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