



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.



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).

					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		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P
Management	SNMP Sy	rstem Su	mmary			-	Ар	ply
Summary	Name		wlc-2106-bi	•				
 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	SNMP Por	t Numbei	161					
Local Management Users User Sessions I Logs	Trap Port		162 Enable 🔻					
Mgmt Via Wireless Tech Support	SNMP v2c	Mode	Disable 💌					
	SNMP v3 I	Mode	Enable 🔹					
2							10.00.001	a (7)

Figure 9-2 Enabling SNMP v1 on a Cisco WLC

 $\frac{\mathbf{N}}{\mathbf{Note}}$ 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

a sahaha sa s				Sa <u>v</u> e	Configuration]	Ping Logout	: <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> MMAND	S HE <u>L</u> P
Management	SNMP v1 / v2c C	ommunity > Ne	W		< Ba	ck	Apply
Summary	Community Name	csmars					
 SNMP General SNMP V3 Users 	IP Address	10.20.30.34					
Trap Receivers	IP Mask	255.255.255.2	55				
Trap Controls Trap Logs	Access Mode	Read Only					
НТТР	01-1						
Telnet-SSH	status	Enable 💌					
Serial Port							
Local Management Users							
User Sessions							
🕨 Logs							
Mgmt Via Wireless							
🕨 Tech Support							
Communities Trap Receivers Trap Controls Trap Logs HTTP Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless			_				

Note the following:

- If the IP address and IP Mask fields are left blank, they default to 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).

cisco	MONITOR WLANS CONTROLLEI	R WIRELESS SECURITY	MANAGEMENT COMMANDS HELP
lanagement	SNMP Trap Controls		A
Summary	Miscellaneous Traps	Auto RF Profile Traps	802.11 Security Traps
SNMP	SNMP Authentication	🔽 Load Profile	WEP Decrypt Error
General SNMP V3 Users	🗹 Link (port) Up/Down	🔽 Noise Profile	🔽 IDS Signature Attack
Communities Trap Receivers	Multiple Users	🔽 Interference Profile	
Trap Controls	🗹 Rogue AP	🔽 Coverage Profile	
Trap Logs HTTP	🗹 Config Save	Auto RF Update Traps	
Telnet-SSH	Client Related Traps	Channel Update	
Serial Port	802.11 Association	✓ Tx Power Update	
Local Management Users	802.11 Disassociation		
User Sessions	802.11 Deauthentication	AAA Traps	
Logs	802.11 Failed Authentication	User Authentication	
Mgmt Via Wireless	802.11 Failed Association	🗹 RADIUS Servers Not R	Responding
Tech Support	Exclusion		
	Cisco AP Traps		
	AP Register		
	☑ AP Interface Up/Down		

Figure 9-4 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 9-5).

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

					Sa <u>v</u> e	Configuration	<u>P</u> ing Lo <u>q</u> ou	t <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANE	S HE <u>L</u> P
Management	SNMP Tr	ap Rece	iver > New			< Ba	ck	Apply
Summary	Trap Rece	eiver Nan	ne csmars					
 SNMP General SNMP V3 Users 	IP Addres	s	10.20.30.34					
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								
-								

225313

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).

				SUMMA		QUERY / REPORTS	RULES	MANAGEMENT	ADMIN	HELP
	m Setup System Maintenance	User Management	System Parameters	Custom Setup				Aug 21, 2008 9		
~	ADMIN CS-MARS Standalone:		System rarameters			Login: Administrat	or (pnad			
LC S	-MARS Setup									
	Configuration Information Networks for Dynamic Vulnerability	Scanning (optional)								
	Authentication Configuration									
De	evice Configuration and Discovery	Information								
\checkmark	Security and Monitor Devices									
	NetFlow Config Info (optional)									
	IPS Signature Dynamic Update Set	tings								
	IPS Custom Signature Update									
То	opology Discovery Information (c	ptional)								
	Community String and Networks									
	Valid Networks									
	Topology/Monitored Device Update	Scheduler								
Copyrigh All rights	ht © 2003–2007 Cisco Systems, Inc. s reserved.			s	ımmary :: Incid	ents :: Query / Repo	rts :: Ru	les :: Management	: :: Admin	:: Help

Figure 9-6 CS-MARS System Setup Screen



sco				SUMMARY INCID	ENTS QUERY / REPORTS RULES	MANAGEMENT ADMIN HELP
tem Setup System Maint	tenance User Management System	Parameters	Custom Setup			Aug 28, 2008 4:53:47 AM PDT
ADMIN CS-MARS Star	ndalone: csmars v5.3				Login: Administrator (pn	admin) :: Logout :: Activate
Security and Monitoring	Information					
security and monitoring	mormation					
	Search					\frown
Edu Oberes Berler	Load From Seed File				-	
Edit Change Version						Back Delete Add
Device Name	Device Type Cisco ASA 8.0	Agents	Access IP 10.20.30.32	Reporting IP 10.20.30.32	Monitoring Networks	Device Display
asa-2			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.×			10.20.30.33		
□ ips-3845-2	Cisco IPS 6.x			10.20.200.30		<u> </u>
🗖 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.2ea	Cisco AP 4.x					
wlc-2106-br	Cisco WLAN Controller 4.x		10.20.201.2	10.20.201.2		<u> </u>
AP2.3802	Cisco AP 4.x					
AP1.3804	Cisco AP 4.x					
						1 to 5 of 5 25 per page 🔹

Figure 9-7 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.



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).

halo	
ISCO	SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP
rstem Setup System Maintenance User Management System Parameters Cus	stom Setup Aug 27, 2008 9:57:00 AM PDT
ADMIN CS-MARS Standalone: csmars v5.3	Login: Administrator (pnadmin) :: Logout :: Activate
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system 2. * denotes a required field. Device Type: Cisco ASA 7.0 Cisco Switch-CatOS ANY Ci	m processes the events.
→ Reporti HetScreen St.0 NetScreen St.0 NetScreen St.0 NetScreen St.0 NetScreen St.0 Select ▼ Solect ▼ Solect ▼ Solect ▼	
Password:	
→ Monitor Resource Usage: No r	
	⇔Back Discover Next
yright © 2003-2007 Cisco Systems, Inc. Ights reserved.	Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Figure 9-8 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 9-9).

em Setup System Maintenance	User Management System Parame	eters Custom Setup					Aug 21, 2008 7	7:39:47 AM PDT
ADMIN CS-MARS Standalone:	csmars v5.3			Lo	gin: Administra	itor (pnadr	nin) :: Logout	: Activate
. Enter the reporting IP (the IP address	where events originated from) to ensure th	at the system processes the even	×.					
. * 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 RD Community:	*****							
								_
								-
nter interface information:								
inter interface information:	Remove Interface/IP]						
	Remove Interface/IP	Network Mask:						
Add Interface		Network Mask:		Add IP/Netwo	erk Mask]		
Add Interface	IP Address:			Add IP/Netwo	ork Mask]		
Add Interface	IP Address:			Add IP/Netwo	ork Mask]		
Add Interface	IP Address:				ork Mask ⇔Back	Disco	ver	t
Add Interface	IP Address:					Disco	ver. Nex	t
Add Interface	IP Address:					Disco	ver Nex	t

Figure 9-9 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 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.

վահ										
CISCO			SUMMARY	INCIDENTS	QUERY	REPORTS	RULES	MANA	GEMENT	ADMIN HELP
ystem Setup System Maintenance	User Management System Param	neters Custom Setup						Aug 21	1,20087	:41:57 AM PDT
ADMIN CS-MARS Standalone	csmars v5.3				Login:	Administra	tor (pnac	lmin) ::	Logout	:: Activate
te: 1. Enter the reporting IP (the IP addres	ss where events originated from) to ensure t	hat the system processes the events.								
2. * denotes a required field.										
Device Type: Cisco WLAN Controll	er 4.x									
→ *Device Name:	wic-2106-br									
\rightarrow Access IP:	10 20 201	2								
\rightarrow Reporting IP:	10 20 201	2								
→ *Access Type:	SNMP -									
SNMP RO Community:										
Enter interface information:										_
Add Interface	Remove Interface/IP									
Name:	IP Address:	Network Mask:								
management	10 20 201 2	255 255 255 0	_	Add IP/N	etwork	task	7			
							_			
ap-manager	10 20 201 3	255 255 255 0		Add IP/N	etwork	1ask				
virtual	1 1 1 1			Add to ()		dask				
				AUU IP/P	letwork	TUJK				
				AUG IP7P	TETWOPK	IU JK				
				AUU IP/P	letwork	NJK.				
				AUGIPYN	etwork	TUJK				
	Edit Access Point Delete Ac	ress Point		AUGIPYN	etwork					
Add Access Point	Edit Access Point Delete Ac	cess Point			etwork					
	Edit Access Point Delete Ac	cess Point			etwork					

Figure 9-10 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 9-12).

	Remove Interface/IP
Name:	IP Address: Network Mask:
🗖 ap-manager	10 20 201 3 255 255 255 0 Add IP/Network Mask
🗖 virtual	1 1 1 1 Add IP/Network Mask
🗖 management	10 /20 /201 /2 255 /255 /0 Add IP/Network Mask
Add Access Point	Edit Access Point Deinte Access Point
Access Point Name	Access Point Type Cisco AP 4.x
AP2.3802	Cisco AP 4.x
	⇔ Back Discover Submit

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

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

→ *Device Name:	wlc-2106-br	
→ Access IP:	111 1211 12	
→ Reporting IP:	Attps://10.20.30.34 - [csmars] WLAN Controller Context/Module-Cisco AP 4.x - Microsof	ft Internet Explorer
→ *Access Type:	cisco	
SNMP RD Community:		Aug 27, 2008 10:21:53 AM PDT
	Standalone: csmars v5.3	Login: Administrator (pnadmin) :: Close
nter interface information:	Device Type: Cisco AP 4.x	
	→ *Device Name: AP1.3804	
Add Interface	→ *MAC Address: [n]:[17]:[DF]:[47]:[4F]:[F]]	
Name:	$\rightarrow \text{*MAC Address:} 00 : 17 : DF : A7 : 4F : E0$	
🗖 management		
		Cancel Submit
ap-manager		
🗖 virtual		
	Copyright © 2003–2007 Cisco Systems, Inc.	
	All rights reserved.	
	74 -	
	2 Done	A A A A A A A A A A A A A A A A A A A
Add Access Point	Edit Access Point Delete Access Point	
A Delet Merer	Design Delah Tura	
Access Point Name AP1.3804	Access Point Type Cisco AP 4.x	
AP2.3802	Cisco AP 4.x	
	(Dark	Discover
	🗇 Back	Discover Submit
		🔒 🧑 Internet

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



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

	•					,	MIN HELP
Event N	1anagement IP Management Service Ma	nagement	User Management			Aug 28, 2008 4:56:	16 AM PDT
₩ M	ANAGEMENT CS-MARS Standalone: csma	rs v5.3			Logi	n: Administrator (pnadmin) :: Logout ::	Activate
					_		
Search		/			E	dit Group Delete Group A	dd Group
escriptic	n / CVE:		All Cisco WLAN C	Controller 4.x		All	•
vent D	Description	CVE S Name	evenity Device Even			Groups	
	WLAN Host Blacklisted - Failed 80211 Auth	/ /	Cisco WLAN C	ontroller 4.x: WLA	N Host Blacklisted - Failed 80211 Auth	Info/Mitigation/WLAN	
	WLAN Host Blacklisted - Failed Association	4		ontroller 4.x: WLA	N Host Blacklisted - Failed Association	Info/Mitigation/WLAN 9	
912102	WLAN Host Blacklisted - Failed 802.1x Auth	/		ontroller 4.x: WLA	N Host Blacklisted - Failed 802.1x Auth	Info/Mitigation/WLAN 9	
	WLAN Host Blacklisted - Failed Web Auth	4		ontroller 4.x: WLA	N Host Blacklisted - Failed Web Auth	Info/Mitigation/WLAN	
	WLAN Host Blacklisted - IP Theft 9	6		ontroller 4.x: WLA	N Host Blacklisted - IP Theft	Info/Mitigation/WLAN	
912105	Rogue WLAN AP Detected On Wired Network 🖣			ontroller 4.x: Rogu	e WLAN AP Detected On Wired Network	Info/WLAN/RogueFound	
912106	Rogue WLAN AP Detected	6		ontroller 4.x: Rogu	e WLAN AP Detected	Info/WLAN/RogueFound	
912107	Adhoc WLAN Host Detected a	4	Cisco WLAN C	ontroller 4.x: Adho	c WLAN Host Detected	Info/WLAN/RogueFound	
912108	Rogue WLAN AP Removed	6	Cisco WLAN C	ontroller 4.x: Rogu	e WLAN AP Removed	Info/Misc/WLAN a	
912109	Managed WLAN AP Contained As A Rogue 🕯	4	Cisco WLAN C	ontroller 4.x: Mana	aged WLAN AP Contained As A Rogue	Info/Mitigation/WLAN @	
912110	Managed WLAN AP No Longer Contained As A Rogue	6	Cisco WLAN C Rogue	ontroller 4.x: Mana	aged WLAN AP No Longer Contained As A	Info/Misc/WLAN	
912111	WLAN Adhoc Auto Contained 🖣	4		ontroller 4.x: WLAI	N Adhoc Auto Contained	Info/Mitigation/WLAN	
912112	WLAN Adhoc No Longer Auto Contained	6	Cisco WLAN C	ontroller 4.x: WLA	N Adhoc No Longer Auto Contained	Info/Misc/WLAN a	
912113	Rogue WLAN AP Auto Contained	4		ontroller 4.x: Rogu	e WLAN AP Auto Contained	Info/Mitigation/WLAN	
912114	Rogue WLAN AP No Longer Auto Contained 🖣	6	Cisco WLAN C	ontroller 4.x: Rogu	e WLAN AP No Longer Auto Contained	Info/Misc/WLAN a	
912115	NetStumbler 3.2.0 Wireless Scanner Detected	4	Cisco WLAN C	ontroller 4.x: NetS	tumbler 3.2.0 Wireless Scanner Detected	Probe/Alla), Probe/WLANa	
.912116	NetStumbler 3.2.0 Wireless Scanner No Longer Detected ਕ੍ਰੀ	6	Detected		tumbler 3.2.0 Wireless Scanner No Longer		
.912117	NetStumbler 3.2.3 Wireless Scanner Detected	4		ontroller 4.x: NetS	tumbler 3.2.3 Wireless Scanner Detected	Probe/All @), Probe/WLAN @	
	NetStumbler 3.2.3 Wireless Scanner No Longer Detected 🖣	6	Detected		tumbler 3.2.3 Wireless Scanner No Longer		
912119	NetStumbler 3.3.0 Wireless Scanner Detected	4	Cisco WLAN C	ontroller 4.x: NetS	tumbler 3.3.0 Wireless Scanner Detected	Probe/Alla), Probe/WLANa	
	NetStumbler 3.3.0 Wireless Scanner No Longer Detected 🔄	6	Detected		tumbler 3.3.0 Wireless Scanner No Longer		
912121	Generic NetStumbler Wireless Scanner Detected 🖣	4	Cisco WLAN C	ontroller 4.x: Gene	eric NetStumbler Wireless Scanner Detecte	ed Probe/All@), Probe/WLAN@	
912122	Generic NetStumbler Wireless Scanner No Longer Detected	6	Longer Detect	ed	eric NetStumbler Wireless Scanner No	Info/Misc/WLAN	
.912123	Wellenreiter Wireless Scanner Detected	4	Cisco WLAN C	ontroller 4.x: Welle	enreiter Wireless Scanner Detected	Probe/Alla), Probe/WLANa	

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 E	vent 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 9-2Rules 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).

CISCO SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP Inspection Rules Drop Rules Aug 28, 2008 BisSection AH Aug 28, 2008 BisSection AH PDT Query / REPORTS Edit Group CS-MARS Standalone: comars v5.3 Login: Administrator (pnadmin) :: L	dudu												
Aug 28, 2008 Bit Sci 19 AM PD1 System: Configuration Issue System: Configuration Issue System: Configuration Issue System: Configuration Issue System: Section Bits System: Sectin Bits Bit	CISCO					SUMMARY	INCIDENTS	QUERY / REF		ILES MAN	AGEME	NT AD	MIN HELP
Butts CB-MARS Standalone: csmars v5.3 Login: Administrator (andmin) :: Larger: I Active spection Rules: View: Active : Edit Group Delete Group Add Group system: Configuration Issue system: Rotice Ration Rules: View: Active : Edit Group Delete Group Add Group System: Configuration Issue system: Rotice Ration Rules: View: Active : Edit Group Delete Group Add Group System: Configuration Issue system: Rotice Ration Rules: Image: Ration Ra		on Rules][,			28.200		
View: Active Edit Group Delete Group Add Group up: System: Configuration Issue System: NetWork Attacks and DoS System: NetWork Attacks and DoS System: NetWork Attacks and DoS System: Resource Issue System: Resource Issue System Rule: CS-MARS Failure Saving Certificates/Fingerprints Certificates A CS-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint, CE-MARS failed to Accept New SSH key Fingerprint, CE-MAR	<u>^</u>		e: csmars v5.3	I				Login: Adn	ninistrator				
System: configuration izour System: configuration izour Network Markes and Dos Network Markes and Dos System: item Repeated Network Resonances in the Reported Network Resonance is not Resonance is not Resonance is not Resonance in the Reported Network Resonace in the Reported Network Resonance in the Re	spection Rules:												
diff System: Hoat Advivy System: How Makers Outbrack (Ciso ICS) Usage Status: Advive System: How Makers Outbrack (Ciso ICS) Image: 0:1:10m System: Rew Makers Outbrack (Ciso ICS) Image: 0:1:10m System: Rew Makers Outbrack (Ciso ICS) Image: 0:1:10m System: Resource Issue System: Security Posture Compliance (Ciso NAC) Image: 0:1:10m System: Resource Issue System: Security Posture Compliance (Ciso NAC) Image: 0:1:10m System: Resource Issue System: Security Posture Compliance (Ciso NAC) Image: 0:1:10m System: Resource Issue System: Security Posture Compliance (Ciso NAC) Image: 0:1:10m System: Resource Issue System: System Rule: CS-MARS Failure Saving Certificates/Fingerprints Device Reported Keyword Severity Count Ices Operation Action: None Time Range: 0:1:10m Discord Image: 0:1:10m Description: This null 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. Fiet Open (System Rule: CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS Failed to Accept New SSH Certificates ANY None Image: 0:1:10m Rule Name: System Rule: CS-MAR	System: Configur	ation Issue		•		View:	Active -	Edit Gr	oup	Delete 0	iroup	Ac	ld Group
Avecami operational issue Note Time Range: 0:10m System: Resource Issue System: Resource Issue Time Range: 0:10m System: Resource Issue System: Resource Issue Time Range: 0:10m System: Resource Issue System: Resource Issue Device Reported Keyword Security and will result in didents to purged soon to create space for new events. The spectro is is normal CS-MARS activity and will result in didents to purged form CS-MARS actuations. Operation If the Name: System: Rule: CS-MARS Failure Saving Certificates/Fingerprints Device Reported Keyword Security Count) Close Operation If the Name: System Rule: CS-MARS Failure to save a new or changed device SL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings. Time Range: 0h:10m Time Range: 0h:10m CS-MARS Failure to save a new or changed device SL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings. Time Range: 0h:10m CS-MARS Failer to Accept New SSH Key Fingerprint, CS-MARS failure to accept due to SSL/SSH Settings. Ative If user System Rule: CS-MARS IFS Issenter Update Failure Settings: CS-MARS Settings. Note Time Range: 0h:10m Description: This rule indicates that one or m	dit System: Host Acti System: Network	Attacks and DoS											
Asystem: Resource IP Destination IP Service Name Event Any Any <td< td=""><td></td><td></td><td>ISCO ICS)</td><td>n Usage</td><td></td><td></td><td></td><td></td><td></td><td></td><td>Status</td><td>5:</td><td>Active</td></td<>			ISCO ICS)	n Usage							Status	5:	Active
ANY ANY ANY ANY C:S-MARS DB partition filling up causing the next partition to be purged soon ANY None ANY I Rule Name: System Rule: 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. Status: Active Feet Open (Source IP Destination IP Service Name Events Device Reported Keyword Severity Count J Close Depertion Rule Name: System Rule: CS-MARS TPS signature Update Failure Severity Explicit accept New SSL Certificate ANY None ANY 1 I Cional J Close Depertion Rule Name: System Rule: CS-MARS TPS ignature Update Failure Severity Explicit accept New SSL Certificate ANY None ANY 1 I Cional J Close Depertion Rule Name: System Rule: CS-MARS TPS signature update Failure Setatus: Active Time Range: 01:00n Time Range: 01:00n 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. CS-MARS Failed to download IPS signature package. CS-MARS Failed to download IPS signat	System: Resource System: Restricte System: Security	e Issue d Network Traffic Posture Complian	nce (Cisco NAC)	age. This is normal	filled up to 75% of its cap CS-MARS activity and wi	acity and the next da Il result in old events	tabase partit and incident	ion will be pur s to purged fr	rged soon t om CS-MAR	o create sp	ace for	new ever	nts. The
Rule Name: System Rule: CS-MARS Failure Saving Certificates/Fingerprints Status: Active Description: Time Range: 0h:10m Description: Time Range: 0h:10m Status: Active Time Range: 0h:10m Description: Time Range: 0h:10m Time Range: 0h:10m Status: ANY ANY ANY Description: Time Range: 0h:10m ANY ANY ANY ANY CS-MARS Failed to Accept New SSL Certificate ANY None ANY 1 Description: Time Range: 0h:10m Rule Name: System Rule: CS-MARS IPS Signature Update Failure Status: Active Time Range: 0h:10m Action: None MNY ANY ANY Any Any Active Time Range: 0h:10m Rule Name: System Rule: CS-MARS Failed to Accept New SSL Certificate ANY None ANY 1 Imme Carge: 0h:10m Rule Name: System Rule: CS-MARS IPS Signature Datas Acage. The carge of the carge	fset Open (source n	P Destination IP	Service Name	Event			Device		Keyword	Severity	Count) Close	Operation
Action: None Time Range: Dh: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 atom or automatic accept due to SSL/SSH Settings. Time Range: Dh:10m Seet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count J Close Operation Rule Name: System Rule: CS-MARS IPS signature Update Failure Status: Active Time Range: Dh: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. Time Range: Dh: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. Time Range: D: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. CS-MARS Failed to download IPS signature package. CS-MARS Failed to download IPS signature package. CS-MARS Failed to parse corrupted file from IPS signature package. CS-MARS Failed to download IPS signature package. CS-MARS Failed to download IPS signature package. CS-MARS Failed to	ANY	ANY	ANY	CS-MARS DB partition filling u	p causing the next partition	on to be purged soon	ANY	None	ANY	ANY	1		
Action: Description: Nne Time Range: Dh:10m Description: Time Range: Dh:10m Time Range: Dh:10m Description: Time Range: Device Reported Keyword Severity Could 1 Close Operation Set Open (Surver IP Destination IP Service Name Event Device Reported Keyword Severity (Could) Close Operation Rule Name: System Rule: CS-MARS Failed to Accept New SSL Certificate ANY None ANY 1 Close Operation 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 or other errors while updating signatures in CS-MARS failed to download IPS signature package. No: The cause of error can range from failure to download IPS signature package. Signature package. Could) Close Operation ANY ANY ANY ANY ANY CS-MARS failed to download IPS signature package. Could) Close Operation Could) Close Operation Could) Close Operation Could) Close Operation <	Rule Name:	System Rule: 0	CS-MARS Failure	Saving Certificates/Finge	rprints						Status	5:	Active
None ANY ANY C:S-MARS Failed to Accept New SSH Key Fingerprint, C:S-MARS Failed to Accept New SSL Certificate None ANY None ANY N' I I Active Rule Name: System Rule: C:S-MARS IPS signature Update Failure Status: Active Status: Active Image: Ima			es a CS-MARS fai	lure to save a new or changed	device SSL certificate or	SSH key fingerprint t	ased on exp	licit user actio	n or autom				
Rule Name: System Rule: CS-MARS Field to Accept New SSL Certificate Status: Active Action: None Time Range: Discription: Time Range: Discription: Feet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation Rule Name: System Rule: CS-MARS field to download IPS signature package due to connectivity issues with CCO or local server; corrupted signature package or other errors while updeting signatures in CS: Reported Keyword Severity Count) Close Operation Fiset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation Rule Name: System Rule: CS-MARS failed to download IPS signature package, CS-MARS failed to pack databases with IPS signature package, CS-MARS failed to pack database with IPS signature package, CS-MARS failed to pack databases with IPS signature package, CS-MARS failed to pack datab	fset Open (Source I	P Destination IP	Service Name	Frank			Device	Penorted	N	1			
Action: None Time Range: Dit10m Action: None Time Range: Dit20m Rule Name: System Rule: CS-MARS failed to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updated 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 updated 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 updated signature package. Device Reported Keyword Severity Count) Close Operation ANY ANY ANY CS-MARS failed to download IPS signature package, CS-MARS failed to download IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS failed to parse corrupted diabases with IPS signature package. ANY None ANY ANY CS-MARS failed to download IPS signature package. ANY None ANY ANY I				Event			bottee		Keyword	Severity	Count) Close	Operation
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 attemptive package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in can be applied to parse corrupted file from IPS signature package. The cause of error can attemptive package or other errors while updating package. The cause of error can attemptive package or other errors while updating signatures in can be applied to parse corrupted file from IPS signature package. Device Reported Keyword Severty Count J Close Operation Rule Name: System Rule: CS-MARS LC-GC Communication Figure 2 Certificate Mismatch Sever PS signature package. CS-MARS field to parse corrupted database with PS signature package. ANY None ANY Alve Active Action: None System Rule: CS-MARS LC-GC Communication Failure 2 Certificate Mismatch Status: Active Description: This rule indicates that the current CS-MARS Local Controller failed to communicate with this Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes. Prior to the past 6 minutes. Prior to the past 6 minutes. Severity Count J Close Operation feet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severty Count J Close Operation	ANY	ANY	ANY	CS-MARS Failed to Accept Net				User) Close	Operation
Arrange 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. Stet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation ANY ANY ANY ANY ANY CS-MARS failed to download IPS signature package, CS-MARS failed to update database with IPS signature package. ANY None ANY 1				CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net				User		ANY	1	-	
Rule Name: System Rule: CS-MARS failed to download IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS failed to parse corrupted file from IPS signature package, CS-MARS partially updated database with IPS signature package, CS-MARS partially updated database with IPS signature package, CS-MARS partially updated database with IPS signature package None ANY None ANY I I Rule Name: System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch Status: Active Action: None Time Range: 0h:01m the part 6 minutes, 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 not known. Reported Reported Keyword Severity Count) Close Operation	Rule Name:	System Rule: (CS-MARS IPS Sig	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure	w SSL Certificate		ANY	User None	ANY	ANY	1 Status Time I	s: Range:	Active 0h:10m
Rule Name: System Rule: C5-MARS failed to parse corrupted file from JPS signature package, C5-MARS partially updated database with JPS signature package Status: Active Rule Name: System Rule: C5-MARS LC-GC Communication Failure - Certificate Mismatch Status: Active Action: Nore Time Range: 0h:01m Description: This rule indicates that the current C5-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, control there shows not known. Reported Reported Keyword Seventy Count) Close Operation	Rule Name: Action:	System Rule: C None This rule indicate range from failu	CS-MARS IPS Sig es that one or mo ire to download IP	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure re errors were encountered wi	w SSL Certificate	tically download and O or local server, cor	ANY update CS-M	User None ARS with a ne	ANY w IPS sign	ANY ature pack	1 Status Time I	s: Range: e cause o	Active Oh:10m f error can
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. Time Range: 0h:01m fset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation	Rule Name: Action: Description:	System Rule: C None This rule indicate range from failu MARS database.	CS-MARS IPS Sig es that one or mo rre to download IP	CS-MARS Failed to Accept Nei CS-MARS Failed to Accept Nei jnature Update Failure re errors were encountered wi S signature package due to co	w SSL Certificate	tically download and i O or local server, cor	ANY update CS-M	User None ARS with a ne ture package Reported	ANY w IPS sign or other er	ANY ature pack- rors while u	1 Status Time I age. The	s: Range: e cause o' i signatur	Active 0h:10m ferror can es in CS-
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. Event Device Reported Keyword Severty Count) Close Operation	Rule Name: Action: Description: fset Open (Source II	System Rule: 0 None This rule indicate range from failu MARS database. P Destination IP	CS-MARS IPS Signed es that one or mo ire to download IP Service Name ANY	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net mature Update Failure re errors were encountered wi S signature package due to cc Event CS-MARS failed to download CS-MARS failed to parse corr CS-MARS failed to parse corr	w SSL Certificate	O or local server, cor ure package, package,	ANY update CS-M rupted signat	User None ARS with a ne ture package Reported User	ANY w IPS sign or other er	ANY ature pack- rors while i	1 Time I age. The updating Count	s: Range: e cause o' i signatur	Active 0h:10m ferror can es in CS-
the past 6 minutes, communication was either healthy or the status was not known. first Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation	Rule Name: Action: Description: ffset Open (Source II ANY	System Rule: C None This rule indicate range from failu MARS database. P Destination IP ANY	CS-MARS IPS Sig es that one or mo re to download IP Service Name ANY	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Instance Update Failure re errors were encountered wi S signature package due to cc Event CS-MARS failed to download 1 CS-MARS failed to parse corn CS-MARS failed to parse corn CS-MARS failed to parse dat CS-MARS partially updated dat	w SSL Certificate hile attempting to automa innectivity issues with CC PS signature package, upted fire from IPS signature tabase with IPS signature	O or local server, cor ure package, package,	ANY update CS-M rupted signat	User None ARS with a ne ture package Reported User	ANY w IPS sign or other er	ANY ature pack rors while u Severity ANY	1 Time I age. The updating Count	Range: cause or signatur) Close	Active 0h:10m ferror can es in CS- Operation
	Rule Name: Action: Description: ffset Open (Source II ANY Rule Name: Action:	System Rule: C None This rule indicat range from failu MARS database. P Destination IP ANY System Rule: C None	CS-MARS IPS Signed as that one or mo es that one or mo Service Name ANY	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Insture Update Failure re errors were encountered will S signature package due to co Event CS-MARS failed to download 1 CS-MARS failed to download CS-MARS failed to update dat CS-MARS partially updated da CS-MARS partially updated da	w SSL Certificate	O or local server, cor ure package, package, package	ANY update CS-M rupted signat Device ANY	User None ARS with a ne ture package Reported User None	ANY w IPS sign or other er Keyword ANY	ANY ature pack- rors while t Severity ANY	1 Status Time I age. The updating Count 1 Status Time I	S: Range: e cause or signatur) Close S: Range:	Active Oh:10m f error can es in CS- Operation Active Oh:01m
	Rule Name: Action: Description: ffset Open (Source II ANY Rule Name: Action: Description:	System Rule: C None This rule indicate range from failu MARS database. P Destination IP ANY System Rule: C None This rule indicate the past 6 minut	CS-MARS IPS Signed to a set of the one or mo es that one or mo Service Name ANY CS-MARS LC-GC es that the ourren tes, communicatio	CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Insture Update Failure re errors were encountered will S signature package due to cc Event CS-MARS failed to download I CS-MARS failed to parse corr CS-MARS failed to parse dat CS-MARS failed to parse dat CS-MARS failed to parse dat CS-MARS failed to parse dat CS-MARS partially updated da CC-MARS partially updated dat CS-MARS Local Controller fe	w SSL Certificate	O or local server, cor ure package, package, package	ANY update CS-M update CS-M Update d signar Device ANY Update to a certi	User None ARS with a neture package Reported User None ficate mismat Reported	ANY w IPS sign or other er Keyword ANY ch after 3 r	ANY ature pack- rors while e Severity ANY	1 Status Time I age. The updating Count 1 Status Time I the pas	Range: cause or signatur) Close : Range: t 6 minut	Active Dh:10m ferror can es in CS- Operation Active Dh:01m es. Prior to

Figure 9-14 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 9-15.

lulu Isco					SUMMAR		RY / REPORTS	RULES M	ANAGEMENT	MIN HELP
	rop Rules							A	ıg 28, 2008 8:44:	46 AM PDT
•	ARS Standalone: c	smars v5.3				Lo	gin: Administra		n) :: Logout ::	
Rule Name: Action: Description:	None	ue WLAN AP Detect		ts from a Cisco	o WLAN Con	troller.			Status: Time Range:	Active 0h:10m
set Open (Source)	P Destination IP	Service Name	Event		Device	Reported User	Keyword	Severity	Count) Close	e Operation
ANY Reporting Device	ANY	ANY	Info/WLAN/Rog	ueFound	ANY	ANY	ANY	ANY	1	
Toggle Equal					All Vari	ables			Search	
				्री == यो = Remove कि		ANY Unknown Reportin \$DEVICE01 \$DEVICE02 \$DEVICE03 \$DEVICE03 \$DEVICE05 \$DEVICE05 \$DEVICE06 \$DEVICE06 \$DEVICE08	ig Device			× ×
vyright © 2003–2007 C ights reserved.	isco Systems, Inc.				Sur	nmery :: Incidents :		Apply rts :: Rules :	Previous (Next

Figure 9-15 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 9-16).

Figure 9-16 CS-MARS WLAN-Specific Reports

ahaha	
CISCO	SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP
Query Batch Query Report	Aug 28, 2008 8:50:36 AM PDT
QUERY / REPORTS CS-MARS Standalone: csmars v5.3	Login: Administrator (pnadmin) :: Logout :: Activate
Load Report as On-Demand Query with Filter	Incident ID: Show
Select Report Activity: Vulnerable Host Found (Total View) Activity: Vulnerable Host Found via VA Scanner (Total View) Activity: WLAN Probes Detected (Total View) Activity: WLAN Route AP or Adhoe Hosts Detected (Total View)	Session ID: Show
Activity: WLAN Successful Mitogetons (Total View) Activity: WLAN Successful Mitogetons (Total View) Activity: Web Usage - Top Destinations by Systes (Total View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations by Sessions (Peak View) Activity: Web Usage - Top Destinations (Peak	Events Device Reported User Keyword Operation Rule Action ANY ANY ANY ANY ANY ANY ANY
	Save As Report Save As Rule Submit Inline
Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.	Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help
	7

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

ah	du												
	sco					SUM	MARY	INCIDENTS	QUERY / REPORTS	RULES	MANAGEMENT	ADMIN	HELP
Quer	'y Ba	atch Query R	leport								Aug 28, 2008 8	:59:21 A	M PDT
8	QUERY	/ REPORTS C	S-MARS Star	ndalone: csi	nars v5.3				Login: Administ	rator (pna	dmin) :: Logout	: Act	ivate
Load Report as On-Demand Query with Filter Incident ID: Show Select Group Regive AP or Adhoc Hosts Detected (Total View) Session ID: Show Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View) Image: Comparison of the session ID: Session ID: Show													_
		Event Data cells below to ch	ange query crit	eria:									
	Query	y type: Custor	n Columns r	anked by Ti	me, 0d-1h:00m Edit Clear								
	Sourc	e IP Desti	nation IP	Service	Events	Device	Reporte	d User	Keyword	Operat	ion Rule	Action]
	ANY	ANY		ANY	Info/WLAN/RogueFound	ANY	ANY		ANY	None	ANY	ANY	
(Query	Results 🖁 💥						S:	ave As Report	Expan	ve As Rule d All Coll	Submit apse All	
Repoi Devic		Event Type	Time		Raw Message								
AP1.3	304 🖻	Rogue WLAN AP Detected ① A	' Aug 28, 2008	8:15:00 AM PI	DT . 10.20.201.2 SNMPv2-MIB:ssyl SNMPv2-SMI::enterprises.14179 * SNMPv2-SMI::enterprises.14179.21.8.1. SMI::enterprises.14179.21.8.1. 0 SNMPv2-SMI::enterprises.141 SMI::enterprises.14179.2.1.7.1.	0.2.1.7.1.1.0 " 79.2.1.8.1.2.0 5.0 149 SNMP 27.0 15 SNMP 79.2.1.8.1.3.0	00 1E 44 1 SNMP v2-SMI: v2-SMI:	VE4 6E 0E " v2-SMI::ente enterprises. enterprises.	SNMPv2-SMI::ente erprises.14179.2.1 14179.2.1.8.1.7.0 14179.2.6.2.40.0 (rprises.14 8.1.6.0 "H -84 SNMP\ I SNMP\2-	179.2.1.8.1.1.0 "0 -REAPWLAN" SNM /2- SMI::enterprises.:	0 17 DF A: Pv2- L4179.2.6.	7 4F E0
AP2.3	802	Rogue WLAN AP Detected 🖣	+ Total: 2										
pod1-4 4.9e10	ap1250- J.2eac	Rogue WLAN AP Detected	+ Total: 2										
											1 to 3 of 3 25	per page	•
	ght © 2 its reser	003–2007 Cisco rved.	Systems, Inc.				Summ	nary :: Incide	ants :: Query / Rep	orts :: Rul	es :: Managemen	t :: Admin	:: Help

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

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).

C	sco					SUMMARY	INCIDENTS	QUERY / REPORTS RUL	ES MANAG	GEMENT AD	MIN HELP
)u	ery Batch (uery R	eport						Aug 28	, 2008 9:30:0	D3 AM PDT
2	QUERY / REPO	ORTS CS	S-MARS	Standalor	ne: csmars v5.3			Login: Administrator (pr	nadmin) ::	Logout ::	Activate
p	ort Selectior	I									
οι	ip: All				<u> </u>	hedule: All	•	Edit Group	Delete Grou	up Ad	d Group
di	System: FI	atabase Sei SMA Comp	liance Rep	orts	Report View HTML				_		
	System: H	LBA Compli IPAA Compl					Descript	on	Status	Submitted	Time Range
1		etwork Atta ew Malware perational I	Outbreak ssue npliance R nce	: (Cisco ICS	AN/RogueFound in Columns ranked by Time		Wireless-L hosts as d	ts lists all misbehaved AN hosts, APs and Adhoc etected and reported by a N Controller		Aug 28, 2008 9:25:08 AM PDT 1	
	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			t details AAA based g. to the network or to evices).	Not Run	Never	Never
Ŭ	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		(e.g. RAD access att mechanis network d	t details all failed AAA IUS, TACACS) based empts. Typically ms such as 802.1x, evice access, Cisco NAC ervers 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		failed AAA report cov regular AA IP and L3 An auther of policy r	t displays event details or a uthentications. This rers the following cases: AA auth, 802.1x auth, L2 IP auth, L2 802.1x auth, Lication may fail because nisconfiguration on the er or wrong user S.	n Not Run	Never	Never
× .	Activity: AAA Failed Auth - Top NADs	Run on demand only	Total View	None	Event type: Info/FailedAuth/AAA Query Type: Dostination IPs ranked by Sessions Time: 0d-1h:00m		Access De failed AAA report cov regular AA IP and L3 An auther of policy r	t ranks the Network vices (NADs) based on a uthentications. This rers the following cases: A auth, 802.1x auth, L2 IP auth, L2 802.1x auth, tication may fail because nisconfiguration on the r or wrong user S.	Not Run	Never	Never

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

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

_	ISCO						SUMMARY	INCIDENTS	QUERY / REPORTS		ANAGEMENT	ADMIN	HELP
Qu	iery Batch Que	ry Repoi	t							A	ug 28, 2008 9	32:26 AM	1 PDT
Ē	QUERY / REPORT	IS CS-M.	ARS Sta	ndalone: c	smars v5.3				Login: Administr	ator (pnadmin) :: Logout	:: Activ	/ate
эp	oort Selection												
ro	up: System: Netw	ork Attacks	and DoS		¥		Schedule: Al	v	Edit Group	Delete	Group	Add Gro	oup
Ed	lit Delete	Duplicate	Add	Resub	nit View Report	View HTML	*						
	Name	Schedule	Format	Recipients	Query		Description			Status	Submitted	Time Ra	nge
	Activity: Sudden Traffic Increase To Port - All Destinations	Run on demand only	Total View	None	Event type: Sudden increase a port Query Type: Custom Column Time Time: 0d-1h:00m		behavior by suc	denly receiv	ing statistically	Not Run	Never	Never	
~	Activity: Sudden Traffic Increase To Port - All Sources		Total View	None	Event type: Sudden increase a port Query Type: Custom Column Time Time: 0d-1h:00m		behavior by suc	denly sendin	g statistically	Not Run	Never	Never	
~	Activity: WLAN DoS Attacks Detected	Run on demand only	Total View	None	Event type: DoS/Network/W/ Query Type: Custom Column Time Time: 0d-1h:00m			ittacks (e.g. E ociation and o	ther flood	Not Run	Never	Never	
0	Activity: WLAN Probes Detected	Run on demand only	Total View	None	Event type: Probe/WLAN Query Type: Custom Column Time Time: 0d-1h:00m	ns ranked by		er and Weller	nreiter scanners)	Not Run	Never	Never	
~	Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/Rogu Query Type: Custom Column Time Time: 0d-1h:00m			Adhoc hosts			Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2 8:24:00 a PDT - Au 2008 9:2 AM PDT	AM g 28,
~	Attacks: Network DoS - Top Event Types	Run on demand only	Total View	None	Event type: DoS/Network/TC DoS/Network/UDP, DoS/Dist DoS/Network/ICMP, DoS/Ne DoS/NetworkDevice, DoS/Ne Query Type: Event Types ra Sessions Time: 0d-1h:00m	ributed, twork/Misc, stwork/WLAN	attacks may inc	enial of servi dude crashing levice such a reasing netwo	ce attempts. Such or rebooting an s router, firewall ork load by	Not Run	Never	Never	
Ed	it Delete	Duplicate	Add	Resub	nit View Report	View HTML	*						
											1 to 6 of 6 25	per page	¥
	vright © 2003-200								nts :: Ouery / Rep				

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

Select the report of interest and, unless the report was recently generated, click Resubmit. Step 3 To view the newly generated report, click View Report (see Figure 9-20).

	ISCO					SUMMARY INCIDENTS QU	ERY / REPORTS	RULES M.	ANAGEMENT	ADMIN HELP
ļu	ery Batch Que	ry Repo	t					Au	g 28, 2008 9:	37:36 AM PDT
3	QUERY / REPORT	\$ CS-M	ARS Sta	ndalone: c	smars v5.3	Lo	gin: Administra	stor (pnadmin)	:: Logout	:: Activate
	ort Selection									
51	up: System: Netw	ork Attacks	and DoS		•	Schedule: All	Edit Group	Delete	Group	Add Group
di	it Delete	Duplicate	Add	Resub	mit View Report View HTML	•			-	-
-	Name			Recipients		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	behavior by suddenly receiving s	tatistically	Not Run	Never	Never
	Activity: Sudden Traffic Increase To Port - All Sources		Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	behavior by suddenly sending sta	atistically	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- service (DoS) attacks (e.g. Broad Null Probe, Association and other attacks) as reported by a Cisco V Controller	dcast Deauth, flood			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- (e.g. Netstumbler and Wellenreit as reported by a Cisco WLAN Co	er scanners) ntroller	Finished: Aug 28, 2008 9:37:32 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 hosts, APs and Adhoc hosts as de reported by a Cisco WLAN Contro	etected and oller	Finished: Aug 28, 2008 9:25:10 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/Mics, Dos/Network/Device, Dos/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m	This report ranks attacks that rep network wide denial of service at attacks may include crashing or 1 i inline network device such as rou or switch or increasing network li creating TCP, UDP or ICMP traffi	tempts. Such rebooting an Jter, firewall oad by	Not Run	Never	Never
Edi	it Delete	Duplicate	Add	Resub	nit View Report View HTML	•				
									1 to 6 of 6 25	per page 💽

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

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

I





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.

٩, 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 Tes	t 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#wp1345 692

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/cf gCustm.html

General Network Security

• Network Security Baseline

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