



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 | | WIRELESS | <u>S</u> ECURITY | MANAGEMENT | C <u>O</u> MMANDS | HELP |
| Management | SNMP Sy | stem Su | mmary | | | - | Ap | ply |
| Summary | Name | | wlc-2106-br | • | | | | |
| SNMP General SNMP V3 Users | Location | | SW-Branch | | | | | |
| Communities Trap Receivers Trap Controls | Contact | | | | | | | |
| Trap Logs | System D | escriptio | n Cisco Control | ler | | | | |
| HTTP Telnet-SSH | System O | bject ID | 1.3.6.1.4.1.9. | 1.828 | | | | |
| Serial Port | SNMP Port | t Numbei | 161 | | | | | |
| Local Management Users User Sessions | Trap Port | Number | 162 | | | | | |
| Logs | SNMP v1 | Mode | Enable 💌 | | | | | |
| Mgmt Via Wireless Frech Support | SNMP v2c | Mode | Disable 💌 | | | | | |
| | SNMP v3 M | Mode | Enable 💌 | | | | | |
| 0 | | | | | | | 10.00.001 | - <i>(</i>) |

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

| | | | | 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 | | | | | |
| Communities 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 | | | | | | | |
| E Tech Support | | | | | | | |
| | | | | | | | |
| Communities Trap Receivers Trap Controls Trap Logs HTTP Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless Tech Support | IP Mask Access Mode Status | 255.255.255.2 | 55 | | | | |

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).

| | | | | | | Sa Sa | a <u>v</u> e Config | guration | <u>P</u> ing | Logout <u>R</u> efres |
|-------------------------------|-----------------------|-------------|------------|------------------|------------------|------------|---------------------|-----------|---------------|-------------------------|
| CISCO | MONITOR <u>W</u> LANS | | WIRE | LESS | <u>S</u> ECURITY | MANAGEME | NT C <u>O</u> | MMANDS | HE <u>L</u> P | |
| Management | SNMP Trap Contr | ols | | | | | | | | Apply |
| Summary | Miscellaneous Trap | IS | Auto I | RF Pro | file Traps | 8 | 02.11 S | ecurity 1 | Fraps | |
| SNMP | SNMP Authenticat | tion | I 1 | .oad Pro | file | | WEP WEP | Decrypt E | rror | |
| General SNMP V3 Users | 🗹 Link (port) Up/Do | wn | | Noise Pr | ofile | | 🗹 IDS | Signature | Attack | |
| Communities Trap Receivers | 🔽 Multiple Users | | Г 1 | Interfere | nce Profile | | | | | |
| Trap Controls | 🔽 Rogue AP | | | Coverag | e Profile | | | | | |
| HTTP | 🗹 Config Save | | Auto I | RF Upd | late Traps | | | | | |
| Telnet-SSH | Client Related Trap | s | | Channe | el Update | | | | | |
| Serial Port | 🗌 802.11 Associatio | 'n | V | Tx Pow | er Update | | | | | |
| Local Management Users | 🗌 802.11 Disassoci | ation | | ranc | | | | | | |
| User Sessions | 🗌 802.11 Deauthen | tication | | raps Icor Aut | hantiantian | | | | | |
| 🕨 Logs | 🔲 802.11 Failed Aut | hentication | | | Servers Not D | ecoording | | | | |
| Mgmt Via Wireless | 🗌 802.11 Failed Ass | ociation | | (MD103 | 361 761 3 1400 6 | Cosponding | | | | |
| 🕨 Tech Support | Exclusion | | | | | | | | | |
| | Cisco AP Traps | | | | | | | | | |
| | 🗹 AP Register | | | | | | | | | |
| | ☑ AP Interface Up/I | 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 | ick | 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).

| aha | du. | | | SUMMA | | QUERY / REPORTS | RULES | MANAGEMENT | ADMIN | HELP |
|------------------------|---|-----------------------|-------------------|--------------|-----------------|----------------------|-----------|-------------------|------------|---------|
| Euctor | | Hone Management | Ruston Davamotors | Euston Fotus | | | | Aug 21, 2009 0 | 11.01.05 | H BDT |
| 8 | ADMIN CS-MARS Standalone: | csmars v5.3 | System rarameters | | | Login: Administrat | or (pnad | min) :: Logout | :: Acti | vate |
| 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



| w Setun System Maintenanc | e liser Management System Pa | rameters Cust | am Setun | INCIDE | ROLES ROLES | Aug 28, 2008 4:53:47 AM PDT |
|-------------------------------|------------------------------|---------------|---------------|---------------|--------------------------|------------------------------|
| ADMIN CS-MARS Standalon | e: csmars v5.3 | uncers cuse | Sin Secup | | Login: Administrator (pr | admin) :: Logout :: Activate |
| | | | | | | · <u> </u> |
| | | | | | | |
| ecurity and Monitoring Inforr | nation | | | | | |
| Searc | h | | | | | |
| | | | | | | \frown |
| Edit Change Version | Load From Seed File | | | | ¢ | Back Delete Add |
| Device Name | Device Type | Agents | Access IP | Reporting IP | Monitoring Networks | Device Display |
| asa-2 | Cisco ASA 8.0 | | 10.20.30.32 | 10.20.30.32 | | <u>.</u> |
| basic | Cisco ASA 8.0 | | | | | |
| engineering | Cisco ASA 8.0 | | | | | |
| system-asa-2 | Cisco ASA 8.0 | | | | | |
| ITadmin | Cisco ASA 8.0 | | | | | |
| ips-asa-2 | Cisco IPS 6.x | | | 10.20.30.33 | | |
| ips-3845-2 | Cisco IPS 6.x | | | 10.20.200.30 | | |
| ips1-4255 | Cisco IPS 5.x | | | 10.20.30.55 | | |
| pod1-wism-2-1 | Cisco WLAN Controller 4.x | | 10.20.100.150 | 10.20.100.150 | | |
| pod1-ap1250-4.9e1d.2eac | Cisco AP 4.x | | | | | |
| wlc-2106-br | Cisco WLAN Controller 4.x | | 10.20.201.2 | 10.20.201.2 | | |
| AP2.3802 | Cisco AP 4.x | | | | | |
| AP1.3804 | Cisco AP 4.x | | | | | |
| | | | | | | |
| | | | | | | 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).

| hada. | | | | | | |
|---|---|---------------------------------|-----------------------|------------------------|------------------|--------|
| ISCO | | SUMMARY INCIDENTS | QUERY / REPORTS | RULES MANAGEM | ENT ADMIN | HELP |
| stem Setup System Maintenance Us | er Management System Paramete | 's Custom Setup | | Aug 27, 20 | 08 9:57:00 AM | PDT |
| 3 ADMIN CS-MARS Standalone: csm | nars v5.3 | | Login: Administra | itor (pnadmin) :: Lo | gout :: Activ | vate |
| 1. Enter the reporting IP (the IP address wher 2. * denotes a required field. Device Type: Cisco ASA 7.0 Cisco Switch-CatOS ANY Cisco Switch-CatOS ANY Cisco Switch-CatOS ANY Cisco VPN Concentrator 4.7 → * Device Cisco VPN Concentrator 4.7 Cisco VPN Cisco | re events originated from) to ensure that t | he system processes the events. | | | | |
| → *Access Type: | Generic V Select V 3DES V | | | | | |
| Login: Password: | | | | | | |
| Enable Password: | | | | | | |
| Config Path: | |] | | | | |
| File Name: SNMP RO Community: | | | | | | |
| → Monitor Resource Usage: | NO | | | | | |
| | | | ⇔ Back | Discover | Next | |
| yright © 2003–2007 Cisco Systems, Inc. ights reserved. | | Summary :: Incid | dents :: Query / Repo | rts :: Rules :: Manage | ment :: 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 | 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 |] | | | | | | |
| inter interface information: Add Interface Name: | Remove Interface/IP | Network Mask: | | | | | | |
| Add Interface Name: Imanagement | Remove Interface/IP IP Address: | Network Mask: | | Add IP/Netwo | erk Mask |] | | |
| inter interface information: Add Interface Name: IV management | Remove Interface/IP IP Address: 10 {20 {201 }2 | Network Mask: 255 {255 {255 }0 | | Add IP/Netwo | ork Mask |] | | |
| inter interface information: Add Interface Name: IV management | Remove Interface/IP IP Address: 10 {20 {201}2 | Network Mask: 255 (255)(255)0 | | Add IP/Netwo | ork Mask |] | | |
| Inter interface information: Add Interface Name: Image: Image: | Remove Interface/IP IP Address: 10 20 201 2 | Network Mask: 255 (255 (255 (0 | | Add IP/Netwo | ork Mask ⇔Back | Disco | ver | t |
| Inter interface information: Add Interface Name: Imanagement | Remove Interface/IP IP Address: | Network Mask: 255 (255 (255 (0 | | Add IP/Netwo | rk Mask ⇔Back | Disco | ver Nex | t |
| Add Interface Add Interface Name: Imanagement | Remove Interface/IP IP Address: 10 20 201 2 | Network Mask: 255 (255 (255 0 | | Add IP/Netwo | rk Mask ⇔Back | 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.

| ahah | |
|--|---|
| CISCO | SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP |
| System Setup System Maintenance User Management System Parameters Custom Setup | Aug 21, 2008 7:41:57 AM PDT |
| ADMIN CS-MARS Standalone: csmars v5.3 | Login: Administrator (pnadmin) :: Logout :: Activate |
| | |
| ote: 1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the event 2. A decrete exercised Could Find | 5. |
| 2. * denotes a required field. | |
| Device Type: Cisco WLAN Controller 4.x | |
| | |
| → *Device Name: wlc-2106-br | |
| → Access IP: 10 20 201 2 | |
| → Reporting IP: 10 20 201 2 | |
| → *Access Type: | |
| SNMP PO Community | |
| | |
| | |
| | |
| Enter interface information: | |
| Add Interface Remove Interface/IP | |
| Name: IP Address: Network Mask: | |
| | Add 10 /blotwork Mack |
| | |
| ap-manager 10 201 3 255 255 0 | Add IP/Network Mask |
| □ virtual 1 1 1 1 1 | Add IP/Network Mask |
| | |
| | |
| | |
| Add Access Point Edit Access Point Delete Access Point | |
| Aug Access Found Edit Access Found Delete Access Point | |
| Access Point Name Access Point Type | |
| | |

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 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 | 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: | 1n 42n 42n1 42 | | |
| → Reporting IP: | Attps://10.20.30.34 - [csmars] WLAN Controller Context/Module-Cisco AP 4.x | - Microsoft Internet Explorer | - 🗆 |
| → *Access Type: | ululu cisco | | |
| SNMP RO Community: | | Aug 27, 2008 10:21:53 AM PI | DT |
| | Standalone: csmars v5.3 | Login: Administrator (pnadmin) :: Clo | se |
| | | | |
| ter interface information: | Device Type: Cisco AP 4.x | | |
| | → *Device Name: AP1.3804 | | |
| Add Interface | | | |
| Name: | → "MAL Address: 00 : 17 : DF : A7 : 4F : E0 | | |
| 🗖 management | | | |
| | | Cancel Submit | |
| ap-manager | | | |
| 🗖 virtual | | | |
| | Convright @ 2003-2007 Cisco Systems, Inc. | | |
| | All rights reserved. | | |
| | (199) _ | | |
| | Done | 🔄 🔁 👹 Internet | |
| Add Access Point | Edit Access Point Delete Access Point | | |
| | | | |
| Access Point Name | Cisco AP 4.x | | |
| AP2.3802 | Cisco AP 4.x | | |
| | | | |
| | | | |
| | r | | |

| | 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

| junton in zona na | | | | | | | | |
|---|----------|--|--|--|-----|--|--|--|
| alada | | | SUMMARY INCIDENTS QUERY | REPORTS RULES MANAGEMENT ADMIN HE | ELP | | | |
| CISCO | * | line Management | | Aug 20, 2000, 4/5(-1/, AN D | DT | | | |
| | nagement | Oser management | | Mug 20, 2000 4.30.10 MH PI | | | | |
| MANAGEMENT CS-MARS Standalone: csma | rs v5.3 | | Login: | Administrator (pnadmin) :: Logout :: Activat | e. | | | |
| | | | | | | | | |
| Search | | | Edi | t Group Delete Group Add Group | р | | | |
| escription / CVE: | (| All Cisco WI AN Controller 4 x | 1) | | T I | | | |
| vent Description | CVE | Severity Device Event ID | | Groups | - | | | |
| | Name | A circumstant constanting a second state | half the state of the second state | | | | | |
| 912100 WLAN Host Blacklisted - Failed 80211 Auth[g] | | CISCO WLAN CONTroller 4.X: WLAN Host E | lacklisted - railed 80211 Auth | Info/Mitigation/WLAN[9] | | | | |
| VIZIUL WLAN Host Blacklisted - Failed Association [9] | | CISCO WLAN CONTroller 4.X: WLAN Host E | lacklisted - railed Association | Info/Mitigation/WLAN[9] | _ ! | | | |
| 912102 WLAN Host Blacklisted - Failed 802.1x Auth[q] | | CISCO WLAN CONTroller 4.X: WLAN Host E | lacklisted - Falled SU2.1X Auto | Info/Mitigation/WLAN[q] | - 1 | | | |
| 712103 WLAN Host Blacklisted - Failed Web Auth g | | CISCO WLAN CONTroller 4.x: WLAN Host E | lacklisted - Falled Web Auth | Info/Mitigation/WLAN[9] | | | | |
| 12104 WLAN Host Blacklisted - IP Theft[g] | 4 | CISCO WLAN CONTroller 4.X: WLAN Host E | lacklisted - IP Inett | Info/Mitigation/WLAN[q] | | | | |
| 12105 Rogue WLAN AP Detected On Wired Network | | CISCO WLAN CONTroller 4.X: Rogue WLAN | Cisco WLAN Controller 4.x: Rogue WLAN AP Detected On Wired Network | | | | | |
| 12106 Rogue WLAN AP Detected [9] | | CISCO WLAN CONTroller 4.X: Rogue WLAN | AP Detected | Info/WLAN/RogueFoundig | | | | |
| 12107 Adhoc WLAN Host Detected a | 4 | CISCO WLAN CONTROLLEY 4.X: Adhoc WLAN | Host Detected | Info/WLAN/RogueFound[q] | | | | |
| 12108 Rogue WLAN AP Removed[q] | (| CISCO WLAN Controller 4.X: Rogue WLAN | AP Removed | Info/Misc/WLAN[q] | | | | |
| 12109 Managed WLAN AP Contained As A Rogue | | Cisco WLAN Controller 4.x: Managed WL | AN AP Contained As A Rogue | Info/Mitigation/WLAN[g] | | | | |
| 12110 Managed WLAN AP No Longer Contained As A Rogue | (| Cisco WLAN Controller 4.x: Managed WL Rogue | AN AP No Longer Contained As A | Into/Misc/WLAN(g) | | | | |
| 12111 WLAN Adhoc Auto Contained 9 | | Cisco WLAN Controller 4.x: WLAN Adhoo | Auto Contained | Info/Mitigation/WLAN | | | | |
| 12112 WLAN Adhoc No Longer Auto Contained | (| Cisco WLAN Controller 4.x: WLAN Adhoc | No Longer Auto Contained | Info/Misc/WLAN | | | | |
| 12113 Rogue WLAN AP Auto Contained | | Cisco WLAN Controller 4.x: Rogue WLAN | AP Auto Contained | Info/Mitigation/WLAN | | | | |
| 12114 Rogue WLAN AP No Longer Auto Contained | (| Cisco WLAN Controller 4.x: Rogue WLAN | AP No Longer Auto Contained | Info/Misc/WLAN | | | | |
| 12115 NetStumbler 3.2.0 Wireless Scanner Detected | | Cisco WLAN Controller 4.x: NetStumbler | 3.2.0 Wireless Scanner Detected | Probe/All q), Probe/WLAN q | | | | |
|) 12116 NetStumbler 3.2.0 Wireless Scanner No Longer Detected (| (| Cisco WLAN Controller 4.x: NetStumbler Detected | 3.2.0 Wireless Scanner No Longer | Info/Misc/WLAN @ | | | | |
| 912117 NetStumbler 3.2.3 Wireless Scanner Detected | ė | Cisco WLAN Controller 4.x: NetStumbler | 3.2.3 Wireless Scanner Detected | Probe/All], Probe/WLAN] | | | | |
| 912118 NetStumbler 3.2.3 Wireless Scanner No Longer Detected | (| Cisco WLAN Controller 4.x: NetStumbler Detected | 3.2.3 Wireless Scanner No Longer | Info/Misc/WLAN | | | | |
| 912119 NetStumbler 3.3.0 Wireless Scanner Detected 🖪 | | Cisco WLAN Controller 4.x: NetStumbler | 3.3.0 Wireless Scanner Detected | Probe/Alla), Probe/WLANa | | | | |
| 212120 NetStumbler 3.3.0 Wireless Scanner No Longer Detected 🔄 | (| Cisco WLAN Controller 4.x: NetStumbler Detected | 3.3.0 Wireless Scanner No Longer | Info/Misc/WLAN a | | | | |
| 리그리그 Generic NetStumbler Wireless Scanner Detected 예 | | Cisco WLAN Controller 4.x: Generic Net | stumbler Wireless Scanner Detected | Probe/Alla), Probe/WLANa | | | | |
| 912122 Generic NetStumbler Wireless Scanner No Longer Detected | (| Cisco WLAN Controller 4.x: Generic Nets Longer Detected | tumbler Wireless Scanner No | Info/Misc/WLAN a | | | | |
| 912123 Wellenreiter Wireless Scanner Detected 🖣 | | Cisco WLAN Controller 4.x: Wellenreiter | Wireless Scanner Detected | Probe/All@, Probe/WLAN@ | | | | |

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

Event Groups Featuring WLAN Events

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

| Table 9-1 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 9-2 Rules Based on WLAN Events

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

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

To view the details of a CS-MARS rule:

Step 1 Navigate to RULES.

Step 2 Scroll down the list to find the rule.

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

| Submark Nuclebris Build Outer / Reports Build Add Group Full Configuration lissue Full Full Configuration lissue Full Full Configuration lissue Full Full Configuration lissue Full Full Full Configuration lissue Full Full Full Full Full Configuration lissue Full <p< th=""><th>dudu</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></p<> | dudu | | | | | | | | | | | | |
|--|--|--|---|--|---|---|--|--|---|--|---|--|---|
| Reletion fulles Aug 20, 2008 (size) Aug 20, 2008 (size) Aug 20, 2008 (size) System: Configuration issue Image: Adving and avg 20, 2008 (size) System: Souther South Size Image: Adving and avg 20, 2008 (size) System: Souther South Size Image: System: Souther South Size System: South South Size Image: Size System: South Size Size System: South Size Image: Size Sys | CISCO | | | | | SUMMARY | INCIDENTS | QUERY / REF | | ILES MAN | AGEME | NT AD | MIN HELP |
| Test CS-MARS Standalone: csmars v5.3 Login: Administrator (packing): g: Login: g: Login: Administrator (packing): g: Login: Gin: A | Inspection Rules Dr | on Rules | | | | | |][, | | Aug | 28.200 | 18 8:36:1 | 9 AM PDT |
| System: Revenue I between the lower of the server of the s | S RULES CS-MA | RS Standalone | e: csmars v5.3 | I | | | | Login: Adn | ninistrator | (pnadmin) | :: Lo | gout :: | Activate |
| up: System: Configurational Issue View: Active Edit Group Delete Group Add Group System: Redwork (Caso LS) System: Redwork (Caso LS) Image: System: Redwork (Caso LS) | spection Rules: | | | | | | | | | | | | |
| All System: Database Server Advivy System: Reconsistence Status: Advive System: Reconsistence System: Reconsistence Time Range: 0h:10m System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsistence Time Range: 0h:10m System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsistence System: Reconsiste | oup: System: Operation System: Configur | ation Issue | | • | | View: | Active - | Edit Gr | oup | Delete 0 | iroup | Ac | ld Group |
| It system: New Maker Cuttors & (Ciso 1CS) It usage Status: A dive Dissign: Communication of the Maker Cuttors & (Ciso 1CS) In usage Time Range: 0::::::::::::::::::::::::::::::::::: | dit System: Databas System: Host Acti System: Network | e Server Activity ivity Attacks and DoS | | | | | | | | | | | |
| Asystem: Reconnaissance Time Range: 0h:10m System: Resource issue Bestime: Secure issue Time Range: 0h:10m System: Restricted Network: Traffic System: Secure issue Device Reported Keyword Severity Count) Close Operation System: Restricted Network: Traffic System: Secure issue System: Restricted Network: Traffic System: Secure issue Device Reported Keyword Severity Count) Close Operation System: Rule: CS-MARS DB partition filling up causing the next partition to be purged soon ANY None ANY ANY ANY CS-MARS Failure Saving Certificates/Fingerprints Status: Active Action: None Time Range: 0h:10m Time Range: 0h:10m Time Range: 0h:10m Time Range: 0h:10m System: Rule: CS-MARS Failure to save a new or changed device SSL certificate or SSH key fingerprint, CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS failed to | R System: New Main System: Operation | ware Outbreak (C nal Issue | ISCO ICS) | n Usage | | | | | | | Status | 5: | Active |
| Sect Openic Reported Repor | A System: Reconna System: Resource System: Restricte System: Security | issance e Issue d Network Traffic Posture Complian | nce (Cisco NAC) | database partition 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 RS databas | Time I ace for e. Users | Range: new ever are urge | 0h:10m nts. The ed to archive |
| ANY ANY ANY ANY CS-MARS DB partition filling up causing the next partition to be purged soon ANY None ANY ANY 1 Rule Name: System Rule: CS-MARS Failure Saving Certificates/Fingerprints Status: Active Action: None Time Range: 0h:10m Enscription: This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint, based on explicit user action or automatic accept due to SSU/SSH Settings. Secting 10:10m Feed Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) D Cose Open (ANY ANY ANY ANY ANY CS-MARS Failed to Accept New SSH Key Fingerprint, CS-MARS With a new IPS signature package, CS-MARS Failed to package 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 Key Fingerprint, CS-MARS Failed to Package Accep | fset Open (source n | P Destination IP | Service Name | Event | | | Device | Reported User | Keyword | Severity | Count |) Close | Operation |
| Rule Name: System Rule: C5-MARS Failure Saving Certificates/Fingerprints Status: Active Action: None Time Range: 0h:10m Description: Time landicates a C5-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. Time Range: 0h:10m fset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation ANY ANY ANY ANY C5-MARS Failed to Accept New SSL Key Fingerprint, ANY None ANY None ANY I Image: Operation Rule Name: System Rule: C5-MARS IPS Signature Data Failed to Accept New SSL Certificate ANY None ANY None ANY Image: Op:10m Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update C5-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package. Compacting failure to accept the to to connective is supparting to automatically download and update C5-MARS with a new IPS signature package. C: S-MARS Failed to pareation Device Reported Keyword S | 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: 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 action or automatic accept due to SSU/SSH Settings. Set [Open { Service IP] Destination IP] Service Name Event Device Reported Keyword Severity [Count] Close Dperation Rule Name: System Rule: CS-MARS Failed to Accept New SSL Certificate ANY None ANY ANY CS-MARS Failed to Accept New SSL Certificate ANY None ANY ANY ANY CS-MARS Failed to Accept New SSL Certificate ANY None ANY ANY ANY CS-MARS Failed to Accept New SSL Certificate ANY None ANY ANY ANY CS-MARS failed to Accept New SSL Certificate ANY None Time Range: 0h:10m Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package or other errors while update gate gate. Trans failed to download IPS signature package. Signature package. None ANY ANY Co-MARS failed to parse corrupted fignature package. None ANY I Co-MARS failed to parse corrupted fignature p | Rule Name: | System Rule: 0 | CS-MARS Failure | Saving Certificates/Finge | rprints | | | | | | Status | 5: | Active |
| Seet Open (Service IP Destination IP Service Name Event Device Reported Keyword Severity Count) Elose Operation ANY ANY ANY ANY CS-MARS Failed to Accept New SSH Key Fingerprint, ANY None ANY ANY I | Action: Description: | None This rule indicate | 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 | natic accept | Time I due to | Range: SSL/SSH | 0h:10m Settings. |
| ANY ANY ANY ANY CS-MARS Failed to Accept New SSL Key Fingerprint, CS-MARS Failed to Accept New SSL Certificate ANY None ANY ANY I Rule Name: System Rule: CS-MARS IPS Signature Update Failure Status: Active Time Range: 0h:10m Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package or other errors while updating signatures package. The cause of error can MARS database. fset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation fset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation rstatus: ANY ANY ANY CS-MARS failed to download IPS signature package, CS-MARS parially updated database with IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS failed to update database with IPS signature package, C | fset Open (Source I | P Destination IP | Service Name | Frank | | | Device | Penorted | N | 1 | | | |
| Rule Name: System Rule: C5-MARS IPS Signature Update Failure Status: Active Action: None Time Range: 0h:10m Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package or other errors while updating signatures package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS failed to download IPS signature package, CS-MARS failed to download IPS signature package, CS-MARS failed to update database with IPS signat | | | | Event | | | bottee | User | Keyword | Severity | Count |) Close | Operation |
| Action: None Time Range: 0h:10m Description: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package or other errors while updating signatures act age. The cause of errors MARS distabase. feet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation feet Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity Count) Close Operation Key Mark ANY ANY ANY CS-MARS failed to download IPS signature package, CS-MARS failed to update database with IPS signature package, CS-MARS LC-GC Communication Failure - Certificate Mismatch ANY ANY ANY Min 1 1 1 1 1 fisted Open (Source IP Source IP Severity CS-MARS LC-GC Communica | ANY | ANY | ANY | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net | w SSH Key Fingerprint, w SSL Certificate | | ANY | None | ANY | ANY | Count |) Close | Operation |
| Description: This rule indicates that one or more errors were encountered while attempting to automatically download update CS-HARS with a new IPS signature package. The cause of error can find the to download IPS signature package to encountered while update signature package or other errors while update signature package. The cause of error can find the to download IPS signature package to the errors while update signature package. The cause of error can find the to download IPS signature package. fset Open (Source IP Destination IP Service Name Event Device Reported IVSER Keyword Severity Count J Close Operation Image: ANY ANY ANY CS-HARS failed to pack contrupted life inform IPS signature package, CS-HARS failed to update database with IPS signature package, CS-HARS Local Controller failed to communicate with IPS signature package, CS-HARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retrise over the past 6 minutes, Prior to the past 6 minutes, communication was either healthy or the status was not known. Device Reported Keyword Severity Gout J Close Operation iset Open (Severity C Severity C Severity C Sever | ANY Rule Name: | ANY System Rule: 0 | ANY | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure | w SSH Key Fingerprint, w SSL Certificate | | ANY | None | ANY | ANY | 1 Status |) Close | Operation Active |
| Ifset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severty Count) Close Open (or pressure) ANY ANY ANY ANY CS-HARS failed to parse compted finding from IPS signature package, CS-HARS failed to update database with IPS signature package, CS-HARS failed to update matching to update the update the update the update database with IPS signate update | ANY Rule Name: Action: | ANY System Rule: 0 None | ANY CS-MARS IPS SIG | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure | w SSH Key Fingerprint, w SSL Certificate | | ANY | None | ANY | ANY | Count 1 Status Time I |) Close | Operation Active 0h:10m |
| ANY ANY CS-MARS failed to download IPS signature package, CS-MARS failed to update database with IPS signature package, Description: This rule indicates that the current CS-MARS 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, communicate with GC due to certificate mismatch after 3 retries over the past 6 minutes. This rule indicates for the past 6 minutes. Prior to the past 6 minutes, communicate with GC due to certificate mismatch AMY None ANY 1 failed to communicate with GC due to certificate mismatch ANY None ANY ANY 1 | ANY Rule Name: Action: Description: | ANY System Rule: 0 None This rule indicate range from failu MARS database. | ANY CS-MARS IPS Signs sthat one or mo re to download IP | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure re errors were encountered wi S signature package due to cc | w SSH Key Fingerprint, w SSL Certificate hile attempting to automa nnectivity issues with CC | tically download and O or local server, cor | ANY update CS-M | None ARS with a ne | ANY w IPS sign or other er | ANY ature pack | 1 Status Time I age. The updating |) Close 5: Range: e cause o i signatur | Active 0h:10m f error can es in CS- |
| Rule Name: System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch Status: Active Action: None Time Range: 0h:01m Description: This: rule indicates that the current CS-MARS LC-GC Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 review rule past 6 minutes. Prior to the past 6 minu | ANY Rule Name: Action: Description: fset Open (Source II | ANY System Rule: 0 None This rule indicate range from failu MARS database. P Destination IP | ANY SS-MARS IPS Sig es that one or mo re to download IP Service Name | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Inature Update Failure re errors were encountered w S signature package due to oc Event | w SSH Key Fingerprint, w SSL Certificate hile attempting to automa nnectivity issues with CC | tically download and i O or local server, cor | ANY update CS-M rupted signar | ARS with a ne ture package | ANY ANY w IPS sign or other er | ANY ature pack- rors while i | Count 1 Status Time I age. The updating Count |) Close S: Range: e cause or i signatur) Close | Active Oh:10m f error can es in CS- Operation |
| 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. Device Reported Keyword Severity [Count] Operation fset Open (Source IP Destination IP Service Name Event Device Reported Keyword Severity [Count] Operation ANY ANY ANY CS-MARS LC failed to communicate with GC due to certificate mismatch ANY None ANY 1 | ANY Rule Name: Action: Description: fset Open (Source II ANY | ANY System Rule: C None This rule indicate range from failu MARS database. P Destination IP ANY | ANY S-MARS IPS Signer es that one or mo re to download IP Service Name ANY | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net Science (CS-MARS Failed to Accept Net ere errors were encountered wi S signature package due to co Event CS-MARS failed to download CS-MARS failed to parse corr CS-MARS failed to parse corr | w SSH Key Fingerprint, w SSL Certificate hile attempting to automa nnectivity issues with CC PS signature package, pued file from JPS signature abase with JPS signature | tically download and O or local server, cor ure package, package, package | ANY ANY Device ANY | ARS with a ne ture package Reported User None | ANY W IPS sign or other er Keyword ANY | ANY ANY ature pack- rors while i Severity ANY | Count 1 Status Time I age. The updating Count 1 |) Close | Active Oh:10m f error can es in CS- Operation |
| the past 6 minutes, communication was either healthy or the status was not known. Open (Source Reported Keyword Severity Count) Close Operation ANY ANY ANY CS-MARS LC failed to communicate with GC due to certificate mismatch ANY None ANY 1 | ANY Rule Name: Action: Description: fset Open (Source II ANY Rule Name: | ANY System Rule: E None This rule indicate range from failu MARS database. P Destination IP ANY System Rule: E | ANY S-MARS IPS Sig es that one or mo to download IP Service Name ANY S-MARS LC-GC | CS-MARS Failed to Accept Nei CS-MARS Failed to Accept Nei pature Update Failure re errors were encountered wi S signature package due to co Event CS-MARS failed to download I CS-MARS failed to parse corr CS-MARS failed to parse corr CS-MARS failed to parse dor CS-MARS failed to parse dor CS-MARS failed to parse dor CS-MARS failed to parse dor | w SSH Key Fingerprint, w SSL Certificate hile attempting to automa nnectivity issues with CC PS signature package, puted file from JPS signature tabase with JPS signature ertificate Nismatch | tically download and O or local server, cor ure package, package, p package | ANY update CS-M rupted signar Device ANY | ARS with a ne ure package Reported User None | ANY ANY Keyword ANY | ANY ANY ature pack. rors while u Severity ANY | Count 1 Status Time I age. The updating Count 1 Status |) Close S: Range: a cause or a signatur) Close | Active 0h:10m f error can es in CS- Operation Active |
| ANY ANY CS-MARS LC failed to communicate with GC due to certificate mismatch ANY None ANY ANY 1 | Rule Name: Action: Description: ifset Open (Source II ANY Rule Name: Action: Description: | ANY System Rule: C None This rule indicat; mARS database, P Destination IP ANY System Rule: C None This rule indicat; | ANY CS-MARS IPS Sig es that one or mo to download IP Service Name ANY S-MARS LC-GC es that the curren | CS-MARS Failed to Accept Nei CS-MARS Failed to Accept Nei CS-MARS Failed to Accept Nei re errors were encountered wi S signature package due to co Event CS-MARS failed to parse corr CS-MARS | SSH Key Fingerprint, v SSL Certificate hile attempting to automa nmedtivity issues with CC PS signature package, pted file from IPS signature dabase with IPS signature entificate Nismatch lied to communicate with | tically download and O or local server, cor ure package, package, package, its Global Controller | ANY update CS-M rupted signal Device ANY | ARS with a ne ture package Reported User None | ANY w IPS sign or other er Keyword ANY ch after 3 r | ANY ature pack- rors while e Severity ANY etries over | Count 1 Status Time I age. The updating Count 1 Status Time I the pas |) Close Range: e cause or signatur) Close | Active Dh:10m f error can es in CS- Operation Active Dh:01m es. Prior to |
| | Rule Name: Action: Description: Ifset Open (Source II ANY Rule Name: Action: Description: fset Open (Source II | ANY System Rule: (None This of le indicate MARS database P Destination IP ANY System Rule: (None This rule indicate the past 6 minute () Destination IP Destination IP | ANY CS-MARS IPS Sig es that one or mo re to download IP Service Name ANY S-MARS LC-GC es that the curren as, communicable (Service Name | CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net CS-MARS Failed to Accept Net re errors were encountered will S signature package due to co Event CS-MARS failed to download I CS-MARS failed to download I CS-MARS failed to parse corn CS-MARS partially updated do Communication Failure - C t CS-MARS Local Controller fa n was either healthy or the sta Event | SSH Key Fingerprint, w SSL Certificate hile attempting to automa nnectivity issues with CC PS aignature pael age, updat file from IPS agnature tabase with IPS signature ertificate Mismatch iled to communicate with two was not known. | tically download and O or local server, cor ure package, package, package its Global Controller of | ANY Jpdate CS-M rupted signal Device ANY lue to a certi Device | ARS with a neture package Reported User None Reported Rep | ANY w IPS sign or other or Keyword ANY ch after 3 r keyword | ANY ature pack- rors while u Severity ANY etries over Severity | Count 1 Status age. The age. The age. The status Time I Status Time I the pas Count |) Close Close Close Close Close Close Close Close | Active Operation Active Operation Active Oh:01m es. Prior to Operation |

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.

| huhu usco | | | | | SUMMAR | | RY / REPORTS | RULES M | ANAGEMENT | MIN HELP |
|---|--|-------------------|----------------|--------------------------------|----------|---|-----------------|-------------------------|------------------------|----------------------|
| spection Rules D | rop Rules | | | | | | | Au | 19 28, 2008 8:44: | 46 AM PDT |
| RULES CS-MA | ARS Standalone: c | smars v5.3 | | | | Lo | gin: Administra | ator (pnadmir | n) :: Logout :: | Activate |
| Rule Name: Action: Description: | System Rule: Rog None This rule detects Ro | ue WLAN AP Detect | ed | ; from a Cisco | WLAN Con | troller. | | | Status: Time Range: | Active 0h:10m |
| set Open (Source) | IP Destination IP | Service Name | Event | | Device | Reported User | Keyword | Severity | Count) Close | e Operation |
| ANY | ANY | ANY | Info/WLAN/Rogu | eFound | ANY | ANY | ANY | ANY | 1 | |
| Reporting Device | es Select All | | | | All Vari | ables | | | Search | |
| ANY | | | | (d) == (d) i= Ramove (b) | View | ANY Unknown Reportin \$DEVICE01 \$DEVICE02 \$DEVICE03 \$DEVICE03 \$DEVICE03 \$DEVICE05 \$DEVICE06 \$DEVICE07 \$DEVICE08 | ig Device | | | • |
| ⊃yright © 2003–2007 C rights reserved. | cisco Systems, Inc. | | | | Sur | nmary :: Incidents : | Query / Repo | Apply rts :: Rules : | Previous [| Next dmin :: Help |

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: VLAN POSS Detected (Total View) Activity: VLAN Poss Detected (Total View) | Session ID: Session ID: |
| Activity: WLAN Successful Mitigations (Total View) Activity: WLAN Successful Mitigations (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 by Sessions (Peak View) Activity: Web Usage - Top Destinations (Peak View) Activity: Web Usage - Top Sessions (Peak View) Activity: Web Web Research (Peak View) Activity: We | Events Device Reported User Keyword Operation Rule Action ANY ANY ANY ANY ANY None 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 | | | | | | | | | | | | | A |
|---|---|-----------------------------|---------------|--------------|--------------------------|----------|----------|---------------|---------------------|-------------|--------------------------|--------------------|----------|
| CIS | sco | | | | | SUM | MARY | INCIDENTS | QUERY / REPORTS | RULES | MANAGEMENT | ADMIN | HELP |
| Quei | ry Ba | atch Query R | eport | | | | | | - | | 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 Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View) Session ID: Show | | | | | | | | | | | w w | | |
| C | Query Event Data Click the cells below to change query criteria: | | | | | | | | | | | | |
| | Query | type: Custor | n Columns r | anked by Ti | me, 0d-1h:00m Edit Clear | | | | | | | | |
| | Sourc | e IP Desti | nation IP | Service | Events | Device R | Reported | l User | Keyword | Operat | ion Rule | Action |] |
| | ANY | ANY | | ANY | Info/WLAN/RogueFound | ANY A | ANY | | ANY | None | ANY | ANY | |
| (|)uery | Results 🖁 💥 | | | | | | Si | ave As Report | Sa Expan | ve As Rule d All Coll | Submit apse All | |
| Repoi Devic | rting e | Event Type | Time | | Raw Message | | | | | | | | |
| AP1.3804 Detected 🔐 | | | | | | | | 2.44.0 | | | | | |
| AP2.3 | 802 | Rogue WLAN AP Detected 🖣 | + Total: 2 | | | | | | | | | | |
| pod1-4 4.9e10 | ap1250- 1.2eac | Rogue WLAN AP Detected | + Total: 2 | | | | | | | | | | |
| | | | | | | | | | | | 1 to 3 of 3 25 | per page | × |
| Copyri All righ | ght © 2 its reser | 003–2007 Cisco ved. | Systems, Inc. | | | | Summa | ary :: Incide | ents :: Query / Rep | orts :: Rul | es :: Managemen | t :: Admin | :: Help |

| Figure 9-17 | Sample CS-MARS Roque 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 9-18).

| C | isco | | | | | SUMMARY | INCIDENTS QUERY / REPORTS RUL | S MANA | GEMENI | MIN HELP |
|-----|---|---|--|--------------------------------|--|---------------|---|---|--|---|
| Qu | uery Batch (| Query R | eport | | | | | Aug 28 | , 2008 9:30: | 03 AM PDT |
| ĺ | QUERY / REP | ORTS CS | S-MARS | Standalon | e: csmars v5.3 | | Login: Administrator (pr | admin) :: | Logout :: | Activate |
| (et | port Selection | ı | | | | | | | | |
| iro | up: All System: D | atabase Se | rver Activi | itγ | | Schedule: All | Edit Group | Delete Gro | up Ac | ld Group |
| EC | Nan System: F Nan System: G System: H | ISMA Comp LBA Compli IPAA Comp | liance Rep ance Rep liance Rep | orts orts orts | - Report View HIML | - | Description | Status | Submitted | Time Range |
| ¢ | Activ System: N Rogl System: N Adhd System: O Dete System: P System: R System: R | ost Activity etwork Atta ew Malware perational I CI DSS Cor econnaissar esource Iss | cks and D Outbreak ssue npliance R nce ue | oS : (Cisco ICS) leports | _AN/RogueFound m Columns ranked by Tim | e | This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller | Finished: Aug 28, 2008 9:25:10 AM PDT | Aug 28, 2008 9:25:08 AM PDT 1 | 3 Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT |
| 0 | Activity: AAA Based Access - All Events | Run on demand only | Total View | None | Event type: Info/SuccessfulLogin/AAA Query Type: Custom Columns ranked by Tim Time: 0d-1h:00m | ie | This report details AAA based access (e.g. to the network or to specific devices). | Not Run | Never | Never |
| 0 | 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 Tim Time: 0d-1h:00m | e | This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control | Not Run | Never | Never |
| 0 | Activity: AAA Failed Auth - All Events | Run on demand only | Total View | None | Event type: Info/FailedAuth/AAA Query Type: Custom Columns ranked by Tim Time: Od-1h:00m | e | This report displays event details or failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth, An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials. | n Not Run | Never | Never |
| 0 | Activity: AAA Failed Auth - Top NADs | Run on demand only | Total View | None | Event type: Info/FailedAuth/AAA Query Type: Destination IPs ranked by Sessi Time: Dd-11:00m | DINS | This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, 12 IP and L3 IP auth, 12.802.1x auth, An authentication may fail because of policy misconfiguration on the AAA server or wrong user | Not Run | Never | Never |
| | | | | | | | LI EUCIIUGIS. | | | |

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).

| ery Batch Que | PV Denoi | | | | | | | |
|---|--------------------------|---------------|------------|---|--|--|-----------------------------------|---|
| | ry Kepu | rt | | | | Au | 1g 28, 2008 9: | 32:26 AM PDT |
| QUERY / REPORT | \$ CS-M. | ARS Sta | ndalone: c | smars v5.3 | Login: Administ | rator (pnadmin |) :: Logout | 11 Activate |
| ort Poloction | | | | | | | | |
| STC Selection | | | | | | | | |
| ip: System: Netw | ork Attacks | and DoS | | | Schedule: All Edit Group | Delete | Group | Add Group |
| t Delete | Duplicate | Add | Resubr | mit View Report View HTML | • | | | |
| Name | Schedule | Format | Recipients | Query | Description | Status | Submitted | Time Range |
| Activity: Sudden Traffic Increase To Port - All Destinations | Run on demand only | Total View | None | Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m | This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic. | Not Run | Never | Never |
| Activity: Sudden Traffic Increase To Port - All Sources | Run on demand only | Total View | None | Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m | This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic. | Not Run | Never | Never |
| Activity: WLAN DoS Attacks Detected | Run on demand only | Total View | None | Event type: DoS/Network/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m | This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller | Not Run | Never | Never |
| Activity: WLAN Probes Detected | Run on demand only | Total View | None | Event type: Probe/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m | This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller | Not Run | Never | Never |
| Activity: WLAN Rogue AP or Adhoc Hosts Detected | Run on demand only | Total View | None | Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m | This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller | Finished: Aug 28, 2008 9:25:10 AM PDT | Aug 28, 2008 9:25:08 AM PDT | Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT |
| Attacks: Network DoS - Top Event Types | Run on demand only | Total View | None | Event type: DoS/Network/TCP, DoS/Network/UDP, DoS/Network/Mic, DoS/Network/UDP, DoS/Network/MicA DoS/NetworkDevice, DoS/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m | This report ranks attacks that represent network wide denial of service attempts. Such attacks may include creating or rebooting an inline network device such a router, frewall or switch or increasing network load by creating TCP, UDP or ICMP traffic. | Not Run | Never | Never |
| t Delete | Duplicate | Add | Resubr | nit View Report View HTML | • | | | |
| | | | | | | | 1 to 6 of 6 25 | per page 💽 |

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).

| CIS | | _ | | | | | 30MMART INCIDEN | QUERT / REFORM | KOLES M | | ADMIN |
|------------------------|--|--------------------------|---------------|------------|--|--|---|---|--|-----------------------------------|---|
| luer | y Batch Que | ry Repoi | rt∥ | | | | | | Au | ig 28, 2008 9: | 37:36 AM PDT |
| \$ | QUERY / REPORT | \$ CS-M. | ARS Sta | ndalone: c | smars v5.3 | | | Login: Administr | ator (pnadmin |) :: Logout | Activate |
| | | | | | | | | | | | |
| epor | t Selection | | | | | | | | | | |
| oup | : System: Netw | ork Attacks | and DoS | | • | | Schedule: All | Edit Group | Delete | Group | Add Group |
| dit | Delete | Duplicate | Add | Resubn | nit View Re | port View H | TML - | | | | |
| Né | ame | Schedule | Format | Recipients | Query | | Description | | Status | Submitted | Time Range |
| C Ac Tr Po De | tivity: Sudden affic Increase To rt - All estinations | Run on demand only | Total View | None | Event type: Sudden a port Query Type: Custor Time Time: 0d-1h:00m | increase of traffi n Columns ranke | c to This report lists hosts th behavior by suddenly re d by significant volume on a traffic. | at exhibit anomalous ceiving statistically FCP/UDP port or ICMP | Not Run | Never | Never |
| O Ac Tr Po | tivity: Sudden affic Increase To rt - All Sources | Run on demand only | Total View | None | Event type: Sudden a port Query Type: Custor Time Time: 0d-1h:00m | increase of traffi n Columns ranke | c to This report lists hosts th behavior by suddenly se d by significant volume on a traffic. | at exhibit anomalous nding statistically FCP/UDP port or ICMP | Not Run | Never | Never |
| O Ac Do Do | tivity: WLAN S Attacks stected | Run on demand only | Total View | None | Event type: DoS/Ne Query Type: Custor Time Time: 0d-1h:00m | twork/WLAN n Columns ranke | This reports lists all the d by service (DoS) attacks (e Null Probe, Association a attacks) as reported by Controller | Wireless-LAN denial of .g. Broadcast Deauth, Ind other flood a Cisco WLAN | Finished: Aug 28, 2008 9:36:42 AM PDT | Aug 28, 2008 9:36:40 AM PDT | Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT |
| O Ac Pr | tivity: WLAN obes Detected | Run on demand only | Total View | None | Event type: Probe/1 Query Type: Custor Time Time: 0d-1h:00m | VLAN n Columns ranke | This reports lists all the d by (e.g. Netstumbler and W as reported by a Cisco V | Wireless-LAN probes ellenreiter scanners) VLAN Controller | Finished: Aug 28, 2008 9:37:32 AM PDT | Aug 28, 2008 9:37:30 AM PDT | Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT |
| C Ac Ro Ac De | tivity: WLAN Igue AP or Ihoc Hosts stected | Run on demand only | Total View | None | Event type: Info/Wl Query Type: Custor Time Time: 0d-1h:00m | AN/RogueFound n Columns ranker | This reports lists all mist d by hosts, APs and Adhoc ho reported by a Cisco WLA | ehaved Wireless-LAN sts as detected and N Controller | Finished: Aug 28, 2008 9:25:10 AM PDT | Aug 28, 2008 9:25:08 AM PDT | Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT |
| D At Do Ty | tacks: Network IS - Top Event pes | Run on demand only | Total View | None | Event type: DoS/Net DoS/Network/UDP, DoS/Network/ICMP DoS/NetworkDevice Query Type: Event Sessions Time: 0d-1h:00m | twork/TCP, DoS/Distributed, DoS/Network/Mi DoS/Network/W Types ranked by | This report ranks attack network wide denial of s sc, attacks may include cra- 'LAN inline network device su or switch or increasing r creating TCP, UDP or IC | s that represent ervice attempts. Such shing or rebooting an ch as router, firewall etwork load by MP traffic. | Not Run | Never | Never |
| Edit | Delete | Duplicate | Add | Resubr | nit View Re | port View H | TML - | | | | |
| | [| | | | | | | | | 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 L | 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.

| Iable 5-4 Iest beu naiuwale aliu Soltwale | Table 9-4 | Test Bed Hardware | and Software |
|---|-----------|-------------------|--------------|
|---|-----------|-------------------|--------------|

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

Reference Documents

Cisco Unified Wireless

Cisco Wireless

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

- Cisco Wireless Control System (WCS) http://www.cisco.com/en/US/products/ps6305/index.html
- Managing Rogue Devices

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