



CHAPTER 25

Cisco Wireless LAN Controller

Cisco Secure MARS supports the collection, parsing, and analysis of SNMP security traps generated by Cisco Wireless Controller, version 4.x and 5.x devices. In addition, MARS includes this event data in new and existing reports and rules.

The following system rules support Cisco Wireless Controller devices:

- System Rule: WLAN DoS Attack Detected
- System Rule: Operational Issue: WLAN



Tip

If you need to customize the count or time range of this or system rule, clone the system rule, edit the clone to fit your requirements, and then disable the corresponding system rule.

- System Rule: Rogue WLAN AP Detected

The following system reports support Cisco Wireless Controller devices:

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



Note

Because MARS does not perform a MAC address lookup for an IP address that appears in events from other reporting devices, the inspection rules cannot always correlate different types of events (for example, a Probe/WLAN and a DoS/Network/WLAN type of event). Whenever an event type is mapped to an existing event group already used in rules with multiple offsets, some source IP-based or destination IP address-based correlation rules may not work because the WLAN event does not contain a meaningful IP.

The following bugs apply to this feature set:

- **CSCsj19199**—WLAN: deleted device still show up Query as "Unknown Reporting Device"

If a user deletes a device from the MARS web interface (Admin > Security and Monitoring Devices page) and clicks Activate, MARS will report any future events (syslog, SNMP traps, etc.) received from that device as Unknown Reporting Device. To prevent these events from appearing, configure the device in question to stop sending events to MARS.

- **CSCsk71706**—WLAN: IP not in MARS DB should be define at IP Management

Any IP address that is not already in the MARS database can result in an "unknown device" in pop up windows. For example, in the Event Type: WLAN Radius Server Timeout click on Destination IP. For the IP address to properly display, you must add these addresses in IP Management tab to reflect the actual topology.

This chapter contains the following topics:

- [WLAN Configuration Overview, page 25-2](#)

WLAN Configuration Overview

To enable an access point as a reporting device in MARS, you must identify the Cisco Wireless LAN Controller (WLAN Controller) as the reporting device. The WLAN Controller receives alerts from the access points that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the WLAN Controller that forwarded it; however, a MAC address is found within the body of many of the SNMP traps and those MAC addresses correspond to access points. Therefore, MARS requires host definitions for each of the access points that can potentially trigger an event. These definitions are added as sub-components under the device definition of the WLAN Controller through either discovery of the controller or manual definition of the access point.

You are required to define the WLAN Controller; however, you are not required to define each agent (access point). The MARS Appliance attempts to discover access points as alerts they generate are forwarded by the WLAN Controller, eliminating the need to manually define the access points. MARS parses the alert to identify the access point hostname. MARS uses this information to add any undefined agents as children of the WLAN Controller as a host. The default topology presentation for discovered access points is within a cloud.



Note

The first SNMP notification from an unknown access point appears to originate from the WLAN Controller. MARS parses this notification and defines a child agent of the WLAN Controller using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the access point.

If a MAC address cannot be attributed to a discovered or defined access point, the event is attributed to the WLAN controller. Some traps do not include access point information, such as the MAC address. Such events are also attributed to the WLAN controller.

To configure MARS to collect and parse events generated by a Cisco WLAN Controller device, you must perform the following tasks:

1. Bootstrap the WLAN Controller device to generate the required events and to allow MARS to discover its settings and retrieve the events.
2. Represent the WLAN Controller device in the MARS web interface.

—or—

Define the WLAN Controllers using a seed file. For information on using seed files, see [Adding Multiple Reporting and Mitigation Devices Using a Seed File, page 1-34](#).


3. Discover or manually define the access points managed by the WLAN controller.

Bootstrap the WLAN Controller

To prepare the WLAN controller, you must:

- Enable SNMPv1 so that discovery works.
- Define the MARS appliance as a SNMP receiver.
- Define an SNMP community string for use by MARS.
- Verify all required SNMP traps are enabled.

To bootstrap the WLAN Controller to send SNMP events to the Local Controller, follow these steps:

-
- Step 1** In the WLAN Controller user interface, select **Management > SNMP > General**, and enable SNMP v1.
- Step 2** Select **Management > SNMP > Trap Receivers**.
- Step 3** Click **New** and define the MARS appliance as a trap receiver by specifying the following values
- **Name**—Enter the name of the MARS appliance.
 - **IP Address**—Enter the IP address of the appliance.
 - **Status**—Set to enable.
- Step 4** To define the SNMP communities value, select **Management > SNMP > Communities**.
-  **Note** This value is required when you define the WLAN controller in the MARS web interface.
-
- Step 5** To selectively enable/disable traps, select **Management > SNMP > Trap Controls**. Verify the traps are being generated for the receiver that represents the MARS appliance.
-

Add a Cisco Wireless LAN Controller to MARS

Before you can identify the access points, you must add the Cisco Wireless LAN Controller to MARS. All access points forward notifications to the WLAN Controller, and the WLAN Controller forwards SNMP notifications to MARS. Once you define the WLAN Controller and activate the device, MARS can discover the access points that are managed by that WLAN Controller. However, you can also choose to manually add the access points.

To configure MARS to receive SNMP traps from the WLAN Controller device, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Select **Cisco WLAN Controller 4.x** from the Device Type list.



Note If you are running version 5.x, select Cisco WLAN Controller 4.x. The 5.x version support is a full implementation, including all events defined in 4.x as well as all new events found in version 5.0.

The Enter interface information area appears at the bottom of the page and the login information disappears.

- Step 3** Specify values for the following fields:

- **Device Name**—Specify the name of this controller.
- **Access IP**—Required to enable MARS to discover settings from the controller device, including the list of managed access points, enter the administrative IP address in the Access IP field.
This IP address is the one assigned to the management interface on the controller.
- **Reporting IP**—Enter the IP address of the interface that publishes SNMP notifications in the Reporting IP field
- **Access Type**—Select SNMP.
- **SNMP RO Community**—Required for discovery to enable MARS to retrieve values of the MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.

Before you can specify the SNMP RO string, you must define an access IP address. MARS uses the SNMP RO string to discover device and network settings.

- Step 4** Click **Add Interface** and specify the name, IP address, and mask values for at least one interface. Typically, this required interface information corresponds to the management IP (access IP), reporting IP, or both.



Note At a minimum, you must defined the administrative interface for the WLAN controller.

- Step 5** Do one of the following:
- To discover the controller settings and all access points associated with the controller, click **Discover**
 - To manually define access points, continue with [Manually Define Access Points, page 25-4](#).

- Step 6** To save your changes, click **Submit**.

- Step 7** To enable MARS to start mapping events from this device, click **Activate**.

MARS does not sessionize SNMP traps receive from the WLAN controller because sessionization does not work with MAC addresses. When a trap is received, MARS parses it and creates an event. Because very few traps from a WLAN controller include IP addresses, sessionization does not occur. System inspection rules use event type groups. Therefore, when an event belonging to an event type group in an inspection rule is generated, that rule fires.



Tip The Device name is updated after successful discovery of WLAN controller.

Manually Define Access Points

Access points are automatically discovered as the controller receiver and forwards notifications from the access points to MARS. However, you can manually add an access point as a child of the WLAN Controller device. This feature allows you to represent all of your access points, even if they have not generated any notifications.

To manually define access points, follow these steps:

- Step 1** Click **Admin > System Setup > Security and Monitor Devices**.

- Step 2** From the list of devices, select the host running Cisco WLAN Controller 4.x, and click **Edit**
- Step 3** (Optional) Click **Add Access Point** and specify the following values for at least one access point:
- **Device Name**—Identifies the name of this access point as it will appear under the Access Point Name list on the WLAN controller device page.
 - **MAC Address**—Identifies the MAC address of the access point.
- Step 4** To create the access point and save your changes, click **Submit**.
- Step 5** To save your changes to the controller, click **Submit**.
- Step 6** To enable MARS to start parsing events from this device, click **Activate**.
-

