



# CHAPTER 16

## Extreme ExtremeWare 6.x

---

MARS can use Extreme ExtremeWare switches to enforce L2 mitigation. To configure MARS to communicate with an ExtremeWare switch, you must configure the switch to publish SNMP notifications to the MARS Appliance. In addition, you must add and configure the switch in the web interface.

This chapter contains the following topics:

- [Configure ExtremeWare to Generate the Required Data, page 16-1](#)
- [Add and Configure an ExtremeWare Switch in MARS, page 16-1](#)

## Configure ExtremeWare to Generate the Required Data

To bootstrap an ExtremeWare switch, you must configure two features. First, you must configure the switch to send syslog messages to the MARS Appliance. Next, you must configure the SNMP RO community for MARS to access available L2 information.

To prepare the ExtremeWare device to generate the data required by MARS, follow these steps:

---

**Step 1** For syslog configuration, add this command:

```
configure syslog add <MARS's IP address> local7 debug
enable syslog
```

**Step 2** For SNMP configuration add these commands:

```
enable snmp dot1dTpFdbTable
configure snmp delete community readonly all
configure snmp delete community readwrite all
configure snmp add community readonly encrypted <encrypted community string>
configure snmp add community readwrite encrypted <encrypted community string>
```

---

## Add and Configure an ExtremeWare Switch in MARS

To add and configure an ExtremeWare switch in MARS, follow these steps:

---

**Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.

- Step 2** Select **Extreme ExtremeWare 6.x** from the Device Type list.
- Step 3** Enter the name of the device in the Device Name field.
- MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.
- Step 4** (Optional) To enable MARS to discover settings from this device, enter the administrative IP address in the Access IP field.
- To learn more about the access IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- Step 5** Enter the IP address of the interface that publishes syslog messages, SNMP notifications, or both in the Reporting IP field.
- To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#).
- Step 6** If you entered an address in the Access IP field, select **SNMP** from the Access Type list.
- For more information on understanding the access type, see [Selection of the Access Type, page 1-11](#).
- Step 7** (Optional) To enable MARS to retrieve 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 read MIBs related to a reporting device's CPU usage, network usage, and device anomaly data and to discover device and network settings.
- Step 8** To add this device to the MARS database, click **Submit**.
- The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.
- Step 9** Click **Activate**.
- MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion.
-