



CHAPTER 1

Configuring Reporting and Mitigation Devices in MARS

Cisco Security Monitoring, Analysis, and Response System (MARS) operates by analyzing the event streams of other network devices. These network devices play one of two roles in the MARS system: *reporting devices* that provide details about network activities and attacks, or *security devices* that can report about network activities as well as stop an attack using an access control list or policy rule to block the traffic. This guide describes how to prepare these reporting and mitigation devices so that they play an effective role in the MARS system.

This chapter contains the following topics:

- [Preparation Overview, page 1-1](#)
- [Bootstrap Summary Table, page 1-3](#)
- [Understanding Access IP, Reporting IP, and Interface Settings, page 1-10](#)
- [Selection of the Access Type, page 1-11](#)
- [Activate the Reporting and Mitigation Devices, page 1-15](#)
- [Discovering Your Network: Layer 3 Topology Discovery, page 1-15](#)
- [Scheduling Topology Updates, page 1-18](#)
- [Configuring Resource Usage Data, page 1-21](#)
- [Adding Reporting and Mitigation Devices, page 1-31](#)

Preparation Overview

Reporting devices follow a simple preparation process:

1. Determine which messages for that device type are parsed by MARS.
2. Enable the audit of those messages that MARS parses.
3. If required, identify the Local Controller appliance as a target for the audit messages.
4. If supported, enable SNMP RO community sharing with MARS.
5. Add that reporting device in the MARS web interface (tell MARS where it is and what format the logs will be in).

Security devices include these five steps and enabling write access to the devices via an administrative username/password and specified connection type (SSH, SNMP, or Telnet).

Taskflow for Adding Devices to MARS

This checklist focuses on the easiest population approach to MARS. The recommended taskflow provides MARS with the most accurate delineation of your network as quickly as possible.

Step 1 Prepare all Devices that Support SNMP

The fastest way to populate MARS is through network discovery. During discovery, MARS can identify the layer 3 security and reporting devices, populate the network topology it uses to determine attack paths, and begin collecting data about typical network loads. However, to make this discovery truly effective, you must prepare the layer 3 devices you want MARS to monitor. You should also prepare any layer 2 devices that you plan to add, however, these devices are not automatically discovered. You must manually define the layer 2 devices.

SNMP RO strings are provided for all devices able to share information. Events are enabled and forwarded to MARS.

For more information, see See references

Step 2 Define Key Reporting Devices

Using either a seed file or manual process, define the key reporting devices, such as IPS and vulnerability assessment devices. The goal here is to begin collecting events from key devices; those focused specifically on network and host-based vulnerabilities.

MARS begins to correlate security-related events from the primary reporting devices on your network.

For more information, see the following references:

1. [Adding Multiple Reporting and Mitigation Devices Using a Seed File, page 1-34](#)
2. [Add Reporting and Mitigation Devices Individually, page 1-33](#)
3. [Verifying Connectivity with the Reporting and Mitigation Devices, page 1-47](#)
4. [Activate the Reporting and Mitigation Devices, page 1-15](#)

Step 3 Discover Layer 3 Network

The discovery process identifies supported reporting and mitigation devices and adds those devices to the Monitoring and Security Devices list, identifying them by the Reporting IP. You can later edit these discovered devices to provide Access IP information and perform more thorough device-level discovery.

As much of your layer 3 network as possible is mapped out. Important route information and network configuration is available, which helps identify choke points for stopping ongoing attacks.

For more information, see the following references:

1. [Adding Reporting and Mitigation Devices Using Automatic Topology Discovery, page 1-32](#)
2. [Verifying Connectivity with the Reporting and Mitigation Devices, page 1-47](#)
3. [Activate the Reporting and Mitigation Devices, page 1-15](#)

Step 4 Import Undiscovered Security Devices and Hosts with Seed Files

With the CSV file, you can enter the values, passwords, and information for each device that you want the MARS Appliance to monitor in its appropriate row and column. While the seed file is useful for getting the MARS Appliance started processing event data for most devices, you may need to use the Admin > System Setup > Security and Monitoring Devices page to fine-tune the device manually. In addition, you must **activate** the devices that you add using a seed file (see [Activate the Reporting and Mitigation Devices, page 1-15](#)).

For more information, see the following references:

1. [Adding Multiple Reporting and Mitigation Devices Using a Seed File, page 1-34](#)
2. [Verifying Connectivity with the Reporting and Mitigation Devices, page 1-47](#)
3. [Activate the Reporting and Mitigation Devices, page 1-15](#)

Step 5 Manually Define Security Devices

As not all devices are supported via the seed file import, you must continue defining those security devices that are not discovered or imported via a seed file. In addition, you must manually define any layer 2 devices that you prepared as part of Item 1.

For more information, see the following references:

1. [Add Reporting and Mitigation Devices Individually, page 1-33](#)
2. [Verifying Connectivity with the Reporting and Mitigation Devices, page 1-47](#)
3. [Activate the Reporting and Mitigation Devices, page 1-15](#)

Step 6 Manually Define Key Assets as Hosts

Application hosts are simply hosts on your network that are running important applications. Also, many of the supported reporting devices and security devices cannot be represented in MARS until the base host on which they are running is defined. Such reporting applications include Checkpoint Firewalls and all web servers.

For more information, see the following references:

1. [Chapter 36, “Configuring Generic, Solaris, Linux, and Windows Application Hosts”](#)
2. [Activate the Reporting and Mitigation Devices, page 1-15](#)

Prioritizing the Devices to Add

To add a device, you provide MARS with the details required to discover a device’s settings and configuration, as well as configured that device to send audit event data to MARS.

Selecting which devices to add to MARS is closely tied to the function of the devices. Devices that detect attacks and false positives, such as intrusion detection or prevention, anti-virus, and vulnerability assessment devices are critical to providing MARS with active attack and efficacy data. You should add them first. Second, you should add those devices that can block an attack, such as Cisco routers and switches.

To further reduce false positives, you can also provide host-based data for the hosts on your network. You want to begin defining the host data for the critical assets on your network, such as servers that house databases of sensitive employee records or financial data.

You can also configure MARS to discover many of the layer 3 devices on your network, as described in [Discovering Your Network: Layer 3 Topology Discovery, page 1-15](#)

Bootstrap Summary Table

[Table 1-1](#) summarizes the settings that you must configure for the identified reporting and mitigation devices. It also provides links to any required agent downloads and to detailed configuration information.

Table 1-1 Reporting and Mitigation Device Bootstrap Summary

Device Type/Name	Bootstrap Summary	Reference Information
Router/Switch		
Cisco Router	<ol style="list-style-type: none"> 1. Access to IP address/interface by MARS. 2. FTP, SNMP, Telnet or SSH access by MARS. 3. Define SNMP RO community string. 4. Turn on syslog, define log level, and define MARS as target of syslog messages. 5. Enable NAC features. 	Chapter 17, "Cisco Routers"
Cisco Switch (IOS)		Chapter 15, "Cisco Switch Devices"
Cisco Switch (CatOS)		
Extreme ExtremeWare	<ol style="list-style-type: none"> 1. Access to IP address/interface by MARS. 2. (ExtremeWare only) Turn on syslog, define log level, and define MARS as target of syslog messages. 3. SNMP access by MARS. 4. Define SNMP RO community string. 	Chapter 16, "Extreme ExtremeWare 6.x"
Generic Router		Chapter 18, "Generic Router Device"

Table 1-1 Reporting and Mitigation Device Bootstrap Summary (Continued)

Firewall Devices		
Cisco PIX	<ol style="list-style-type: none"> 1. Access to access and reporting IP address/interface by MARS. 2. FTP, Telnet, or SSH access by MARS. 3. Define SNMP RO community string. <p>Note SNMP settings should be defined for the admin context on ASA and FWSM. You do not need to define these settings for each security context.</p> <ol style="list-style-type: none"> 4. Turn on syslog, define log level, and define MARS as target of syslog messages. 	Bootstrap the Cisco Firewall Device, page 19-2
Cisco Adaptive Security Appliance (ASA)		Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1
Cisco Firewall Services Module (FWSM)		Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1
Cisco IOS Firewall Feature Set		
Juniper Netscreen		Chapter 22, “NetScreen ScreenOS Devices”
Checkpoint Opsec NG and Firewall-1	<ol style="list-style-type: none"> 1. Add the MARS Appliance as a host. 2. Create and install an OPSEC Application object for the defined host. 3. Define policies to permit SIC traffic between the MARS Appliance, the Check Point management server, and any remote servers. 4. Define the log settings to push the correct events to the defined host. 5. Install the policies. 	Bootstrap the Check Point Devices, page 21-5
Nokia Firewall (running Checkpoint)		Bootstrap the Check Point Devices, page 21-5

Table 1-1 Reporting and Mitigation Device Bootstrap Summary (Continued)

VPN Devices		
Cisco VPN Concentrator		Chapter 24, “Cisco VPN 3000 Concentrator”
Network IDS/IPS		
Cisco Network IDS Cisco IDSM	<ol style="list-style-type: none"> 1. Enable RDEP for IDS modules. 2. Configure the following signature actions: <ul style="list-style-type: none"> – Alert – (Optional) To view trigger packets, enable the “produce-verbose-alert”. – (Optional) To view IP logs, enable the alert or “produce-verbose-alert” and “log-pair-packets”. 	Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1
Cisco Intrusion Prevention System (IPS), Network IPS	<ol style="list-style-type: none"> 1. Enable SDEE for IPS modules. 2. Configure the following signature actions: <ul style="list-style-type: none"> – Alert – (Optional) To view trigger packets, enable the “produce-verbose-alert”. – (Optional) To view IP logs, enable the alert or “produce-verbose-alert” and “log-pair-packets”. 	Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1

Table 1-1 Reporting and Mitigation Device Bootstrap Summary (Continued)

Cisco IPS ASA module	<ol style="list-style-type: none"> 1. Enable SDEE for IPS modules. 2. Configure the following signature actions: <ul style="list-style-type: none"> – Alert – (Optional) To view trigger packets, enable the “produce-verbose-alert”. – (Optional) To view IP logs, enable the alert or “produce-verbose-alert” and “log-pair-packets”. 	Chapter 9, “Cisco IPS Modules”
Cisco IOS IPS module	<ol style="list-style-type: none"> 1. Enable SDEE for IPS modules. 2. Configure the following signature actions: <ul style="list-style-type: none"> – Alert – (Optional) To view trigger packets, enable the “produce-verbose-alert”. – (Optional) To view IP logs, enable the alert or “produce-verbose-alert” and “log-pair-packets”. 	Chapter 9, “Cisco IPS Modules”
McAfee Intrushield		Chapter 7, “McAfee IntruShield”
Juniper Netscreen IDP		Chapter 3, “NetScreen IDP Device and Server Support”
Symantec Manhunt		Chapter 8, “Symantec ManHunt”
ISS RealSecure		Chapter 11, “ISS RealSecure 6.5 and 7.0”
Snort		Chapter 6, “Snort Devices”
Enterasys Dragon		Chapter 5, “Enterasys Dragon 6.x”
Host IDS		
Cisco Security Agent		Chapter 27, “Cisco Security Agent 4.x and 5.x Device”

Table 1-1 Reporting and Mitigation Device Bootstrap Summary (Continued)

McAfee Enterecept		Chapter 28, “Enterecept Enterecept 2.5 and 4.0”
ISS RealSecure Host Sensor		Chapter 11, “ISS RealSecure 6.5 and 7.0”
Anti-virus		
Symantec AntiVirus		Chapter 29, “Symantec AntiVirus Configuration”
Cisco Incident Control System (Cisco ICS), Trend Micro Outbreak Prevention Service (OPS)		Chapter 31, “Cisco Incident Control Server”
McAfee ePolicy Orchestrator		Chapter 30, “McAfee ePolicy Orchestrator Devices”
Network Associates VirusScan		Chapter 30, “McAfee ePolicy Orchestrator Devices”
Vulnerability Assessment		
eEye REM		Chapter 13, “eEye REM 1.0”
Qualys QualysGuard		Chapter 12, “Qualys QualysGuard Devices”
Foundstone Foundscan		Chapter 14, “McAfee Foundstone”
Host Operating Systems		
Windows	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Install and configure the SNARE agent • Create or edit an administrative account to ensure that it has permissions to pull the event data 	<p>Syslog (pushed by SNARE agent) or event data pull using MS-RPC</p> <p>Push Method: Configure Generic Microsoft Windows Hosts, page 36-5</p> <p>Pull Method: Configure the Microsoft Windows Host, page 36-7</p>
Solaris	—	<p>Syslog (from Device)</p> <p>Sun Solaris and Linux Hosts, page 36-2</p>
Redhat Linux	—	<p>Syslog (from Device)</p> <p>Sun Solaris and Linux Hosts, page 36-2</p>
Web Server		
Microsoft Internet Information Server	—	<p>Syslog (from SNARE agent)</p> <p>Install and Configure the Snare Agent for IIS, page 34-1</p>

Table 1-1 Reporting and Mitigation Device Bootstrap Summary (Continued)

Sun iPlanet	—	HTTP (from MARS Agent) Install and Configure the Web Agent on UNIX or Linux, page 34-7
Apache	—	HTTP (from MARS Agent) Install and Configure the Web Agent on UNIX or Linux, page 34-7
Web Proxy		
NetApp NetCache	—	HTTP Chapter 35, “Network Appliance NetCache Generic”
Database Server		
Oracle	TCP	SQLnet (from Host) Chapter 33, “Oracle Database Server Generic”
AAA Server		
Cisco Secure Access Control Sever (ACS)	—	Syslog (from MARS Agent) Install and Configure the PN Log Agent, page 26-8 (Cisco Secure ACS)
Cisco Secure ACS Appliance 4.x	Publish syslog messages to MARS Appliance.	Supporting Cisco Secure ACS Solution Engine 4.x, page 26-2
Cisco Secure ACS Appliance 3.x	Install and configure remote log agent.	Syslog (from MARS Agent) on secondary host Supporting Cisco Secure ACS Solution Engine 3.x, page 26-2 Install and Configure the PN Log Agent, page 26-8 (Cisco Secure ACS)
SNMP and Syslog Servers		
Generic Syslog Server	Publish syslog messages to MARS Appliance. Enable SNMP access by MARS Appliance.	Adding Generic Devices, page 36-1
Generic SNMP Server	Enable SNMP access by MARS Appliance.	Adding Generic Devices, page 36-1

Understanding Access IP, Reporting IP, and Interface Settings

When defining a reporting or mitigation device in the web interface, MARS allows (and at times, requires) you to specify several IP addresses. Understanding the purpose of the different addresses is important to effectively defining the devices that you want to monitor and manage. It is also important to understand their relationship to other settings that you can identify.

If a device has a single interface and a single IP address associated with that interface, the access and reporting IP addresses are the same as the address assigned to the interface. MARS collects this information separately to support those devices that have multiple interfaces, multiple IP addresses associated with a single interface, or both.



Note

Not all reporting devices support both an access and reporting IP address. Some devices use only access IP addresses to query the device for the required information (e.g., QualysGuard security service), while others have no settings that MARS can discover and only generate event messages for MARS to process (e.g., NetCache appliances). In addition, not all devices require the definition of interfaces.

This section discusses the following three addresses and their relationship to other settings:

This section contains the following topics:

- [Access IP, page 1-10](#)
- [Reporting IP, page 1-11](#)
- [Interface Settings, page 1-11](#)

Access IP

MARS uses the access IP address to either connect to the device for network-based administrative sessions or connect to a remote server on which a file containing the device's configuration is stored. The expected value is determined by the access type you select. Most devices also require that you explicitly identify the IP addresses of hosts allowed to administer them. The MARS Appliance must be listed among such hosts as part of the device preparation.

The protocol that MARS uses to connect to the device is defined by the access type value, which is a dependency for enabling administrative access. Once MARS has administrative access, it can perform device discovery, which includes settings such as ARP tables, NAT, routes, and active ACLs, all of which helps MARS understand the topology, perform attack path analysis, and identify false positive incidents. Discovery can be performed to varying degrees using any of the access types. For more information on access types, see [Selection of the Access Type, page 1-11](#).

MARS also uses SNMP RO and SNMPwalk to discover the device settings and topology information. However, the two methods of discovery are distinct and have distinct requirements. SNMPwalk requires the access IP address and the SNMP access type. SNMP RO discovery does not require the SNMP access type, but it does require the access IP address.



Note

MARS does not support the following characters in the SNMP RO community string: ' (single quote), " (double quote), < (less than symbol), and > (greater than symbol).

In addition, both SNMPwalk and SNMP RO are unrelated to SNMP notifications or SNMP traps. SNMPwalk and SNMP RO both require that MARS initiate the information request, whereas SNMP notifications are event notifications published by the reporting device, much the same as syslog messages are. As with syslog messages, SNMP notifications are published over the reporting IP address.

Reporting IP

The reporting IP is the source IP address of event messages, logs, notifications, or traps that originate from the device. MARS uses this address to associate received messages with the correct device. For single-homed devices, the reporting IP address is the same as the access IP; for dual- or multi-homed devices, this address must be explicitly associated with the syslog, NetFlow, and SNMP services running on the reporting device. Most devices also require, for each message type, that you explicitly identify the IP addresses of hosts to which messages should be published. These hosts are commonly referred to as target log servers. The MARS Appliance must be listed among such hosts as part of the device preparation.

The role in MARS of the reporting IP address differs from that of the access IP address in that the reporting IP address is treated passively from the MARS perspective. MARS does not query the device using this address. Such operations are performed using the access IP address and the access type.

MARS accepts only one reporting IP address per device. For devices supporting two message formats, such as NetFlow and syslog, you must ensure that both message formats are bound to the same source IP address (the reporting IP). In Cisco IOS devices, this common association is not the default so you must change either the syslog or the NetFlow reporting IP address to match the other. If the message types do not originate from a common IP address, one of them is seen as originating from an unreported device and MARS does not parse those events correctly.

The supported format of event data varies among reporting devices. Just because the device is able to generate syslog, NetFlow, and SNMP notifications does not mean that MARS processes all three formats. The document, [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#), identifies the event retrieval protocol supported by each device type.

Interface Settings

Interface settings are exclusive to hosts and software applications running on hosts. While MARS can discover the settings of a reporting device that is a software application running on a host, it cannot discover settings about the host itself. The role of interface settings in MARS is different from that of the access IP address and reporting IP address. Interface settings represent static information, not discovered or learned, about the host.

When correlating events specific to a host or reporting devices running on that host, MARS needs to understand the number of interfaces installed in the host, their names, and the IP addresses and networks associated with them. MARS uses the interface settings to guide discovery operations, to determine attack path vectors, and to perform Nessus vulnerability assessments.

Selection of the Access Type

The access type refers to the administrative protocol that MARS uses to access a reporting device or mitigation device. For most devices monitored by MARS, you can choose from among four administrative access protocols:

- **SNMP**—SNMP access provides administrative access to the device using a secured connection. It allows for the discovery of the settings using SNMPwalk, such as routes, connected networks, ARP tables, and address translations. If granted read-write access, SNMP also allows for mitigation on any L2 devices that support MIB2.



Note MARS uses SNMP v. 1 to perform device discovery. If MARS is unable to discover a device and you are confident that the configuration settings are correct, verify that the device is not expecting the authentication from MARS to occur over an encrypted channel.

- **Telnet**—Telnet provides full administrative access to the device using an unsecured connection. It allows for the discovery of the settings, such as routes, connected networks, ARP tables, and address translations. It also allows for mitigation on L2 devices.
- **SSH**—SSH provides full administrative access to the device using a secured connection. It allows for the discovery of the settings, such as routes, connected networks, ARP tables, and address translations. It also allows for mitigation on L2 devices. This access method is recommended for DTM support; however, Telnet access can achieve the same results.



Note Device discovery based on an SSH connection does not support 512-byte keys. The OpenSSH client (OpenSSH_3.1p1) used by MARS does not support a modulus size smaller than 768.

- **FTP**—FTP passive discovery of settings by providing MARS access to a file copy of the configuration running on the router. FTP does not support mitigation, DTM, or discovery of dynamic settings, such as NAT and ARP tables. In addition, if you select the FTP access type for device types, such as Cisco ASA and FWSM, you can only discover settings for the admin context. This access method is the least preferred and most limited access method. To enable configuration discovery using FTP access, you must place a copy the device's configuration file on an FTP server to which the MARS Appliance has access. This FTP server must have users authentication enabled.



Tip

TFTP is not supported. You must use an FTP server.

You can use any access scheme in conjunction with an SNMP RO community string. The division between Access IP and Reporting IP is clearly illustrated by an FTP access type example. Assume that you have SNMP RO access to a router, but your configuration discovery (access type) is restricted to a file stored on an FTP server.

When you define a device in MARS, the Access IP is the IP address of the FTP server (not the router), and the authentication information is used to access the FTP server. The Access Method is set to FTP. The Reporting IP is the IP address of the interface over which SNMP traps are published by the router.

This section describes how to configure each access type, identifying the fields that should be completed when a specific access type is selected. For efficiencies sake, these procedures are referenced throughout the specific device configuration topics, as they related to a specific device type.

This section contains the following topics:

- [Configure SNMP Access for Devices in MARS, page 1-13](#)
- [Configure Telnet Access for Devices in MARS, page 1-13](#)
- [Configure SSH Access for Devices in MARS, page 1-13](#)
- [Configure FTP Access for Devices in MARS, page 1-14](#)

Configure SNMP Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting SNMP in the Access Type list. To select SNMP as the access type, you must provide MARS with SNMP read-write access.

**Note**

The SNMP access type is not required to enable the SMPO RO strings. In fact, no access type is required to support SNMP RO. SNMP RO uses a shared, read-only community string; it does not require a read-write community string as does the SNMP access type.

If you selected SNMP as the access type, follow these steps:

Step 1

In the Login field, enter the username of the administrative account to use when accessing the reporting device.

**Note**

MARS uses SNMP v. 1 to perform device discovery. If MARS is unable to discover a device and you are confident that the configuration settings are correct, verify that the device is not expecting the authentication from MARS to occur over an encrypted channel.

Step 2

In the Password field, enter the password associated with the username specified in the Login field.

Step 3

If this device supports an enable mode, enter that password in the Enable Password field.

Configure Telnet Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting TELNET in the Access Type list.

If you selected TELNET as the access type, follow these steps:

Step 1

In the Login field, enter the username of the administrative account to use when accessing the reporting device.

Step 2

In the Password field, enter the password associated with the username specified in the Login field.

Step 3

If this device supports an enable mode, enter that password in the Enable Password field.

Configure SSH Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting SSH in the Access Type list.

**Note**

Device discovery based on an SSH connection does not support 512-byte keys. The OpenSSH client (OpenSSH_3.1p1) used by MARS does not support a modulus size smaller than 768.

If you selected SSH as the access type, follow these steps:

-
- Step 1** From the list box to the right of the Access Type list, select **3DES**, **DES**, or **BlowFish** as the encryption cipher for SSH sessions between the MARS Appliance and the reporting device.
 - Step 2** In the Login field, enter the username of the administrative account to use when accessing the reporting device.
 - Step 3** In the Password field, enter the password associated with the username specified in the Login field.
 - Step 4** If this device supports an enable mode, enter that password in the Enable Password field.
-

Configure FTP Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting FTP in the Access Type list.



Note

When configuring FTP Access Type, the Access IP is the IP address of the FTP server from which MARS retrieves the reporting Device Type's configuration file. The Reporting IP is the IP address of the reporting Device Type from which MARS receives event data.

If you selected FTP as the access type, follow these steps:

-
- Step 1** In the Login field, enter the username of the FTP server account to use when accessing the configuration file of the reporting device.



Note

Login and Password must match the username and password with access to the FTP server on which the configuration file reside for the device identified in the Access IP field.

- Step 2** In the Password field, enter the password associated with the username specified in the Login field.
- Step 3** In the Config Path field, enter the path to the reporting device's configuration file residing on the FTP server.

This path begins at the root of the FTP server's published folder, not at the root directory of server.

- Step 4** In the File Name field, enter the name of the reporting device's configuration file residing on the FTP server.



Note

If you select FTP, you cannot enter an enable password.

Activate the Reporting and Mitigation Devices

After you have added reporting devices and mitigation devices to MARS, you must activate those devices before MARS begins to fully process the data provided by those devices. This processing is different from those devices discovered on the network, where the logs sent to the appliance are stored, but your ability to interact with that data is limited to queries and reports. Typically, MARS runs inspection rules and generates notifications only against the data retrieved from activated devices.

Once a device is known to the MARS Appliance, all data provided by that particular device can be normalized and sessionized, which enables that device's data to be used to fire an incident.

**Note**

Default installations of MARS do not fire incidents based on data received from unknown devices. However, you can still enable this by creating one or more rules that use keyword search. A device must be defined for the MARS to be able to parse and sessionize the event data. The act of parsing the event data correctly is what ensures rules fire more accurately.

**Tip**

You must click **Activate** whenever you add or modify rules, drop rules, reports, or add or modify any options or settings under in the Admin tab other than those on the User Management subtab. Otherwise, the changes that you make will not take effect.

To activate added devices, follow these steps:

- Step 1** For each device that you want to add, provide the device details and click **Submit** to add the device. The Submit action stores the device details in the database. Once you click Submit, your work is saved, even if you drop the administrative connection before clicking **Activate**.
- Step 2** Once you have all of the devices desired for this administrative session, click **Activate**. The Activate action differs from Submit in that MARS begins to inspect and generate notifications about the data provided by the devices.

**Tip**

If you are adding or editing several devices, it is better for the system to click **Activate** for several changes rather than for each individual change.

Discovering Your Network: Layer 3 Topology Discovery

For MARS to reach full operability, you must specify the SNMP community strings and select the networks to discover. Once the appliance discovers these networks, you get a more accurate view of MAC addresses, end-point lookup (attack paths), and network topology. Topology discovery enables operation level three, see “Levels of Operation” for more information.

There are many advantages to discovering your network; for example, the discovery process identifies Cisco routers and gateways, it provides a more complete topology graph on the Dashboard page, and you can refine the discovery parameters to ensure that you do not discover your ISPs network.

Select the **Summary > Dashboard** page in the MARS web interface for a view of the topologies.

**Note**

Remember to activate additions and changes to your community strings and valid networks by clicking **Activate**.

How Layer 3 Topology Discovery Works

Network discovery is an iterative, SNMP-based layer 3 discovery. Starting with the layer 3 seed device (known as the SNMP target), MARS discovers its layer 3 neighbors and then iterates through each neighbor as a layer 3 seed device to discover other devices. SNMP read only access to the layer 3 devices is required via an SNMP RO community string.

This process discovers your entire layer 3 network with two exceptions:

1. A device, such as a firewall, that blocks SNMP access to itself or a network segment.
2. You've listed the networks to discover and a network segment is identified but not in the network discovery list.

To work around the first exception, where a device blocks SNMP access, do the following:

1. Configure MARS to discover the SNMP-blocked devices separately using administrative protocols such as Telnet, SSH, or Checkpoint CPMI.
2. If the routes cannot be discovered for a SNMP-blocked device via the administrative protocol (such as a software-based Checkpoint Firewall-1), either manually define the routes known to that device in MARS or provide a different SNMP target on the far side of the firewall so MARS can continue network discovery.

The MARS network discovery engine combines the complete topology from the partially discovered topologies of different SNMP targets and devices discovered via Telnet, SSH, Checkpoint CPMI, and so forth. The Layer 3 network discovery is automatic because of next hop address information in routes that can be used to iteratively discover additional devices. However this is not the case for Layer 2 networks, so you must manually configure the Layer 2 devices, their management interfaces, and access credentials (such as SNMP community strings) on MARS. This information can also be imported from a seed CSV file written in a CiscoWorks format.

Add a Community String for a Network

To add a community string for a network address, follow these steps:

-
- Step 1** To open the Community Strings and Networks page, click **Admin > Community Strings and Networks**, located in the Topology Discovery Information box.

Community Strings and Networks

- Step 2** Click the **Network IP** radio button.
- Step 3** Enter the Community String, Network IP address, and Mask.
- Step 4** Click **Add**.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for all the community strings that you want to add.
- Step 6** Click **Submit** to commit these additions.

Add a Community String for an IP Range

To add a community string for an IP range, follow these steps:

- Step 1** To open the Community Strings and Networks page, click **Admin > Community Strings and Networks**.
- Step 2** Click the **IP Range** radio button.
- Step 3** Enter the Community String and its IP Range.
- Step 4** Click **Add**.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for all the community strings that you want to add.
- Step 6** Click **Submit** to commit these additions.

You can add multiple community strings for the same network by adding similar entries.

Add Valid Networks to Discovery List

Adding valid networks confines the MARS to discover only the networks that you want. MARS uses this information to create topologies, find MAC addresses, and for end-point lookup (attack paths).



Note

You can only specify networks for the zone where the MARS Appliance operates.

To add valid networks, follow these steps:

-
- Step 1** Click **Admin > Valid Networks** to open the Valid Networks page.
 - Step 2** Enter the **SNMP Target**'s IP address.
The SNMP target is the entry-point where the MARS starts discovering devices on a network. It typically identifies an address on a default gateway of the network.
 - Step 3** Click either **Network IP** or **Network Range** to define the scope of the scan.
 - Step 4** Enter the appropriate information.
 - Step 5** Click **Submit**.
-

Remove Networks from Discovery List

To remove a network, follow these steps:

-
- Step 1** Click **Admin > Valid Networks** to open the Valid Networks page.
 - Step 2** Click the network that you want to remove.
 - Step 3** Click **Remove**.
-

Discover Layer 3 Data On Demand

You can schedule topology discovery, as defined in [Scheduling Topology Updates, page 1-18](#). However, you can also initiate an on-demand discovery.

To perform an on-demand discovery, follow these steps:

-
- Step 1** Click **Admin > Valid Networks** to open the Valid Networks page.
 - Step 2** Verify that the list of Valid Network Addresses contains the networks that you want to discover.
 - Step 3** Click **Discover Now**.
-

Scheduling Topology Updates

You can configure MARS to run automatic topology updates on devices, networks, and groups of networks. Scheduling topology updates is a critical part of keeping the MARS Appliance abreast of changes in the network and of changes to the configuration settings of the reporting devices and mitigation devices. This operation is similar to clicking Discover when defining a reporting device.

Configuration discovery depends on the device type, proper authorization, an access type, such as Telnet or SSH, and an access IP address. When device discovery is performed, MARS contacts the device and conducts a topology and configuration discovery. This discovery collects all of the route, NAT, and ACL-related information for the device or admin context. In addition, the name of the device may change

to hostname.domain format if it was not already entered as such. If discovering a device that supports them, MARS also discovers information about modules, admin contexts, and security contexts. Another effect of scheduled updates is that MARS keeps the network diagram and attack paths current in the Dashboard.

This feature also allows you to pull data from those devices that require interval-based polling. The list to devices that require such polling are:

- Qualys QualysGuard
- eEye REM
- FoundStone FoundScan
- Check Point log servers

Figure 1-1 Example Scheduled Update for eEye REM

Name:

10.1.1.0/255.255.255.255	<input type="button" value="Add"/>	<input type="radio"/> Select: <input type="text" value="1.1.0.0/255.255.0.0(n-1.1.0.0/16)"/>
	<input type="button" value="Remove"/>	<input type="radio"/> Network IP: <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> Mask: <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/>
		<input type="radio"/> IP Range: <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/>

Schedule	Time of Day	Days
<input checked="" type="radio"/> Run On Demand Only		
<input type="radio"/> Daily	<input type="text" value="12:00 Midnight"/>	
<input type="radio"/> Weekly	<input type="text" value="12:00 Midnight"/>	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
<input type="radio"/> Monthly	<input type="text" value="12:00 Midnight"/>	<input type="checkbox"/> 1st <input type="checkbox"/> 2nd <input type="checkbox"/> 3rd <input type="checkbox"/> 4th <input type="checkbox"/> 5th <input type="checkbox"/> 6th <input type="checkbox"/> 7th <input type="checkbox"/> 8th <input type="checkbox"/> 9th <input type="checkbox"/> 10th <input type="checkbox"/> 11th <input type="checkbox"/> 12th <input type="checkbox"/> 13th <input type="checkbox"/> 14th <input type="checkbox"/> 15th <input type="checkbox"/> 16th <input type="checkbox"/> 17th <input type="checkbox"/> 18th <input type="checkbox"/> 19th <input type="checkbox"/> 20th <input type="checkbox"/> 21st

143360

Schedule a Network Discovery

To add a network for scheduled discovery, follow these steps:

- Step 1** Click **Admin > Topology/Monitored Device Update Scheduler**.
The Topology/Monitored Device Update Scheduler page displays.
- Step 2** Click **Add**.
- Step 3** Enter a name for the network (or group of networks).
- Step 4** Select or enter your networks:
 - Click the **Select** radio button, and select a network from the list.
 - Click the **Network IP** radio button, and enter the IP address and Mask.
 - Click the **IP Range** radio button, and enter the IP ranges.
- Step 5** Click **Add** to move the network into the selected field.

- To remove an item in the selected field, click it to highlight it, and click **Remove**.

Step 6 In the schedule table, select the appropriate radio button and its time criteria:

- **Run On Demand Only**
- **Daily** and the Time of Day
- **Weekly**, the Time of Day, and the Days
- **Monthly**, the Time of the Day, and the Dates

Step 7 Click **Submit**.

Edit a Scheduled Topology Discovery

Step 1 Check the box next to the Topology Group.

Step 2 Click **Edit**.

Step 3 Click **Add** to move the network into the selected field.

- To remove an item in the selected field, click it to highlight it, and click **Remove**.

Step 4 In the schedule table, select the appropriate radio button and its time criteria:

- **Run On Demand Only**
- **Daily** and the Time of Day
- **Weekly**, the Time of Day, and the Days
- **Monthly**, the Time of the Day, and the Dates

Step 5 Click **Submit**.

Delete a Scheduled Topology Discovery

Step 1 Click **Admin > Topology/Monitored Device Update Scheduler**.

The Topology/Monitored Device Update Scheduler page displays.

Step 2 Check the box next to the Topology Group.

Step 3 Click **Delete**.

Run a Topology Discovery on Demand

Step 1 Check the box next to the Topology Group.

Step 2 Click **Run Now**.

Troubleshoot Layer 3 Network Discovery

Table 1-2 Troubleshooting Discovery Issues

Issues	Resolution/Workaround
MARS did not discover all of the layer 3 devices in my network. Why?	The configuration settings for discovery may be incomplete. Make sure you entered all required SNMP Community Strings, and make sure all target networks are listed as Valid Networks.
I want to change the interval time for polling the network (discovery) for the topology.	Set the value on the Admin > System Setup > Topology/Monitored Device Update Scheduler page.
I need to set a customized banner for SSH logins.	MARS does not expect a banner when logging in to a device. When certain keywords, such as <i>login</i> , <i>Password</i> , or <i>#</i> , are present in a banner, they can cause discovery issues. You can customize the login prompt expected by MARS, but it applies globally to all devices. You cannot define a custom login prompt for a single or specific set of devices. To customize the login and pwd prompt for all devices, set the values on the Admin > System Parameters > TACACS/AAA Server Prompts page.

Configuring Resource Usage Data

While the Monitor Resource Usage box appears on every host and reporting device, only three device types actually provide resource usage data to MARS:

- Cisco IOS routers running 12.2
- Cisco IOS switches running 12.2
- Cisco PIX 6.0, 6.1, 6.2, 6.3, 7.0
- Cisco ASA 7.x
- Cisco FWSM 2.x and 3.x
- Check Point devices (Opsec NG FP3)

For these six devices, MARS can provide data about CPU utilization, memory utilization, and device saturation. For FWSM, MARS monitors system context level resources (CPU, memory, connections) via the CLI and per-context resources (CPU, memory, connections, interface utilization, and errors) via SNMP. Therefore, you can monitor three views of the FWSM module: base platform (IOS switch hosting the module), module level (system context), and security context level.

To enable the collection of resource usage data, you must ensure that the resource usage-specific events are logged by the reporting devices, that the SNMP RO community string is set, that those devices forward the events to MARS, and that the device is defined in the web interface as a reporting device or mitigation device. In addition, you must select **Yes** in the Monitor Resource Usage box of the General tab for each supported reporting device.

Once configured, MARS uses SNMP to poll the device every 5 minutes for the following SNMP OIDs:

- Bytes in/out of every interface on the device (Cisco IOS, Cisco PIX)
- Number of current connections (Cisco PIX, Check Point)
- CPU of last second and last 60 seconds (Cisco IOS, Cisco PIX)
- Memory free/used (Cisco IOS, Cisco PIX)

It also detects anomalous resource utilization if the consumption is significantly higher than the hourly average.

The following resource usage data reports are available:

- Resource Utilization: Bandwidth: Inbound - Top Interfaces
- Resource Utilization: Bandwidth: Outbound - Top Interfaces
- Resource Utilization: CPU - Top Devices
- Resource Utilization: Concurrent Connections - Top Devices
- Resource Utilization: Errors: Inbound - Top Interfaces
- Resource Utilization: Errors: Outbound - Top Interfaces
- Resource Utilization: Memory - Top Devices

You can define custom rules, reports, and queries about resource usage based on the following events:

- CPU Utilization Higher Than 50%
- CPU Utilization Higher Than 75%
- CPU Utilization Higher Than 90%
- CPU Utilization Abnormally High
- Memory Utilization Higher Than 50%
- Memory Utilization Higher Than 75%
- Memory Utilization Higher Than 90%
- Memory Utilization Abnormally High

There is also a pre-defined resource utilization inspection rule:

- System Rule: DoS: Network Device - Success Likely
- System Rule: DoS: Network - Success Likely
- System Rule: Resource Issue: Network Device

Enabling the Required SNMP OIDs for Resource Monitoring

[Table 1-3 on page 1-23](#) lists the OIDs to enable, on a per device basis, for the supported model and versions.

Table 1-3 *SNMP OIDs Required for Resource Monitoring*

Vendor, Model, and Version	OID Descriptor	OID
Cisco IOS 12.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.2.1.56.0
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco Switch-IOS 12.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.2.1.56.0
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	
Cisco PIX 6.0	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco PIX 6.1	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	
Cisco PIX 6.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i	
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco PIX 6.3	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco PIX 7.0	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco FWSM 2.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco FWSM 2.3	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco FWSM 3.1	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	

Table 1-3 *SNMP OIDs Required for Resource Monitoring (Continued)*

Cisco ASA 7.0	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i	
DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i	
CheckPoint OpSec NG FP3	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.2620.1.1.25.3.0
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0

Adding Reporting and Mitigation Devices

Three methods exist for adding reporting devices and mitigation devices to MARS:

- Discover devices automatically using SNMP RO community strings.
- Add multiple devices using a seed file.
- Manually add the devices one at a time.

From the Security and Monitor Devices page, you can add or edit the reporting devices and mitigation devices that MARS monitors. To access this page, click **Admin > System Setup > Security and Monitor Devices**. You can search for, add, edit, delete, change display status, and load or update devices from the seed file.

The device support is categorized into three categories:

- **HW-Based Security Devices**—Hardware-based devices represent routers, switches, and other dedicated security appliances. You can add such reporting devices by selecting the appropriate device.

- **SW-Based Security Devices**—Software-based devices represent applications that reside on a host, rather than a dedicated appliance. You can add reporting device on a new host by selecting **Add SW security apps on new host** or on an existing host by selecting **Add SW security apps on existing host**.

You can only define one SW security application for each reporting device. For example, if you have multiple Oracle databases running on a server, you cannot add separate instances to the same host. To work around this issue, use multiple servers or have the different applications report to MARS using unique reporting IP addresses. When using unique IP addresses, each one represents a unique host in MARS on which you can define a single SW security application.

- **On-Demand Security Services**—Security services represent subscription-based services provided by vendors using a central security operations center (SOC) with remote monitoring nodes. These services, such as Qualys QualysGuard, represent systems from which MARS periodically pulls data. You can add such reporting devices by selecting the appropriate service. These devices also require you to define a schedule for pulling data (see [Scheduling Topology Updates](#), page 1-18).

The complete list of supported devices is presented in the [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#) document. Devices are added to this list on an ongoing basis via software upgrade packages. See the document [Cisco Security MARS Initial Configuration and Upgrade Guide 6X](#) for details on how to upgrade your MARS Appliance.

MARS can also support any syslog or SNMP devices, even if they do not appear on the list of devices supported by the MARS. You can enter any syslog or SNMP device into the network topology, configure it to report data to the MARS, and query it using a free-form keyword query. (See [To Run a Keyword Query](#).)

For more information on adding devices, see:

- [Adding Reporting and Mitigation Devices Using Automatic Topology Discovery](#), page 1-32
- [Adding Multiple Reporting and Mitigation Devices Using a Seed File](#), page 1-34
- [Add Reporting and Mitigation Devices Individually](#), page 1-33

Regardless of the method that you have used to add the devices, you should also perform the following tasks:

- [Verifying Connectivity with the Reporting and Mitigation Devices](#), page 1-47
- [Activate the Reporting and Mitigation Devices](#), page 1-15

Adding Reporting and Mitigation Devices Using Automatic Topology Discovery

On the Admin page, under the Topology Discovery Information section, three links exist, allowing you to define the settings required to discover reporting and mitigation devices automatically. These links are:

- **Community String and Networks**—Allows you to define SNMP RO community strings on a per network or IP range basis. Networks and SNMP RO strings can overlap. At least one SNMP string must be defined before discovery is attempted.
- **Valid Networks**—Identifies the set of networks and IP ranges that you want to discover. You should also define one or more SNMP targets. If no SNMP targets are defined, MARS uses its own gateway as the SNMP target. SNMP targets should be layer 3 gateway devices, such as a router or firewall with SNMP RO community strings defined and discovery permitted; they should also be defined on a per network or per range basis if you wish to separate the discovery using schedule rules. At least one valid network must be defined before discovery is attempted.

- **Topology/Monitored Device Update Scheduler**—While not required for discovery, it does allow you to increase the frequency of topology discovery and further refine the potential depth of a discovery based on a particular schedule rule. The default schedule rule is once a month for all valid networks. However, if no valid networks are defined, the process wakes up, sees no valid networks are defined, and quits. Each schedule rule allows you to select which networks, as defined within the list of valid networks and ranges, that should be discovered according to frequency also specified in the rule. As connected networks often exist, you can refine which networks are discovered by ensuring that separate schedule rule exists for each network that you do not want to be automatically discovered as part of a connected network.

Based on the networks defined within the schedule rules, MARS starts with the first SNMP target associated with those networks or ranges as defined under Valid Networks and attempts to discover that device using SNMP discovery. The discovery process continues as long as the target device provides additional routes and the addresses of such routes are part of the networks in another schedule rule. The process also iterates through each SNMP target that is defined. The entire discovery process is limited based on the schedule rule's bounding networks, the SNMP targets, the valid network and IP ranges, and the SNMP RO community strings, which are defined on a per network basis. Networks and SNMP RO community strings can overlap, in which case MARS tries each string against the gateway addresses discovered within that network. The discovery process only discovers Layer 3 gateway devices, such as routers and firewalls. It does not discover hosts, unless those hosts are defined as the explicit target within a schedule rule (see [Scheduling Topology Updates, page 1-18](#)).

As the discovery process identifies supported reporting and mitigation devices, it adds those devices to the Monitoring and Security Devices list (Admin > Monitoring and Reporting Devices), identifying them by the Reporting IP. You can later edit these discovered devices to provide Access IP information and perform more thorough device-level discovery. Once a device is listed under Monitoring and Reporting Devices, it may be rediscovered, but it will not be added again unless it has been properly deleted (see [Delete a Device](#)).

For more information on these settings, see:

- [Configuring Layer 3 Topology Discovery](#)
- [Scheduling Topology Updates, page 1-18](#)

**Note**

Once the discovery process is complete, you must click **Activate** for MARS to correctly process events received from that device. For more information, see [Activate the Reporting and Mitigation Devices, page 1-15](#).

Add Reporting and Mitigation Devices Individually

In general, you have two choices for adding devices that you want to monitor into your MARS. You can create a seed file or you can add each device manually. Seed file support is limited to a few device types, see Column E of [Table 1-4Seed File Column Description columnsseed filePN MARSseed file columns](#) for the devices supported.

When manually configuring devices, select the devices that are most interesting to you. Once added, you can come back and edit them as necessary. Manual configuration is also useful when you add or change a single security device on your network.

**Note**

Remember that you do not have to add all of the devices configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the MARS starts to report to you, and provide more details.

To add a device manually, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Add**.
 - Step 2** Select the device from the list.
 - Step 3** Enter the information needed to communicate with the device.
 - Step 4** Click **Submit**.
 - Step 5** Once add a device, you must click **Activate** for MARS to correctly process events received from that device. For more information, see [Activate the Reporting and Mitigation Devices, page 1-15](#).
-

Adding Multiple Reporting and Mitigation Devices Using a Seed File

The seed file is a comma-delimited file with the file extension .csv (comma-separated value). Most spreadsheet programs let you import and export files as CSV files.

The following is a sample seed file as exported from a popular spreadsheet program:

```
10.1.1.1,,,PIX,TELNET,,,cisco,,,,,,,,,
192.168.229.241,,,IOS,TELNET,,,csRv$12*,EcsRv$12$,,,,,,,,,
10.1.1.83,,,PIX,SSH,pix,Vpnsn12,,vPfwlne,,,,,,,,,
192.168.151.169,,,PIX,SSH,pix,lpt$12,,pot$1*d1,,,,,,,,,
10.4.2.4,,,NETSCREEN,SSH,netscreen,nt*$scn25,,,,,,,,,
10.4.2.3,,,NETSCREEN,SSH,netscreen,nt*$scn10,,,,,,,,,
10.1.1.241,,,IOS,TELNET,,,cisco,cisco,,,,,,,,,
10.4.2.1,,,IOS,TELNET,,,Qa$1*5ft,gt*$j15,,,,,,,,,
10.4.2.2,,,IOS,TELNET,,,Qa$1*5ft,gt*$j15,,,,,,,,,
wanRouter,public,,,IOS,SNMP,,,,,,,,,
myPix63,,,PIX,SSH,pix,test1,,test1234,,,,,,,,,10.2.3.1
MyPc,,,WINDOWS,RPC,myname,mypass,,,,,,,,,
myPix70,,,PIX7X,SSH,,,,,,,,,
myids40,,,CiscoIDS4x,SSL,,,,,,,,,
myids50,,,CiscoIPS5x,SSL,,,,,,,,,
myASA70,,,ASA,SSH,,,,,,,,,
myWindowsNT,,,WindowsNT,RPC,,,,,,,,,
myFWSM23,,,FWSM,SSH,,,,,,,,,
```

With the CSV file, you can enter the values, passwords, and information for each device that you want the MARS Appliance to monitor in its appropriate row and column. While the seed file is useful for getting the MARS Appliance started processing event data for most devices, you may need to use the Admin > System Setup > Security and Monitoring Devices page to fine-tune the device manually. In addition, you must **Activate** the devices that you add using a seed file (see [Activate the Reporting and Mitigation Devices, page 1-15](#)).

Limitations and Restrictions

The following limitations and restrictions apply to importing devices using a seed file:

- **Appliance Devices**—These devices appear directly in the Monitoring and Reporting Devices list. Supported for the devices identified in [Column E of Table 1-4Seed File Column Description columnsseed filePN MARSseed file columns](#).
- **Applications on Hosts**—Software applications running on hosts are not supported via seed file import. You can import the Linux, Solaris, or Windows-based host, which will appear in the device list. However, you cannot specify a software application running on that host within the seed file. You must add that application manually after you import or otherwise define the host.

- **Hosts**—Hosts imported using a seed file appear differently in the web interface. Instead of appearing in the IP device list, they appear as monitored hosts in the Monitoring and Reporting Devices list. However, any applications running on these hosts are not discovered. You must manually define them.
- **Modules**—Modules, including IPS and FWSM, for ASA and IOS switches and routers are treated similar to applications on host-based devices. The deference is that modules have device names that are unique from their parent devices. If you attempt to import them using a seed file, modules are imported as an independent device and not as a module, appearing directly in the Monitoring and Reporting Devices.

Devices that Require Custom Seed Files

Some reporting devices represent the management consoles for the actual host- or node-based reporting devices. These consoles often represent centralized log servers for the devices they manage. However, for MARS to correctly correlate the logs for these centralized log servers, you must identify those host- or node-based reporting device. In some cases, MARS is able to dynamically learn of the hosts or nodes by parsing the logs. In other cases, you must use a seed file generated by management console to identify each of the managed reporting devices.

Once you generate the seed file, you must import that seed file under the host that represents the management console in the MARS web interface to load the sensor module information from the CSV or seed file. The device types that use a custom seed file are as follows:

- **Entercept**—For more information, see [Extracting Entercept Agent Information into a CSV file \(for Entercept Version 2.5\)](#), page 28-1.
- **IntruVert IntruShield**—For more information, see [Extracting IntruShield Network Sensor Information from the IntruShield Security Manager](#), page 7-4.
- **Cisco Security Agent**—While MARS can learn of the CSA agents dynamically, you can also import the initial list of agents using a custom seed file. For more information, see [Export CSA Agent Information to File](#), page 27-2.
- **Symantec AntiVirus**—While MARS can learn of the Symantec AntiVirus agents dynamically, you can also import the initial list of agents using a custom seed file. For more information, see [Export the AntiVirus Agent List](#), page 29-7.

Devices that Require Updates After the Seed File Import

When you add specific reporting devices using a seed file, you must edit them to complete the definition of the device before you can monitor them. Typically, these devices are IDS/IPS devices that monitor specific networks. The device types that you must update are as follows:

- **Cisco IDS 4.x Devices.** These sensors are defined by importing a MARS-specific seed file as defined in [Load Devices From the Seed File](#), page 1-45. However, once you import a sensor, you must identify the monitored networks that it monitors. For more information, see [Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File](#), page 2-4.
- **Cisco IPS 5.x Devices.** These sensors are defined by importing a MARS-specific seed file as defined in [Load Devices From the Seed File](#), page 1-45. However, once you import a sensor, you must identify the monitored networks that it monitors. For more information, see [Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File](#), page 2-4.

- **Cisco IPS 6.x Devices.** These sensors are defined by importing a MARS-specific seed file as defined in [Load Devices From the Seed File, page 1-45](#). However, once you import a sensor, you must identify the monitored networks that it monitors. For more information, see [Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File, page 2-4](#).
- **IntruShield Senors.** These sensors are defined by importing a custom seedfile; however, once you import the sensors, which appear as children of the IntruShield Manager host, you must identify the monitored networks for each sensor. For more information, see [Add IntruShield Sensors Using a Seed File, page 7-5](#).

Seed File Header Columns

[Table 1-4 on page 1-38](#) describes the columns in the seed files and identifies valid values. If you do not enter a value for a given column, you must enter a comma to delineate that column.



Note

Remember that you do not have to add all of the device's configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the MARS starts to report to you, and provide more details.

Table 1-4 *Seed File Column Description columnsseed filePN MARSseed file columns*

Column	Type	Entry
--------	------	-------

Table 1-4 *Seed File Column Description columnsseed filePN MARSseed file columns*

Column A	NAME OR IP	<p>The device's name or IP address. (Mandatory) If the device name is provided and Column U is empty, MARS performs a DNS lookup to identify the address which will be used to populate the Access and Reporting IP fields</p> <p>Note If an IP address appears in Column U, that address overrides any address or derived address specified in Column A. However, the name value specified in Column A is used. If after the DNS lookup the device with the IP specified is found then the HostName is overwritten with that of the device.</p>
-----------------	------------	---

Table 1-4 Seed File Column Description columnsseed filePN MARSseed file columns

Column B	SNMP RO/RW Community	<p>The device's SNMP RO community name here.</p> <p>Note MARS does not support the following characters in the SNMP RO community string: ' (single quote), " (double quote), < (less than symbol), and > (greater than symbol).</p>
-----------------	----------------------	--

Table 1-4 *Seed File Column Description columnsseed filePN MARSseed file columns*

Column C	EMPTY	Empty placeholder column.
-----------------	-------	---------------------------

Table 1-4 *Seed File Column Description columnsseed filePN MARSseed file columns*

Column D	EMPTY	Empty placeholder column.
-----------------	-------	---------------------------

Table 1-4 Seed File Column Description columnsseed filePN MARSseed file columns

Column E	DEVICE TYPE	The device type designator. (case insensitive)
		<p>Note Some of the devices supported in the GUI cannot be entered via a CSV file.</p> <p>Use the following strings represent the desired device type:</p> <ul style="list-style-type: none"> • ASA: for Cisco ASA devices • CiscoIDS4x: for appliance running Cisco IPS 4.x (not modules) • CiscoIPS5x: for appliance running Cisco IPS 5.x (not modules) • CiscoIPS6x: for appliance running Cisco IPS 6.x (not modules) • SecureACS4: for Cisco Secure Access Control Sever (ACS) 4.x • SecureACSSE: for Cisco Secure ACS Solutions Engine 4.x • FWSM: for Cisco FWSM 1.x, 2.x, 3.x • PIX: for Cisco PIX 6.0, 6.1, 6.2, and 6.3 devices • PIX7X: for Cisco PIX 7.x and 8.0x devices • IOS: for Cisco IOS 12.2 (default) • SWITCH-CATOS: for Cisco Switch in Hybrid Mode • SWITCH-IOS: for Cisco Switch in Native Mode • EXTREME: for Extreme ExtremeWare 6.x • NACApp: for Cisco NAC Appliance 4.1.3 • NETSCREEN, NETSCREEN50, NETSCREEN54, or NETSCREEN60: for ScreenOS 4.0, 5.0, 5.4, and 6.0 respectively • WLANController: 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000

Table 1-4 Seed File Column Description columnsseed filePN MARSseed file columns

Column F	ACCESS TYPE	<p>The Access Type for this device. Your choices are:</p> <ul style="list-style-type: none"> • TELNET • FTP • SSH • SSL • SNMP (default) • RPC (Windows only) <p>In the RPC case, the username field (Column G) should be non-empty. The password can be provided in Column H. If RPC access type and username are given, the PULL flag is set by the backend in addition to the default RECEIVE flag.</p>
-----------------	-------------	--

Table 1-4 Seed File Column Description columnsseed filePN MARSseed file columns

Column G	USER NAME	The TELNET, SSH, SSL, FTP, or RPC user name. This column is only valid if you have used TELNET, SSH, SSL, or FTP in Column F .
Column H	SSH/FTP/RPC PASSWORD	The SSH, SSL, or FTP Password for the device. This column is only valid if you have used SSH, SSL, or FTP in Column F .
Column I	TELNET PASSWORD	The Telnet password for the device.
Column J	ENABLE PASSWORD	The enable password (applicable only with FWSM, PIX, or IOS devices).
Columns K	EMPTY	Empty placeholder column.
Column L	EMPTY	Empty placeholder column.
Column M	EMPTY	Empty placeholder column.
Column N	EMPTY	Empty placeholder column.
Column O	EMPTY	Empty placeholder column.
Column P	EMPTY	Empty placeholder column.
Column Q	EMPTY	Empty placeholder column.
Column R	EMPTY	Empty placeholder column.
Column S	EMPTY	Empty placeholder column.
Column T	FTP LOCATION [if Access Type =FTP]	The location for the FTP file. This location starts from the FTP root, not the sysroot. If, for example, the file is at <ftproot>/configdata/router1.txt , using ./configdata/router1.txt is correct.
Column U	Access/Reporting IP [optional]	The Access IP and Reporting IP address to use when populating this device. The MARS Appliance uses this address to communicate with the device. See Understanding Access IP, Reporting IP, and Interface Settings, page 1-10

Load Devices From the Seed File

Once you have completed the seed file, you must place the CSV file on to the FTP server from which the MARS Appliance will load it.

To load the file into the MARS, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Load From Seed File**.
- Step 2** Enter the FTP Server's IP address, the user name and password for the FTP server, the path, and the file name for the seed file.
- The FTP path starts from the FTP root, not from the sysroot for the configuration path.
- Step 3** Click **Submit**.
- Once you have loaded devices from the seed file, return to each device. Continue to configure the devices and to add information such as reporting IP addresses, and SNMP information.
- Step 4** Once add a device, you must click **Activate** for MARS to correctly process events received from that device. For more information, see [Activate the Reporting and Mitigation Devices, page 1-15](#).



Note Using a seed file to define the reporting devices replaces the manual definition of the device; however, the topology information will not be available. After adding the reporting devices via a seed file, you must either manually discover each device by selecting the device, clicking Edit, and then clicking the Discover button or by scheduling a topology discovery. In addition, some device types required that you define additional settings (see [Devices that Require Updates After the Seed File Import, page 1-35](#)).

Bulk Update of Device Credentials using Seed Files

Using a seed file, you can also update the credentials of some monitoring and reporting devices previously defined in MARS. If we re-import the devices based on the credentials ID, MARS will update that device. The configuration and discovery of the various devices requires different fields. [Table 1-5 on page 1-46](#) identifies which devices and credentials and fields that can be updated.

Table 1-5 Device Credentials and Settings Updated Via Seed File Re-Import

Device	Login	Password	Telnet Password	Enable Password	SNMP Community String	Access Type
PIX	Yes	Yes	Yes	Yes	Yes	Yes
PIX7X	Yes	Yes	Yes	Yes	Yes	Yes
ASA	Yes	Yes	Yes	Yes	Yes	Yes
IOS	Yes	Yes	Yes	Yes	Yes	Yes
SWITCH- IOS	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IPS	Yes	Yes	N/A	N/A	N/A	No
SecureACSSE	N/A	N/A	N/A	N/A	N/A	N/A

Discovering and Testing Connectivity Options

When you add a device, you should check its connectivity or perform the discovery. Checking a device's connectivity or discovery analyzes the device's configuration, checks that MARS can process its events, and that MARS can understand its NAT information.

You can test these devices for connectivity or perform discovery:

- Cisco IOS
- Cisco PIX
- Cisco ASA
- Cisco Switch CatOS
- Cisco Switch IOS
- Cisco IDS
- Cisco IPS 6.x
- Cisco IDSM
- Cisco FWSM
- Cisco Security Manager server
- Cisco VPN Concentrator 4.x
- Check Point
- Extreme ExtremeWare 6.x
- NetScreen

Verifying Connectivity with the Reporting and Mitigation Devices

After loading the seed file or manually adding devices, you can verify that the devices were loaded by clicking **Admin > System Setup > Security and Monitor Devices**. You should see the devices that you have added populating this page.

You can test the devices by checking the box next to the name of the device and clicking **Edit**. On the device's page, click **Discover** or **Test Connectivity**. The UI displays a "holding pattern" screen while it connects to the device. When complete, it shows you the device's discovery screen.

**Note**

Some devices cannot be checked for connectivity nor can be discovered. The next section, [Discovering and Testing Connectivity Options, page 1-47](#), contains a list of devices that can be checked or discovered.

