Device Configuration Guide for Cisco Security MARS, Release 6.x

August 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16778-01

Device Configuration Guide for Cisco Security MARS, Release 6.x

CONTENTS

Preface xiii

Audience xiii

Organization xiii

Conventions xv

Obtaining Documentation, Obtaining Support, and Security Guidelines xvi

xvi

CHAPTER 1 **Configuring Reporting and Mitigation Devices in MARS** 1-1

Preparation Overview 1-1

Taskflow for Adding Devices to MARS 1-2

Prioritizing the Devices to Add 1-3

Bootstrap Summary Table 1-3

Understanding Access IP, Reporting IP, and Interface Settings 1-10

Access IP 1-10

Reporting IP 1-11

Interface Settings 1-11

Selection of the Access Type 1-11

Configure SNMP Access for Devices in MARS 1-13

Configure Telnet Access for Devices in MARS 1-13

Configure SSH Access for Devices in MARS 1-13

Configure FTP Access for Devices in MARS 1-14

Activate the Reporting and Mitigation Devices 1-15

Discovering Your Network: Layer 3 Topology Discovery 1-15

Add a Community String for a Network 1-16

Add a Community String for an IP Range 1-17

Add Valid Networks to Discovery List 1-17

Remove Networks from Discovery List 1-18

Discover Layer 3 Data On Demand 1-18

Scheduling Topology Updates 1-18

Schedule a Network Discovery 1-19

Edit a Scheduled Topology Discovery 1-20

Delete a Scheduled Topology Discovery 1-20

Run a Topology Discovery on Demand 1-20

Troubleshoot Layer 3 Network Discovery 1-21

Configuring Resource Usage Data 1-21
Enabling the Required SNMP OIDs for Resource Monitoring 1-22
Adding Reporting and Mitigation Devices 1-31
Adding Reporting and Mitigation Devices Using Automatic Topology Discovery 1-32
Add Reporting and Mitigation Devices Individually 1-33
Adding Multiple Reporting and Mitigation Devices Using a Seed File 1-34
Devices that Require Custom Seed Files 1-35
Devices that Require Updates After the Seed File Import 1-35
Seed File Header Columns 1-36
Load Devices From the Seed File 1-45
Bulk Update of Device Credentials using Seed Files 1-46
Discovering and Testing Connectivity Options 1-47
Verifying Connectivity with the Reporting and Mitigation Devices 1-47

CHAPTER 2 **Configuring Network-based IDS and IPS Devices 2-1**
Cisco IDS 4.0 and IPS 5.x Sensors 2-1
Bootstrap the Cisco Sensor 2-1
Enable the Access Protocol on the Sensor 2-2
Enable the Correct Signatures and Actions 2-2
Add and Configure a Cisco IDS or IPS Device in MARS 2-2
Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File 2-4
View Detailed Event Data for Cisco IPS Devices 2-5
Verify that MARS Pulls Events from a Cisco IPS Device 2-5

CHAPTER 3 **NetScreen IDP Device and Server Support 3-1**
Bootstrap a NetScreen Security Manager 3-2
Bootstrap a NetScreen IDP Management Server 3-2
Add NetScreen Server or Sensor to MARS 3-2

CHAPTER 4 **Cisco IPS 6.x and 7.x Devices and Virtual Sensors 4-1**
Bootstrap the Cisco Sensor 4-1
Cisco IPS 5.x, 6.x, and 7.x Software 4-1
View Detailed Event Data for Cisco IPS Devices 4-2
Enable the Correct Signatures and Actions 4-2
Add and Configure a Cisco IPS 6.x or 7.x Device in MARS 4-3
Verify that MARS Pulls Events from a Cisco IPS Device 4-6
IPS Signature Dynamic Update Settings 4-6
Troubleshooting IPS Signature Dynamic Updates 4-8

Applying Custom Signature Updates 4-8
File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File 4-8
Example Custom Signature Map Files 4-9
Import Custom Signature Maps into MARS 4-11

CHAPTER 5 **Enterasys Dragon 6.x 5-1**
DPM/EFP Configuration 5-1
Configure the DPM or EFP 5-1
Host-side Configuration 5-2
Configure the syslog on the UNIX host 5-2
MARS-side Configuration 5-2
Add Configuration Information for the Enterasys Dragon 5-2
Add a Dragon NIDS Device 5-3

CHAPTER 6 **Snort Devices 6-1**
MARS Expectations of the Snort Syslog Format 6-1
Configure Snort to Send Syslogs to MARS 6-1
Add the Snort Device to MARS 6-2

CHAPTER 7 **McAfee IntruShield 7-1**
Configure McAfee IntruShield 4.1 to Send SNMP Traps to MARS 7-1
Add the IntruShield Manager Host to MARS 7-2
Add IntruShield Sensors Manually 7-3
Add IntruShield Sensors in MARS using Seed Files 7-4
Extracting IntruShield Network Sensor Information from the IntruShield Security Manager 7-4
Add IntruShield Sensors Using a Seed File 7-5

CHAPTER 8 **Symantec ManHunt 8-1**
Symantec ManHunt Side Configuration 8-1
MARS Side Configuration 8-2
Add Configuration Information for Symantec ManHunt 3.x 8-2

CHAPTER 9 **Cisco IPS Modules 9-1**
Enable SDEE on the Cisco IOS Device with an IPS Module 9-1
Add an IPS Module to a Cisco Switch or Cisco ASA 9-2

CHAPTER 10 **IBM Proventia Management/ISS SiteProtector 2.0** 10-1

IBM Proventia Management/ISS SiteProtector to Define Global Event Policies 10-1

IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device 10-5

Configure SiteProtector to Forward SNMP Notifications to MARS 10-6

Add and Configure a SiteProtector Device in MARS 10-10

Add an ISS Agent Manually 10-11

CHAPTER 11 **ISS RealSecure 6.5 and 7.0** 11-1

Configure ISS RealSecure to Send SNMP Traps to MARS 11-1

Add an ISS RealSecure Device as a NIDS 11-3

Add an ISS RealSecure Device as a HIDS 11-4

CHAPTER 12 **Qualys QualysGuard Devices** 12-1

Configure QualysGuard to Scan the Network 12-1

Add and Configure a QualysGuard Device in MARS 12-2

Schedule the Interval at Which Data is Pulled 12-3

Troubleshooting QualysGuard Integration 12-4

CHAPTER 13 **eEye REM 1.0** 13-1

Configure eEye REM to Generate Required Data 13-1

Add and Configure the eEye REM Device in MARS 13-2

CHAPTER 14 **McAfee Foundstone** 14-1

Enable McAfee Foundstone 5.x and later to Use TCP/IP 14-1

Enable McAfee Foundstone (versions prior to 5.0) to Use TCP/IP 14-2

Add and Configure a McAfee Foundstone Device in MARS 14-3

CHAPTER 15 **Cisco Switch Devices** 15-1

Enable Communications Between Devices Running CatOS and MARS 15-1

Enable SNMP Administrative Access 15-2

Enable Telnet Administrative Access 15-2

Enable SSH Administrative Access 15-2

Enable FTP-based Administrative Access 15-2

Configure the Device Running CatOS to Generate Required Data 15-3

Enable Syslog Messages on CatOS 15-3

Enable SNMP RO/RW Strings on CatOS 15-4

Enable NAC-specific Messages 15-4

Enable NAC Support in Cisco Switches 15-5
Enable L2 Discovery Messages 15-6
Add and Configure a Cisco Switch in MARS 15-6
Adding Modules to a Cisco Switch 15-8
Add Available Modules 15-8
Add Cisco IOS Modules Manually 15-9

CHAPTER 16 **Extreme ExtremeWare 6.x** 16-1
Configure ExtremeWare to Generate the Required Data 16-1
Add and Configure an ExtremeWare Switch in MARS 16-1

CHAPTER 17 **Cisco Routers** 17-1
Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later 17-1
Enable SNMP Administrative Access 17-2
Enable Telnet Administrative Access 17-2
Enable SSH Administrative Access 17-2
Enable FTP-based Administrative Access 17-2
Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data 17-2
Enable Syslog Messages 17-3
Enable SNMP RO Strings 17-3
Enable NAC-specific Messages 17-4
NAC on Cisco Routers 17-4
Enable SDEE for IOS IPS Software 17-5
Add and Configure a Cisco Router in MARS 17-5

CHAPTER 18 **Generic Router Device** 18-1
Add and Configure a Generic Router in MARS 18-1

CHAPTER 19 **Configuring Cisco Firewall Devices** 19-1
Cisco Firewall Devices (PIX, ASA, and FWSM) 19-1
Bootstrap the Cisco Firewall Device 19-2
Enable Telnet Access on a Cisco Firewall Device 19-4
Enable SSH Access on a Cisco Firewall Device 19-4
Send Syslog Files From Cisco Firewall Device to MARS 19-4
Device-Side Tuning for Cisco Firewall Device Syslogs 19-6
Logging Message Command 19-6
List of Cisco Firewall Message Events Processed by MARS 19-7
Add and Configure a Cisco Firewall Device in MARS 19-14

Add Security Contexts Manually 19-17
Add Discovered Contexts 19-19
Edit Discovered Security Contexts 19-20
Failover Considerations for PIX, ASA, and Modules in ASA 19-21

CHAPTER 20 **Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x and 8.2.x with NetFlow** 20-1

Contents 20-1
Information About Configuring the Cisco ASA Version 8.1.x with NSEL 20-1
Taskflow for Configuring NSEL on MARS 20-2
Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS 20-3
Prerequisites 20-3
What to Do Next 20-7
To enable NSEL on the MARS Appliance, go to the procedure, "Enabling NSEL Processing on the MARS Appliance" 20-7
Enabling NSEL Processing on the MARS Appliance 20-7
What to Do Next 20-10
Configuring NSEL for MARS on the Cisco ASA 5580 20-10
Additional References 20-13
Related Documents 20-13

CHAPTER 21 **Check Point Devices** 21-1

Determine Devices to Monitor and Restrictions 21-4
Bootstrap the Check Point Devices 21-5
Add the MARS Appliance as a Host in Check Point 21-6
Define an OPSEC Application that Represents MARS 21-7
Obtain the Server Entity SIC Name 21-10
Select the Access Type for LEA and CPMI Traffic 21-12
Create and Install Policies 21-14
Verify Communication Path Between MARS Appliance and Check Point Devices 21-15
Reset the OPSEC Application Certificate of the MARS Appliance 21-16
Add and Configure Check Point Devices in MARS 21-18
Add a Check Point Primary Management Station to MARS 21-19
Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station 21-23
Add a Check Point Certificate Server 21-26
Edit Discovered Log Servers on a Check Point Primary Management Station 21-27
Edit Discovered Firewall on a Check Point Primary Management Station 21-29
Define Route Information for Check Point Firewall Modules 21-29

Specify Log Info Settings for a Child Enforcement Module or Log Server 21-31
Verify Connectivity Between MARS and Check Point Devices 21-34
Remove a Firewall or Log Server from a Check Point Primary Management Station 21-34
Troubleshooting MARS and Check Point 21-35

CHAPTER 22 **NetScreen ScreenOS Devices** 22-1
Bootstrap the NetScreen Device 22-1
Add the NetScreen Device to MARS 22-5

CHAPTER 23 **Cisco NAC Appliance** 23-1
Bootstrap the Cisco NAC Appliance 23-1
Define a Cisco NAC Appliance in MARS Manually 23-2

CHAPTER 24 **Cisco VPN 3000 Concentrator** 24-1
Bootstrap the VPN 3000 Concentrator 24-1
Add the VPN 3000 Concentrator to MARS 24-2

CHAPTER 25 **Cisco Wireless LAN Controller** 25-1
WLAN Configuration Overview 25-2
Bootstrap the WLAN Controller 25-3
Add a Cisco Wireless LAN Controller to MARS 25-3
Manually Define Access Points 25-4

CHAPTER 26 **Configuring AAA Devices** 26-1
Supporting Cisco Secure ACS Server 26-2
Supporting Cisco Secure ACS Solution Engine 4.x 26-2
Supporting Cisco Secure ACS Solution Engine 3.x 26-2
Bootstrap Cisco Secure ACS 26-3
Configure Cisco Secure ACS 4.x to Generate Logs 26-3
Configure Cisco Secure ACS 3.x to Generate Logs 26-4
Define AAA Clients 26-6
Configure TACACS+ Command Authorization for Cisco Routers and Switches 26-8
Install and Configure the PN Log Agent 26-8
Upgrade PN Log Agent to a Newer Version 26-11
Application Log Messages for the PN Log Agent 26-11
Add and Configure an Cisco Secure ACS Server in MARS 26-13
Add and Configure a Cisco Secure ACS Solutions Engine in MARS 26-15

Troubleshooting Cisco Secure ACS Integration 26-15
Error Messages 26-16

CHAPTER 27 **Cisco Security Agent 4.x and 5.x Device** 27-1
Configure CSA Management Center to Generate Required Data 27-2
Configure CSA MC to Forward SNMP Notifications to MARS 27-2
Export CSA Agent Information to File 27-2
Add and Configure a CSA MC Device in MARS 27-3
Add a CSA Agent Manually 27-4
Add CSA Agents From File 27-5
Troubleshooting CSA Agent Installs 27-6

CHAPTER 28 **Entercept Entercept 2.5 and 4.0** 28-1
Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5) 28-1
Create a CSV file for Entercept Agents in Version 2.5 28-2
Define the MARS Appliance as an SNMP Trap Target 28-2
Specific the Events to Generate SNMP Traps for MARS 28-2
Add and Configure an Entercept Console and its Agents in MARS 28-3
Add the Entercept Console Host to MARS 28-3
Add Entercept Agents Manually 28-4
Add Entercept Agents Using a Seed File 28-4

CHAPTER 29 **Symantec AntiVirus Configuration** 29-1
Configure the AV Server to Publish Events to MARS Appliance 29-2
Export the AntiVirus Agent List 29-7
Add the Device to MARS 29-8
Add Agent Manually 29-9
Add Agents from a CSV File 29-9

CHAPTER 30 **McAfee ePolicy Orchestrator Devices** 30-1
Configure ePolicy Orchestrator 4.0 to Generate Required Data 30-1
Configure ePolicy Orchestrator 3.5 and 3.6 to Generate Required Data 30-6
Add and Configure ePolicy Orchestrator Server in MARS 30-10
Add ePO Agents From File 30-11

CHAPTER 31 **Cisco Incident Control Server** 31-1
Configure Cisco ICS to Send Syslogs to MARS 31-1

Add the Cisco ICS Device to MARS 31-2
Define Rules and Reports for Cisco ICS Events 31-3

CHAPTER 32 Cisco CSC SSM 32-1
Defining a CSC SSM in MARS 32-1
Related Documents 32-2
Define a CSC SSM in MARS Manually 32-2

CHAPTER 33 Oracle Database Server Generic 33-1
Configure the Oracle Database Server to Generate Audit Logs 33-1
Add the Oracle Database Server to MARS 33-2
Configure Interval for Pulling Oracle Event Logs 33-3

CHAPTER 34 Configuring Web Server Devices 34-1
Microsoft Internet Information Sever 34-1
Install and Configure the Snare Agent for IIS 34-1
To configure IIS for web logging 34-2
MARS-side Configuration 34-5
To add configuration information for the host 34-5
Apache Web Server on Solaris or RedHat Linux 34-7
Sun Java System Web Server on Solaris 34-7
Generic Web Server Generic 34-7
Solaris or Linux-side Configuration 34-7
Install and Configure the Web Agent on UNIX or Linux 34-7
Web Server Configuration 34-8
To configure the Apache web server for the agent 34-8
To configure the iPlanet web server for the agent 34-8
MARS-side Configuration 34-9

CHAPTER 35 Network Appliance NetCache Generic 35-1
Configure NetCache to Send Syslog to MARS 35-1
Add and Configure NetCache in MARS 35-2

CHAPTER 36 Configuring Generic, Solaris, Linux, and Windows Application Hosts 36-1
Adding Generic Devices 36-1
Sun Solaris and Linux Hosts 36-2
Configure the Solaris or Linux Host to Generate Events 36-2
Configure Syslogd to Publish to the MARS Appliance 36-2

Configure MARS to Receive the Solaris or Linux Host Logs 36-3
Microsoft Windows Hosts 36-4
Push Method: Configure Generic Microsoft Windows Hosts 36-5
Install the SNARE Agent on the Microsoft Windows Host 36-5
Enable SNARE on the Microsoft Windows Host 36-6
Pull Method: Configure the Microsoft Windows Host 36-7
Enable Windows Pulling Using a Domain User 36-7
Enable Windows Pulling from Windows NT 36-7
Enable Windows Pulling from a Windows 2000 Server 36-8
Windows Pulling from a Windows Server 2003 or Windows XP Host 36-8
Configure the MARS to Pull or Receive Windows Host Logs 36-9
Windows Event Log Pulling Time Interval 36-11
Define Vulnerability Assessment Information 36-12
Identify Network Services Running on the Host 36-14

INDEX

Preface

This guide details how to prepare devices to report network activities to Cisco Secure MARS. It also describes how to add reporting and mitigation devices to MARS using the web interface. It does not include how to integrate MARS with Cisco Security Manager (which is detailed in the *Cisco Security MARS User Guide*).

Audience

Network administrators preparing network devices to act as reporting or mitigation devices withing the MARS security threat management (STM) system.

Organization

This document contains the following chapters:

- **Chapter 1, "Configuring Reporting and Mitigation Devices in MARS"**—This chapter defines basic concepts about configuring the reporting and mitigation devices that communicate with Cisco Security Monitoring, Analysis, and Response System (MARS). It also recommends a taskflow for how to populate MARS, selecting the devices to add, and details procedures for manually adding or discovering such devices.
- **Chapter 2, "Configuring Network-based IDS and IPS Devices"**—This chapter describes how to bootstrap network-based IPS and IDS devices and add them to MARS as reporting devices.
- **Chapter 3, "NetScreen IDP Device and Server Support"**—
- **Chapter 4, "Cisco IPS 6.x and 7.x Devices and Virtual Sensors"**—This chapter describes how to prepare a Cisco IPS 6.x or 7.x device and any configured virtual sensors to act as a reporting devices to Cisco Secure MARS.
- **Chapter 5, "Enterasys Dragon 6.x"**—
- **Chapter 6, "Snort Devices"**—This chapter explains how to bootstrap and add the Snort-based devices as a reporting device to Cisco Security MARS.
- **Chapter 7, "McAfee IntruShield"**—This chapter describes how to bootstrap McAfee IntruShield network-based IPS devices and add them to MARS as reporting devices.
- **Chapter 8, "Symantec ManHunt"**—
- **Chapter 9, "Cisco IPS Modules"**—
- **Chapter 10, "IBM Proventia Management/ISS SiteProtector 2.0"**—

- **Chapter 11, "ISS RealSecure 6.5 and 7.0"**—
- **Chapter 12, "Qualys QualysGuard Devices"**—This chapter explains how to bootstrap and add the Qualys QualysGuard vulnerability assessment (VA) devices to MARS.
- **Chapter 13, "eEye REM 1.0"**—This chapter explains how to bootstrap and add the eEye REM vulnerability assessment (VA) devices to MARS.
- **Chapter 14, "McAfee Foundstone"**—This chapter explains how to bootstrap and add the McAfee Foundstone vulnerability assessment (VA) devices to MARS.
- **Chapter 15, "Cisco Switch Devices"**—This chapter explains how to bootstrap and add a Cisco switch to Cisco Secure MARS.
- **Chapter 16, "Extreme ExtremeWare 6.x"**—This chapter explains how to bootstrap and add an ExtremeWare switch to Cisco Secure MARS.
- **Chapter 17, "Cisco Routers"**—This chapter explains how to bootstrap and add a Cisco router to Cisco Secure MARS.
- **Chapter 18, "Generic Router Device"**—This chapter explains how to bootstrap and add a generic router to Cisco Secure MARS.
- **Chapter 19, "Configuring Cisco Firewall Devices"**—This chapter describes how to bootstrap Cisco Firewall devices and add them to MARS as reporting devices.
- **Chapter 21, "Check Point Devices"**—Describes how to configure Check Point devices so that their logs can be monitored by Cisco Secure MARS.
- **Chapter 22, "NetScreen ScreenOS Devices"**—Describes how to configure Juniper Networks ScreenOS devices so that their logs can be monitored by Cisco Secure MARS.
- **Chapter 23, "Cisco NAC Appliance"**—Prepare and add a Cisco NAC Appliance 4.1 as a reporting device for Cisco Security MARS.
- **Chapter 24, "Cisco VPN 3000 Concentrator"**—This chapter explains how to bootstrap and add the Cisco VPN 3000 Concentrator to MARS.
- **Chapter 25, "Cisco Wireless LAN Controller"**—This chapter explains how to bootstrap and add a Cisco Wireless Controller to MARS.
- **Chapter 26, "Configuring AAA Devices"**—This chapter explains how to prepare the Cisco Secure ACS server or the Cisco Secure ACS Solution Engine to allow MARS to collect the event logs. It also describes how to configure MARS to receive and process these logs correctly. Using the web interface, you must define a host to represent the Cisco Secure ACS server (or the remote logging agent collecting logs for the Cisco Secure ACS Solution Engine) and then add the software application to that host.
- **Chapter 27, "Cisco Security Agent 4.x and 5.x Device"**—This chapter explains how to bootstrap and add the Cisco Security Agent host-based IPS softwrae as a reporting device to Cisco Security MARS.
- **Chapter 28, "Entercept Entercept 2.5 and 4.0"**—
- **Chapter 29, "Symantec AntiVirus Configuration"**—This chapter describes how to configure and add Symantec AntiVirus devices as reporting devices to Cisco Secure MARS.
- **Chapter 30, "McAfee ePolicy Orchestrator Devices"**—This chapter describes how to configure and add McAfee ePolicy Orchestrator devices as reporting devices to Cisco Secure MARS.
- **Chapter 31, "Cisco Incident Control Server"**—This chapter describes how to configure and add the Cisco Inciddent Control Server as a reporting device to Cisco Security MARS.

- **Chapter 32, "Cisco CSC SSM"**—Describes how to configure and add the Cisco Content Security and Control Security Services Module, which is a seperate module that runs in the Cisco ASA to provide an all-in-one antivirus and spyware management solution for a network.
- **Chapter 33, "Oracle Database Server Generic"**—This chapter explains how to bootstrap and add an Oracle-based database applications to MARS.
- **Chapter 34, "Configuring Web Server Devices"**—This chapter explains how to bootstrap and add webservers to MARS.
- **Chapter 35, "Network Appliance NetCache Generic"**—This chapter describes how to define the Network Appliance NetCache web proxy devices.
- **Chapter 36, "Configuring Generic, Solaris, Linux, and Windows Application Hosts"**—This chapter describes how to define hosts as reporting devices or how to describe them to MARS to assist with false positive and vulnerability assessment.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**boldface screen** font
Variables you enter	*italic screen* font
Menu items and button names	**boldface** font
Indicates menu items to select, in the order you select them.	**Option > Network Preferences**

Tip Identifies information to help you get the most benefit from your product.

Note Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

Warning **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

PART 1

Concepts

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 ad 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 summaries 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	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	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	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. **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. 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	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	1. Enable RDEP for IDS modules. 2. Configure the following signature actions: – 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	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: – 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	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: – 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	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: – 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 Entercept		Chapter 28, "Entercept Entercept 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	Do one of the following: • Install and configure the SNARE agent • Create or edit an administrative account to ensure that it has permissions to pull the event data	Syslog (pushed by SNARE agent) or event data pull using MS-RPC Push Method: Configure Generic Microsoft Windows Hosts, page 36-5 Pull Method: Configure the Microsoft Windows Host, page 36-7
Solaris	—	Syslog (from Device) Sun Solaris and Linux Hosts, page 36-2
Redhat Linux	—	Syslog (from Device) Sun Solaris and Linux Hosts, page 36-2
Web Server		
Microsoft Internet Information Server	—	Syslog (from SNARE agent) Install and Configure the Snare Agent for IIS, page 34-1

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 requires 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, where as 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 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:

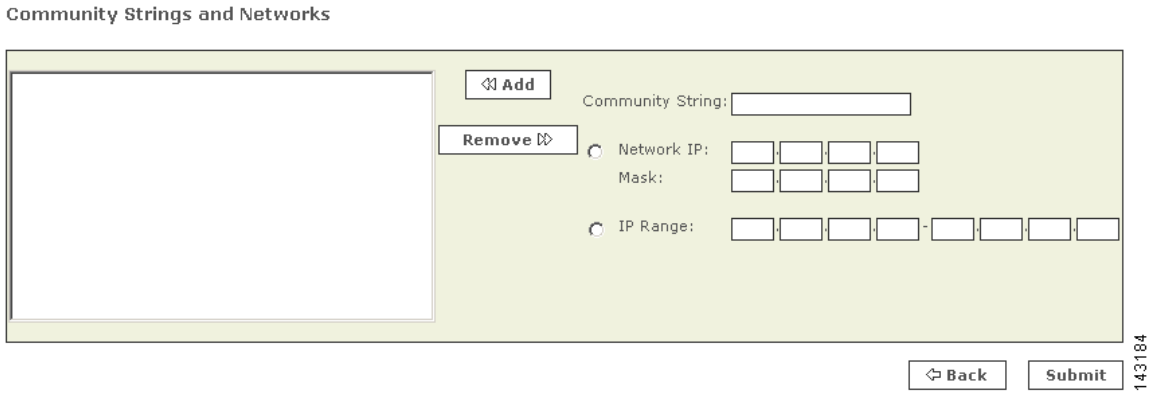
1. Configure MARS to discover the SNMP-blocked devices separately using administrative protocols such as Telnet, SSH, or Checkpoint CPMI.
2. If the routes cannot be discovered for a SNMP-blocked device via the administrative protocol (such as a software-based Checkpoint Firewall-1), either manually define 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.



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.

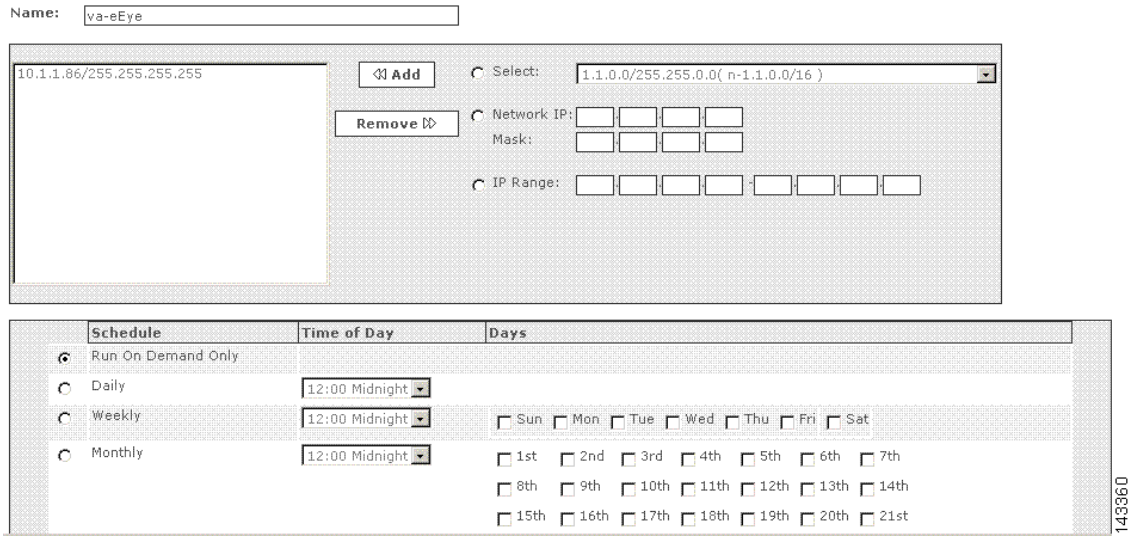
Configuration discovery depends on the device type, proper authorization, an access type, such as Telnet or SSH, and an access IP address. When device discovery is performed, MARS contacts the device and conducts a topology and configuration discovery. This discovery collects all of the route, NAT, and 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



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 *login*, *Password*, or*#,*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 is 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	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	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
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 stings 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 it's 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 stings 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,Vpnspn12,,vPfw1ne,,,,,,,,,
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	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 **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.

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

Column B	SNMP RO/RW Community	The device's SNMP RO community name here. **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).

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) **Note** Some of the devices supported in the GUI cannot be entered via a CSV file. Use the following strings represent the desired device type: • `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`: for Cisco Wireless LAN Controller 4.x, 5.x

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

Column F	ACCESS TYPE	The Access Type for this device. Your choices are: • TELNET • FTP • SSH • SSL • SNMP (default) • RPC (Windows only) 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.

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.

PART 2

Intrusion Detection and Prevention (Network based)

CHAPTER 2

Configuring Network-based IDS and IPS Devices

Revised: June 27, 2008

Network intrusion detection and intrusion preventions systems are a critical source for identifying active attacks to MARS. This chapter explains how to bootstrap and add network-based IDS and IPS devices to MARS.

This chapter contains the following topics:

- Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1

Cisco IDS 4.0 and IPS 5.x Sensors

Adding a Cisco IDS or IPS network sensor to MARS involves two parts:

1. Bootstrap the Cisco Sensor, page 4-1
2. Add and Configure a Cisco IDS or IPS Device in MARS, page 2-2
3. Verify that MARS Pulls Events from a Cisco IPS Device, page 4-6

The following topic supports Cisco IDS and IPS devices:

- View Detailed Event Data for Cisco IPS Devices, page 4-2

Note If you've imported your sensor definitions using the seed file format, as specified in Load Devices From the Seed File, page 1-45, you must define the networks monitored by the sensor.

Bootstrap the Cisco Sensor

Preparing a sensor to be monitored by MARS involves preparing the sensor so MARS can communicate with it and ensuring that the correct data is being generated.

This section contains the following topics:

- Enable the Access Protocol on the Sensor, page 2-2
- Enable the Correct Signatures and Actions, page 4-2

Enable the Access Protocol on the Sensor

The configuration of the sensor depends on the version of the software that is running on the sensor. The following topics identify the requirements of each version:

This section contains the following topics:

- Cisco IDS 4.x Software, page 2-2
- Cisco IPS 5.x, 6.x, and 7.x Software, page 4-1

Cisco IDS 4.x Software

For Cisco IDS 4.x devices, MARS pulls the logs using RDEP over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **accessList ipAddress** ***ip_address****netmask* command to enable this access.

Cisco IPS 5.x, 6.x, and 7.x Software

For Cisco IPS 5.x, 6.x, and 7.x devices, MARS pulls the logs using SDEE over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **access-list*****ip_address/netmask*** command to enable this access.

Enable the Correct Signatures and Actions

If the signature actions are correctly configured, MARS can display the trigger packet information for the first event that fires a signature on a Cisco IDS or IPS device. MARS is also able to pull the IP log data from Cisco IDS and IPS devices, however, this operation is system intensive. Therefore, you should select the set of signatures that generate IP log data carefully.

When configuring the active signatures on a Cisco IDS or IPS device, you must specify the alert action and the action that generates the desired data:

- To view trigger packets, you must enable the “produce-verbose-alert” action.
- To view IP logs, you must enable the alert or “produce-verbose-alert” action and the “log-pair-packets” action.

Caution Configuring IP logging and verbose alerts on the sensor is system intensive and does affect the performance of your sensor. In addition, it affects the performance of your MARS Appliance. Because of these effects, you be cautious in configuring signatures to generate IP logs.

Add and Configure a Cisco IDS or IPS Device in MARS

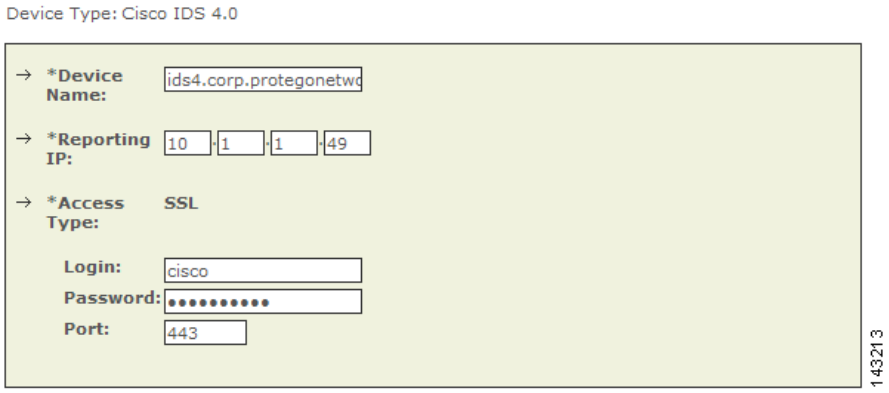
To add and configure a Cisco IDS or IPS device in MARS, follow these steps:

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

Step 2 Do one of the following:

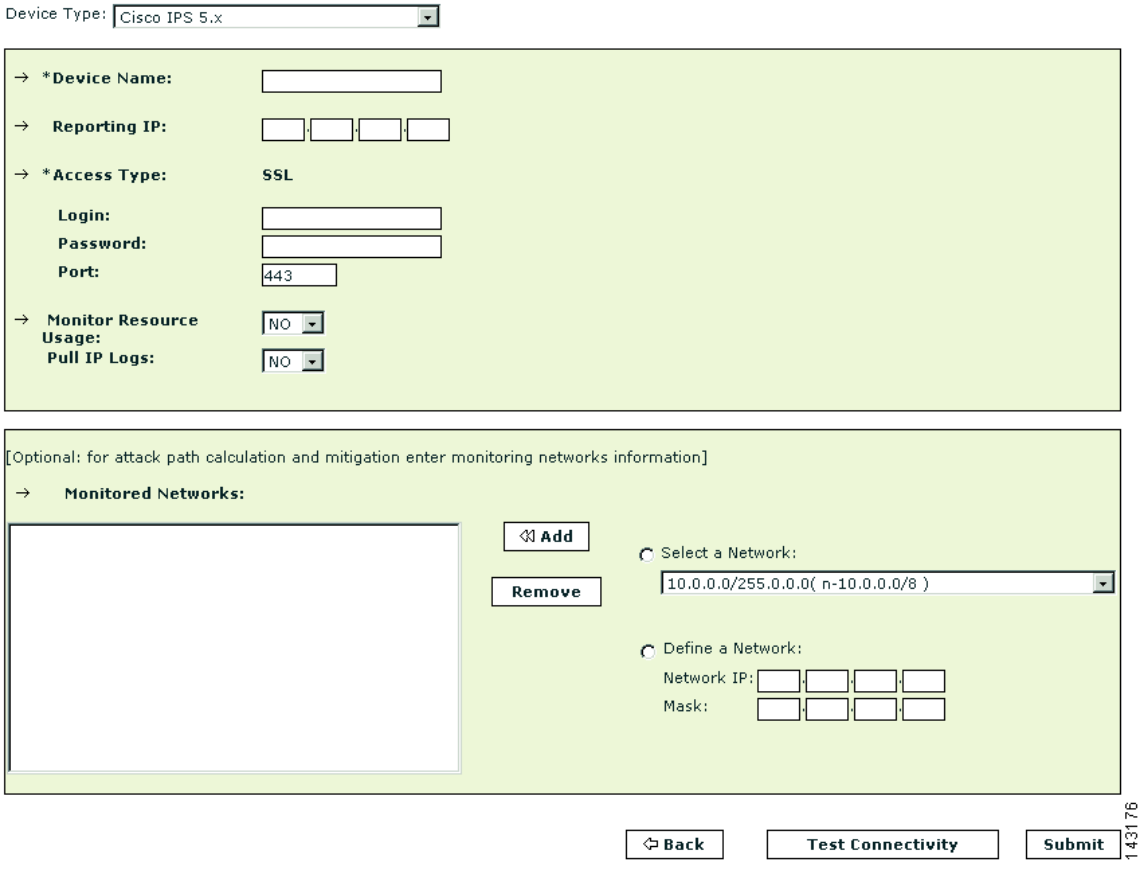
- Select **Cisco IDS 4.0** from the Device Type list.

Figure 2-1 Configure Cisco IDS 4.0



- Select **Cisco IPS 5.x** from the Device Type list.

Figure 2-2 Configure Cisco IPS 5.x



Step 3 Enter the hostname of the sensor in the Device Name field.

The Device Name value must be identical to the configured sensor name.

Step 4 Enter the administrative IP address in the Access IP field.

Step 5 Enter the administrative IP address in the Reporting IP field.

The Reporting IP address is the same address as the administrative IP address.

Step 6 In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.

Step 7 In the Password field, enter the password associated with the username specified in the Login field.

Step 8 In the Port field, enter the TCP port on which the webserver running on the sensor listens. The default HTTPS port is 443.

Note While it is possible to configure HTTP only, MARS requires HTTPS.

Step 9 To pull the IP logs from the sensor, select **Yes** in the Pull IP Logs box.

Step 10 (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.

a. Enter the network address in the Network IP field.

b. Enter the corresponding network mask value in the Mask field.

c. Click **Add** to move the specified network into the Monitored Networks field.

d. Repeat as needed.

Step 11 (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.

a. Select a network from in the Select a Network list.

b. Click **Add** to move the specified network into the Monitored Networks field.

c. Repeat as needed.

Step 12 To verify the configuration, click **Test Connectivity**.

Step 13 Click **Submit**.

Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File

After you import a Cisco IPS or IDS device into MARS using a seed file, you must define the networks that are monitored by that sensor.

To define the networks monitored by a sensor, follow these steps:

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

Step 2 Select the check box next to the Cisco IPS or IDS device that was imported using a seed file. and click **Edit**.

Step 3 (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.

a. Enter the network address in the Network IP field.

b. Enter the corresponding network mask value in the Mask field.

c. Click **Add** to move the specified network into the Monitored Networks field.

d. Repeat as needed.

Step 4 (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.

a. Select a network from in the Select a Network list.

b. Click **Add** to move the specified network into the Monitored Networks field.

c. Repeat as needed.

Step 5 To save your changes, click **Submit**.

Step 6 To enable MARS to start sessionizing events from this module, click **Activate**.

View Detailed Event Data for Cisco IPS Devices

In addition to the alert message, you can view the trigger packets and IP log data associated with incidents reported by Cisco IDS 4.x and Cisco IPS 5.x, 6.x, and 7.x devices, whether they are sensor appliances or modules. This information is useful when an in-depth understanding of the attack method is desired. MARS includes two event types that focus on the these two data types:

- **Trigger packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. The trigger packet provides a single data packet—the data packet that caused the alarm to fire.
- **Packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. Although the amount of data contained in an IP log varies based on sensor configuration, by default an IP log contains 30 seconds of packet data. To view this data, you must enable the Pull IP Logs option on the Cisco IPS device under Admin > System Setup > Security and Monitor Devices.

For the correct signature settings required to generate this data, see Enable the Correct Signatures and Actions, page 4-2.

If the IP log feature is enable for the reporting Cisco IPS device, these event types are combined as part of the incident data. You can view this data by drilling down in an incident, expanding the desired event type (either Packet Data or Trigger Packet Data), selecting an event, and clicking on the RAW Events for this Session icon under the Reporting Device column of that event. The source, destination, and other data displayed for these events matches that of the original alert. In addition, this data appears hexadecimal and binary format.

Note The trigger packet and IP log data is stored using a base64-encoded format in the MARS database. Therefore, keyword search does not work on it if you just provide the search string.

Verify that MARS Pulls Events from a Cisco IPS Device

Note If the Test Connectivity operation does not fail when configuring a Cisco IPS device in the MARS web interface, then communications are enabled. This task allows you to further verify the alerts are generated and pulled correctly.

It is common to create benign events on the network to verify the data flow. To verify the data flow between a Cisco IPS device and MARS, perform the following tasks:

1. On the Cisco IPS device, enable and alert on the signatures 2000 and 2004. The signatures monitor ICMP messages (pings).
2. Ping a device on the subnet on which the Cisco IPS device is listening. The events are generated and pulled by MARS.
3. Verify that the events appear in the MARS web interface. You can perform a query using the Cisco IPS device.
4. Once the dataflow is verified, you can disable the 2000 and 2004 signatures on the Cisco IPS device.

CHAPTER 3

NetScreen IDP Device and Server Support

MARS supports multiple versions of NetScreen IDP. How this support is realized within MARS differs based on the version of the sensor that you are running.

- **NetScreen IDP-Management Server**—The NetScreen IDP Management Server is the management software for IDP version 2.x and 3.x sensors. Usually, the IDP-Management Server is installed on the IDP appliance. However, it can be removed from the IDP appliance an and installed on a Solaris or Linux server. In MARS, IDP v2.1 and 3.x are both supported as agents on a Linux host running IDP-Management Server.
- **NetScreen Security Manager**— (NSM) provide support for the following NetScreen sensors:
  - NetScreen IDP 4.0
  - NetScreen IDP 4.1

Note It also supports other Juniper Networks devices such as NetScreen-x, ISG-x and SSG-x. These devices are not currently supported in MARS.

IDP sensors running 4.0 and later are supported by NSM running on a Linux host. NSM forwards syslog events to MARS for processing.

Tip Because MARS does not support multiple reporting devices on the same host (as defined by reporting IP address), IDP-Management Server and NSM cannot co-exist on the same host unless they report to MARS via different IP addresses. However, you can define multiple sensors per management server.

Adding a NetScreen IDP sensor to MARS involves two parts:

1. Bootstrap the management server (or IDP sensor 4.1) that will publish syslog events to MARS.
2. Add and configure the management server (or IDP 4.1 sensor) in the MARS web interface.

This chapter contains the following topics:

- Bootstrap a NetScreen Security Manager, page 3-2
- Bootstrap a NetScreen IDP Management Server, page 3-2
- Add NetScreen Server or Sensor to MARS, page 3-2

Bootstrap a NetScreen Security Manager

MARS can retrieves logs from a NetScreen Security Manager server in support of IDP 4.x sensors. To prepare the NetScreen Security Manager server, you must enabling logging and syslog generation for the security policies that are running on IDP sensors that it manages.

Bootstrap a NetScreen IDP Management Server

MARS can retrieves logs from a NetScreen IDP Management Server in support of IDP 2.x and 3.x sensors. To prepare the NetScreen IDP Management Server, you must enabling logging and syslog generation for the security policies that are running on IDP sensors that it manages.

To enable logging and syslog generation, follow these steps:

Step 1 Click **NetScreen-Global Pro > IDP Manager > IDP**.

Step 2 Log in to the IDP Manager.

Step 3 From the main menu, click **Tools > Preferences**.

Step 4 In the tree on the left, click **Management Server**, enter the Local Controller's address in the Syslog host field, and click **OK**.

Step 5 Click **Security Policies**, and the name of your policy.

Step 6 In the Notification column, right-click anywhere in the cell in the field and select **Configure**.

Step 7 Check **enable logging** and **syslog** for each policy, and click **OK**. Repeat for all of your policies.

Step 8 From the main menu, click **Policy > Install**.

Add NetScreen Server or Sensor to MARS

Whether the syslog messages are being sent to MARS from a management server on behalf of sensors or an IDP 4.1 sensor is publishing the syslog messages directly to MARS, you must perform three steps:

1. Define a Linux host that represents the management server
2. Add configuration information about the software on the management server. This information appears as a software-based security application (a management console) running on the Linux host.
3. Add configuration information for the IDP sensors that are managed by the server. These sensors appears as modules of a management console.

To define the IDP sensors, follow these steps:

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 If adding a new host, specify the following values:

enter the and IP Addresses, and click **Apply**.

- **Device Name**—Specify a name for the host that is representing either a management server.

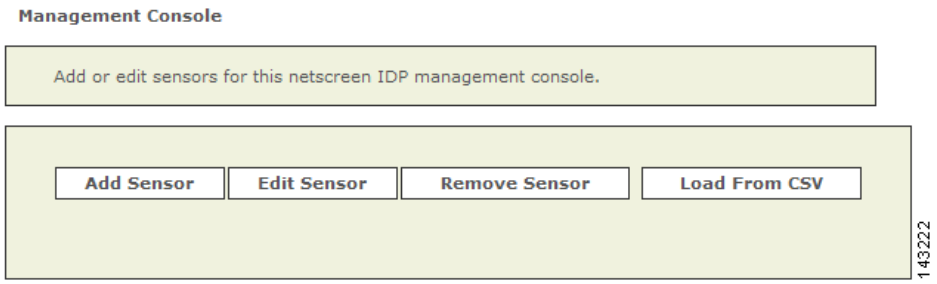
- **Reporting IP Address**—Enter the IP address from which MARS will receive the syslog messages from this device.
- **Operating System**—Select Linux.
- **IP Address and Network Mask**—Under Enter interface information, specify the values of at least one interface. You must define the name, IP address, and network mask for that interface.

Step 4 Click **Apply**, then click **Reporting Applications** tab, and select one of the following values from the Select application list:

- **NetScreen IDP 2.1**—Select this value to add a NetScreen IDP Management Server (IDP 2.1) to this host.
- **NetScreen IDP 3.x**—Select this value to add a NetScreen IDP Management Server (IDP 3.x) to this host.
- **Juniper IDP 4.x**—Select this value to add a NetScreen-Security Manager (IDP 4.x) to this host. This value is also the one that you add to specify a standalone IDP 4.1 sensor (the software version simply instructs MARS as to how to parse the incoming syslog messages).

Step 5 Click **Add**.

The Management Console page appears.



Step 6 To add a sensor, click **Add Sensor**.

The Select the device on which sensor is running or enter a new device page appears.

Step 7 Click **Add New**.

The Add Sensor page appears.

Step 8 Specify the following values:

- **Device Name**—This name is the name that will appear in the list of devices attached to this management console.
- **Sensor Name**—Specify the hostname of the sensor.
- **Reporting IP**—Specify the IP address used by the sensor to send syslog messages to this management console.
- **Interface name, IP address, and network mask**—Specify the name, IP address and network mask values for at least one interface running on the sensor.
- **Monitored Networks**—Specify which networks are monitored by the sensor. This information is used for attack path calculation and mitigation.

Step 9 Click **Submit** to add the sensor the management console.

Step 10 Click **Submit** on the Management Console page to add the application to the host.

Depending on the device type that you added, one of the following values appears under the Device Type list:

- NetScreen IDP Management Server (IDP 2.1)
- NetScreen IDP Management Server (IDP 3.x)
- NetScreen-Security Manager (IDP 4.x)

Step 11 Click **Done** to commit your changes to the database.

Step 12 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 4

Cisco IPS 6.x and 7.x Devices and Virtual Sensors

This chapter describes how to prepare a Cisco IPS 6.x and 7.x devices and any configured virtual sensors to act as a reporting devices to Cisco Secure MARS.

This chapter contains the following topics:

- Bootstrap the Cisco Sensor, page 4-1
- Add and Configure a Cisco IPS 6.x or 7.x Device in MARS, page 4-3
- Verify that MARS Pulls Events from a Cisco IPS Device, page 4-6
- IPS Signature Dynamic Update Settings, page 4-6
- Applying Custom Signature Updates, page 4-8

Bootstrap the Cisco Sensor

Preparing a sensor to be monitored by MARS involves preparing the sensor so MARS can communicate with it and ensuring that the correct data is being generated.

This section contains the following topics:

- Cisco IPS 5.x, 6.x, and 7.x Software, page 4-1
- View Detailed Event Data for Cisco IPS Devices, page 4-2

Cisco IPS 5.x, 6.x, and 7.x Software

For Cisco IPS 5.x, 6.x, and 7.x devices, MARS pulls the logs using SDEE over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **access-list***ip_address/netmask* command to enable this access.

View Detailed Event Data for Cisco IPS Devices

In addition to the alert message, you can view the trigger packets and IP log data associated with incidents reported by Cisco IDS 4.x and Cisco IPS 5.x, 6.x, and 7.x devices, whether they are sensor appliances or modules. This information is useful when an in-depth understanding of the attack method is desired. MARS includes two event types that focus on the these two data types:

- **Trigger packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. The trigger packet provides a single data packet—the data packet that caused the alarm to fire.
- **Packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. Although the amount of data contained in an IP log varies based on sensor configuration, by default an IP log contains 30 seconds of packet data. To view this data, you must enable the Pull IP Logs option on the Cisco IPS device under Admin > System Setup > Security and Monitor Devices.

For the correct signature settings required to generate this data, see Enable the Correct Signatures and Actions, page 4-2.

If the IP log feature is enable for the reporting Cisco IPS device, these event types are combined as part of the incident data. You can view this data by drilling down in an incident, expanding the desired event type (either Packet Data or Trigger Packet Data), selecting an event, and clicking on the RAW Events for this Session icon under the Reporting Device column of that event. The source, destination, and other data displayed for these events matches that of the original alert. In addition, this data appears hexadecimal and binary format.

Note The trigger packet and IP log data is stored using a base64-encoded format in the MARS database. Therefore, keyword search does not work on it if you just provide the search string.

Enable the Correct Signatures and Actions

If the signature actions are correctly configured, MARS can display the trigger packet information for the first event that fires a signature on a Cisco IDS or IPS device. MARS is also able to pull the IP log data from Cisco IDS and IPS devices, however, this operation is system intensive. Therefore, you should select the set of signatures that generate IP log data carefully.

When configuring the active signatures on a Cisco IDS or IPS device, you must specify the alert action and the action that generates the desired data:

- To view trigger packets, you must enable the “produce-verbose-alert” action.
- To view IP logs, you must enable the alert or “produce-verbose-alert” action and the “log-pair-packets” action.

Caution Configuring IP logging and verbose alerts on the sensor is system intensive and does affect the performance of your sensor. In addition, it affects the performance of your MARS Appliance. Because of these effects, you be cautious in configuring signatures to generate IP logs.

Add and Configure a Cisco IPS 6.x or 7.x Device in MARS

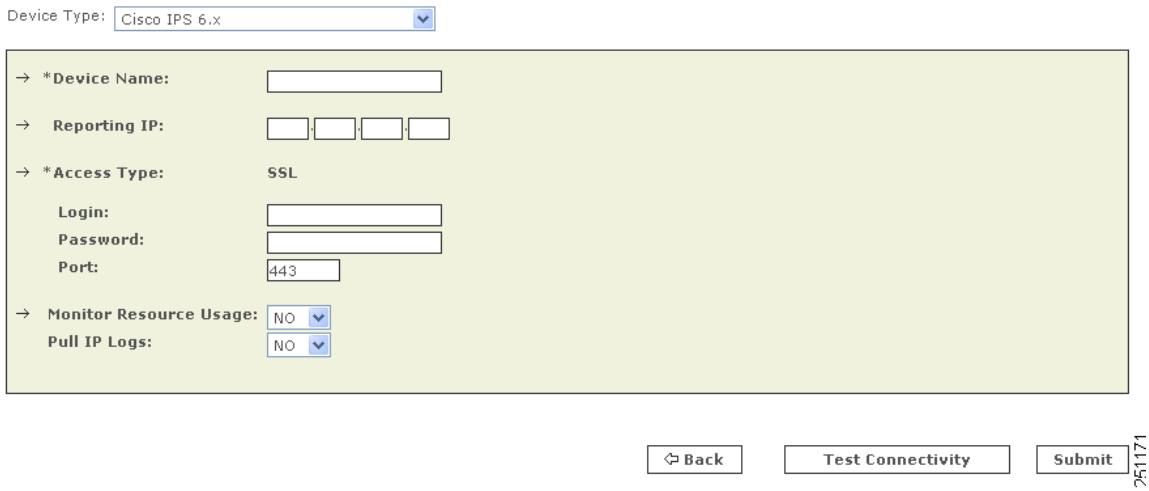
When you define a Cisco IPS 6.x or 7.x device in MARS, you can discover any virtual sensors configured on the device. Discovering these virtual sensors allows MARS to separate the reported events by virtual sensor. It also allows you to tune the list of monitored networks to each virtual sensor, improving the accuracy of the desired reporting.

To add and configure a Cisco IPS 6.x or 7.x device in MARS, follow these steps:

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

Step 2 Select **Cisco IPS 6.x** or **Cisco IPS 7.x** from the Device Type list.

Figure 4-1 Configure Cisco IPS 6.x



Step 3 Enter the hostname of the sensor in the Device Name field.

The Device Name value must be identical to the configured sensor name.

Step 4 Enter the administrative IP address in the Reporting IP field.

The Reporting IP address is the same address as the administrative IP address.

Step 5 In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.

Step 6 In the Password field, enter the password associated with the username specified in the Login field.

Step 7 In the Port field, enter the TCP port on which the webserver running on the sensor listens. The default HTTPS port is 443.

Note While it is possible to configure HTTP only, MARS requires HTTPS.

Step 8 Verify that **NO** is selected in the Monitor Resource Usage list.

While the Monitor Resource Usage option appears on this page, it does not function for Cisco IPS.

Step 9 (Optional) To pull the IP logs from the sensor, select **Yes** from the Pull IP Logs list.

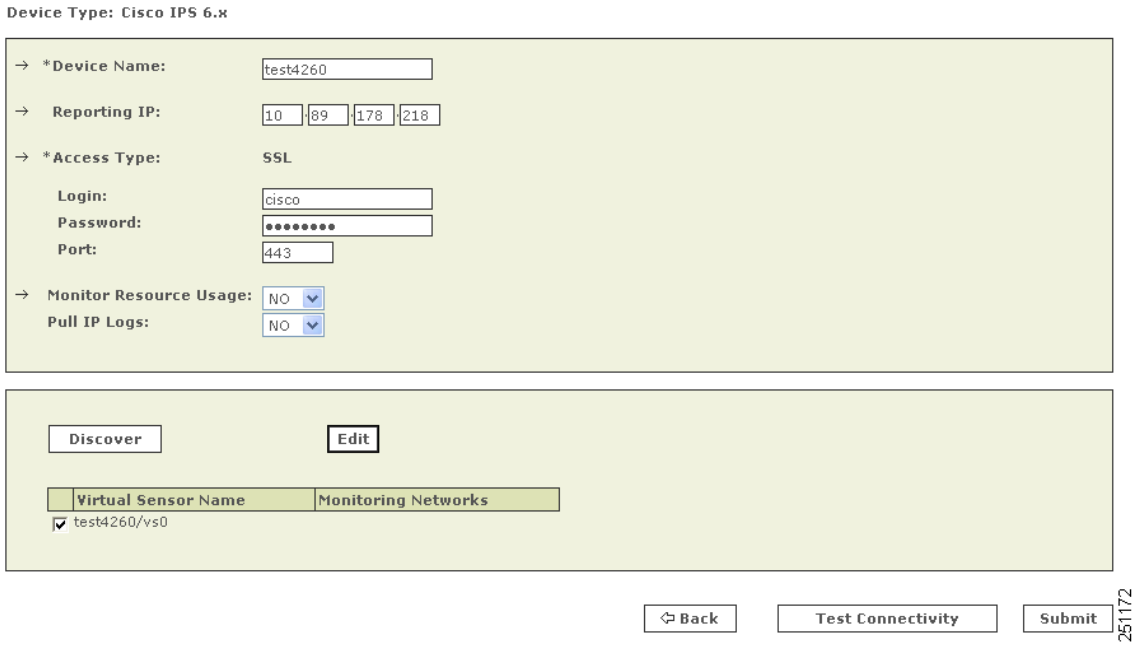
This setting applies to the entire sensor, including those logs generated for virtual sensors alerts. For details on this setting, see View Detailed Event Data for Cisco IPS Devices, page 4-2.

Step 10 To verify the configuration and enable the discovery of virtual sensors, click **Test Connectivity**.

Step 11 To discover any defined virtual sensors, click **Discover**.

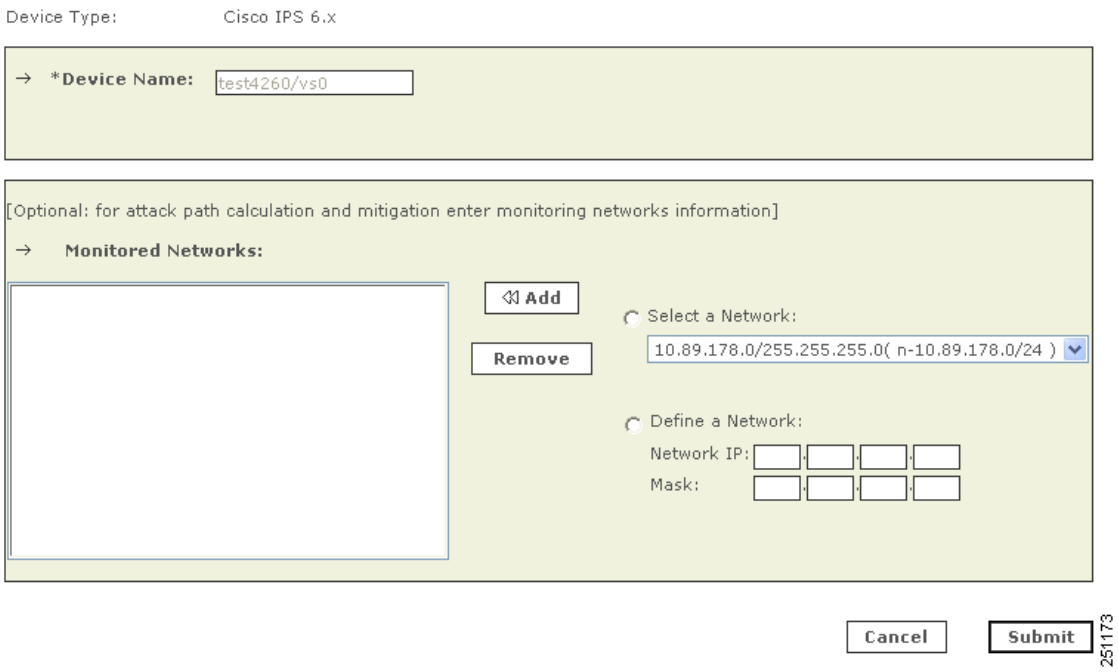
Tip MARS is unaware of changes made to the sensor. Anytime you make changes to the virtual sensor settings, you must click **Discover** on that sensor configuratin page to refresh the virtual sensor details in MARS.

Any virtual sensors are discovered.



Step 12 To define the monitored networks for each virtual sensor, select the checkbox next to the Virtual Sensor Name and click **Edit**.

The IPS Module page appears.



Step 13 (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.

a. Enter the network address in the Network IP field.

b. Enter the corresponding network mask value in the Mask field.

c. Click **Add** to move the specified network into the Monitored Networks field.

d. Repeat as needed.

Step 14 (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.

a. Select a network from in the Select a Network list.

b. Click **Add** to move the specified network into the Monitored Networks field.

c. Repeat as needed.

Step 15 (Optional) Repeat Step 12 through Step 14 for each virtual sensor.

Step 16 To save your changes, click **Submit**.

The device name appears under the Security and Monitoring Information list. 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 17 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Verify that MARS Pulls Events from a Cisco IPS Device

Note If the Test Connectivity operation does not fail when configuring a Cisco IPS device in the MARS web interface, then communications are enabled. This task allows you to further verify the alerts are generated and pulled correctly.

It is common to create benign events on the network to verify the data flow. To verify the data flow between a Cisco IPS device and MARS, perform the following tasks:

1. On the Cisco IPS device, enable and alert on the signatures 2000 and 2004. The signatures monitor ICMP messages (pings).
2. Ping a device on the subnet on which the Cisco IPS device is listening. The events are generated and pulled by MARS.
3. Verify that the events appear in the MARS web interface. You can perform a query using the Cisco IPS device.
4. Once the dataflow is verified, you can disable the 2000 and 2004 signatures on the Cisco IPS device.

IPS Signature Dynamic Update Settings

In releases 6.0 and later, Cisco IPS supports dynamic signature updates. MARS can discover the new signatures and correctly process and categorize received events that match those signatures. If this feature is not configured, the events appears as unknown event type in queries and reports, and MARS does not include these events in inspection rules. These updates provides event normalization and event group mapping, and they enable your MARS Appliance to parse Day Zero signatures from the IPS devices.

The downloaded update information is am XML file that contains the IPS signatures. However, this file does not contain detailed information, such as vulnerability information. Detailed signature information is provided in later MARS signature upgrade packages just as with 3 rd -party signatures.

Note The dynamic IPS signature updates is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail. To check the version, click **Help > About**.

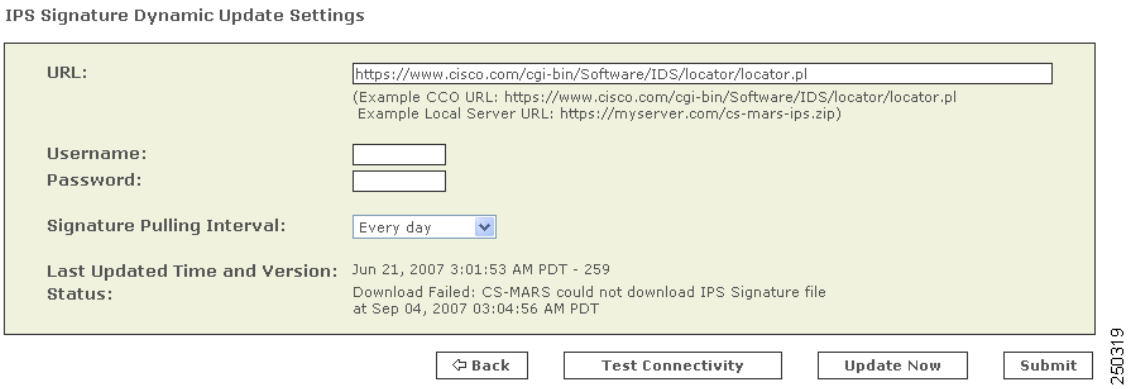
Before You Begin

- Dynamic IPS signature updates are disabled by default.
- Custom IPS signatures are not supported. You must manually import these signatures using the process defined in Applying Custom Signature Updates, page 4-8.
- You can retrieve updates from CCO or from a local web server. After downloading and installing an update, the MARS Appliance performs an auto-activate to load the new signature information.
- If configured to retrieve the signatures from CCO, MARS downloads the most recent package as determined by a combination of package name and the MD5 sum.
- MARS checks for updates at the specified interval, hourly (1, 2, 3, 6, or 12) or daily (1 through 14).

- In a Global Controller-Local Controller deployment, configure the dynamic signature URL and all relevant settings on the Global Controller. Do not attempt to configure these features on the Local Controllers even though the web interface allows you to do so.
- When the Global Controller pulls the new signatures from CCO, all managed Local Controllers download the new signatures from the Global Controller.

To specify the dynamic update settings, follow these steps:

Step 1 Click **ADMIN > System Setup > IPS Signature Dynamic Update Settings**.



Step 2 Enter the following values:

- **URL**—Verify that the path to the software locator is defined. The default value is https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl (https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl), which is located on the Cisco Software Download site. You can specify a local server using the following example https://myserver.com/cs-mars-ips.zip (the zip files can be downloaded from http://www.cisco.com/cgi-bin/tablebuild.pl/mars-ips-sigup).
- **Username**—Specify the username of the account that accesses the secure server. If you are using the default URL value, this is a CCO username.
- **Password**—Specify the password associated with the username value provided.
- **Signature Pulling Interval**—Specify the interval at which the signature updates should be pulled from the server identified in the URL field. Valid options include: Never (default), Every 1, 2, 3, 6, or 12 hours, or Every 1 to 14 days.

Step 3 To verify the settings are correct, click **Test Connectivity**.

Step 4 Once the settings are verified, click **Submit**.

Step 5 Click **Activate**.

Tip Once this feature is enabled, you can determine the current signature version pulled down by MARS by selecting **Help > About** and reviewing the IPS Signature Version value.

Troubleshooting IPS Signature Dynamic Updates

Two types of failures can occur, and they are identified in the Status field of the IPS Signature Dynamic Update Settings page:

- **Failure to download the package.** Verify that the MARS Appliance has connectivity to the specified destination and that it is using the correct username and password.
- **Failure to install.** Indicates a problem with the package itself, possibly corrupted during the download.

Applying Custom Signature Updates

Cisco IPS 6.0 enables you to define custom signatures for Cisco IPS devices. Before you can define an inspection rule in MARS that fires when that signature is detected, you must map that signature to a MARS event type.

To enable this mapping within MARS, you must perform the following tasks:

1. Define a custom signature map file (an XML file) that maps between the custom IPS signature and a MARS event type.
2. Import that custom map file into the Local Controller that monitors the Cisco IPS device on which that custom signature is running.

Note Cisco recommends that any Global Controller/Local Controller relationships be established prior to applying any custom signature updates.

This section contains the following topics:

- File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File, page 4-8
- Example Custom Signature Map Files, page 4-9
- Import Custom Signature Maps into MARS, page 4-11

File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File

Adhere to the following naming conventions for any XML file that maps a custom Cisco IPS signature to a MARS event type:

- **<number>.custom.inc.xml**—Where <number> is an integer . Start with 1 and increment for each additional signature (for example, 1.custom.inc.xml) This number indicates the version number of the custom signature package. Subsequent updates must increment this version number.

  MARS uses this number to ensure that the Local Controllers are synchronized with the Global Controller. The Help About page of each MARS appliance displays the customer signature version, such as Custom version: 1.

The following elements or attributes are required for the custom signature XML mapping file:

- **encoding**—The header of the XML file varies based on the version of software running on the MARS appliance. If the software version is 4.3.1, then the header should be <?xml version="1.0" encoding="ISO-8859-1"?>. Otherwise, if it is running 5.3.1, the header must be <?xml version="1.0" encoding="UTF-8"?>.
- **<EventType />**—This element specifies the custom signature ID for this event. The EVENT_TYPE attribute value identifies either an existing MARS event type or a new MARS event type. If it is a new MARS event type, it should be in the range of 90000000-9049000. For example: ET-9000000. The prefix "ET-xxxxxxx" is required for all values in this attribute. This value range is reserved for custom signature IDs.

  Note If the ID maps to a previously used custom ID, information for that custom event is updated with the data in this XML file. If ID maps to a system event type, the information is not updated.

- **<EVENT_PRIORITY />**—This element organizes the priority of this custom signature. The expected value is one of the following: HIGH, MEDIUM, or LOW. The event priority value should match the severity of the firing signature as configured on the Cisco IPS device.
- **<EVENT_TYPE_NAME />**—This element names the custom signature event. The expected value is a string of up to 300 characters. Valid character sets are WE8ISO8859P1 for 4.3.1 and AL32UTF8 for 5.3.1. Cisco recommends that this event type name match that of the signature name as configured on the Cisco IPS device.
- **<LONG_DESCRIPTION />**—This element describes the custom signature event. Acceptable value is a "unlimited" string of characters. Valid character sets are WE8ISO8859P1 for 4.3.1 and AL32UTF8 for 5.3.1.
- **<Device Event Type DEVICE_ET="signatureId/subId"/>**—The DEVICE_ET attribute of this element identifies the IPS custom signatureId/subId. For example, if the IPS signature has sigID=60001 and subID=0 then DEVICE_ET=NR-60001/0. The prefix "NR-" is required for all values in this attribute.
- **<DeviceType DEVICE_TYPE="Cisco IPS"/>**—The DEVICE_TYPE attribute value indicates that all signatures originate from a Cisco IPS device. You must specify this value as Cisco IPS in the mapping file.
- **<EventTypeGroup>**—The value of this required element must be an existing MARS event type group. You can map MARS event types to more than one event type group.

Example Custom Signature Map Files

This example, 1.custom.inc.xml, maps the custom signature NR-60000/0 to the new MARS normalized event type ET-9000001. It is written for a MARS appliance running 5.3.1:

```
<?xml version="1.0" encoding="UTF-8"?>
<CS_MARS_EVENT_DATA_UPDATE xsi:schemaLocation="EventDataUpdate.xsd"
xmlns="http://www.cisco.com/2007/CS-MARS/EVENT-DATA-UPDATE"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <EventTypeList>
        <EventTypeListElement>
            <EventType EVENT_TYPE="ET-9000001">
                <EVENT_PRIORITY>LOW</EVENT_PRIORITY>
                <EVENT_TYPE_NAME>Custom Event 9000001</EVENT_TYPE_NAME>
                <LONG_DESCRIPTION>This is custom event</LONG_DESCRIPTION>
                <CVE_NAME>String</CVE_NAME>
                <AffectedPlatforms>
```

```
                    <OSInfo>
                        <Vendor>String</Vendor>
                        <Model>String</Model>
                        <Version>String</Version>
                        <Patch>String</Patch>
                    </OSInfo>
                    <ApplicationInfo>
                        <Program>String</Program>
                        <ProgramVersion>String</ProgramVersion>
                        <Application>
                            <Vendor>String</Vendor>
                            <Model>String</Model>
                            <Version>String</Version>
                            <Patch>String</Patch>
                        </Application>
                    </ApplicationInfo>
                </AffectedPlatforms>
                <VULNTY_FLAG>0</VULNTY_FLAG>
                <DENY_FLAG>0</DENY_FLAG>
                <INFO_LINKS>http://cve.mitre.org</INFO_LINKS>
                <FP_CONDITION>None</FP_CONDITION>
                <RECOM_ACTION>None</RECOM_ACTION>
            </EventType>
            <EventTypeGroup ET_GROUP_NAME="Penetrate/BufferOverflow/Web"/>
            <DeviceEventType DEVICE_ET="NR-60001/0">
                <DeviceType DEVICE_TYPE="Cisco IPS"/>
                <LINKS>http://www.mycompany.com</LINKS>
            </DeviceEventType>
        </EventTypeListElement>
    </EventTypeList>
    <Version>001</Version>
</CS_MARS_EVENT_DATA_UPDATE>
```

To remap this signature, NR-60000/0, to a different MARS event type, create a new xml file named 2.custom.inx.xml and change the <EventType> attribute to a different MARS event type, such as ET-3002071 (a system MARS normalized event type).

If the MARS normalized event type is the new user-created normalized event type, you can modify the information of the event type. This example, 3.custom.inc.xml, sets the priority to HIGH and it is written for a MARS appliance running 4.3.1:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<CS_MARS_EVENT_DATA_UPDATE xsi:schemaLocation="EventDataUpdate.xsd"
xmlns="http://www.cisco.com/2007/CS-MARS/EVENT-DATA-UPDATE"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <EventTypeList>
        <EventTypeListElement>
            <EventType EVENT_TYPE="ET-9000001">
                <EVENT_PRIORITY>HIGH</EVENT_PRIORITY>
                <EVENT_TYPE_NAME>Custom Event 9000001</EVENT_TYPE_NAME>
                <LONG_DESCRIPTION>This is custom event</LONG_DESCRIPTION>
                <CVE_NAME>String</CVE_NAME>
                <AffectedPlatforms>
                    <OSInfo>
                        <Vendor>String</Vendor>
                        <Model>String</Model>
                        <Version>String</Version>
                        <Patch>String</Patch>
                    </OSInfo>
                    <ApplicationInfo>
                        <Program>String</Program>
                        <ProgramVersion>String</ProgramVersion>
```

```
                    <Application>
                        <Vendor>String</Vendor>
                        <Model>String</Model>
                        <Version>String</Version>
                        <Patch>String</Patch>
                    </Application>
                </ApplicationInfo>
            </AffectedPlatforms>
            <VULNTY_FLAG>0</VULNTY_FLAG>
            <DENY_FLAG>0</DENY_FLAG>
            <INFO_LINKS>http://cve.mitre.org</INFO_LINKS>
            <FP_CONDITION>None</FP_CONDITION>
            <RECOM_ACTION>None</RECOM_ACTION>
        </EventType>
        <EventTypeGroup ET_GROUP_NAME="Penetrate/BufferOverflow/Web"/>
        <DeviceEventType DEVICE_ET="NR-60001/0">
            <DeviceType DEVICE_TYPE="Cisco IPS"/>
            <LINKS>http://www.mycompany.com</LINKS>
        </DeviceEventType>
    </EventTypeListElement>
</EventTypeList>
<Version>001</Version>
</CS_MARS_EVENT_DATA_UPDATE>
```

Import Custom Signature Maps into MARS

Once you've defined a custom signature map, you can import that map into the Local Controller. This operation allows MARS to begin processing events about your custom signature and allow you to include such events in event type groups and inspection rules.

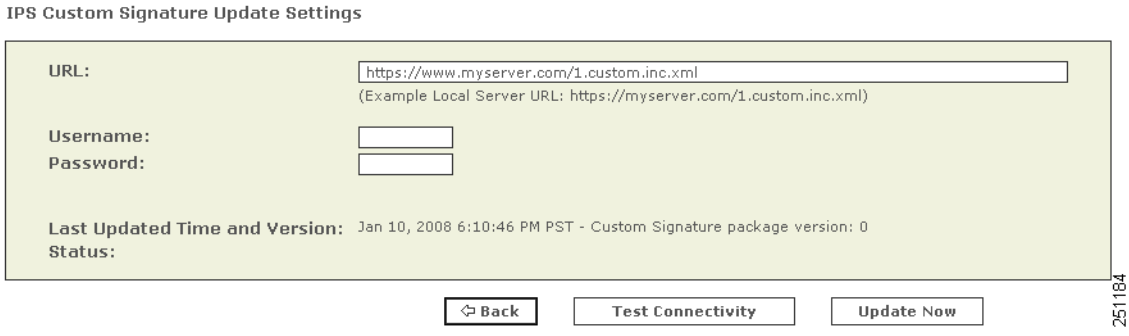
Before You Begin

The following requirements must be satisfied before attempting this procedure:

- An xml file that defines the custom signature mappings and that adheres to the guidelines specified in File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File, page 4-8.
- A http server that hosts the xml file to be uploaded into the Local Controller.

To import a custom signature map file into MARS, follow these steps:

Step 1 To import a customer signature map file, click **Admin > System Setup > IPS Custom Signature Update** in the web interface of the Local Controller.



Step 2 Enter the local server and the xml filename in the URL field.

This server identifies the HTTP server from which MARS can download the custom XML file. For example, `https://www.myserver.com/1.custom.inc.xml`.

Step 3 If required by the local server, enter the Username/password required for the Local Controller to authenticate to that server.

Step 4 Click **Update Now** to start the on demand custom signature import.

Step 5 Click **Activate** to enable the custom signatures on the Local Controller.

CHAPTER 5

Enterasys Dragon 6.x

To configure the Enterasys Dragon devices, you must:

- Configure the Dragon Policy Manager (DPM) or Event Flow Processor (EFP).
- Configure the syslog daemon running on the same system as the DPM or EFP.
- Configure the MARS.

This chapter contains the following topics:

- DPM/EFP Configuration, page 5-1
- Host-side Configuration, page 5-2
- MARS-side Configuration, page 5-2

DPM/EFP Configuration

Before you configure the DPM or EFP, you must install and enable the Alarmtool.

This section contains the following topics:

- Configure the DPM or EFP, page 5-1

Configure the DPM or EFP

Step 1 Log into the DPM or EFP.

Step 2 Click **Alarmtool**.

Step 3 In the left menu, click **Notification Rules**.

Step 4 In the right window, select syslog if it exists. If not, you need to create it:

a. Click **New Notification Rules** and select **syslog**.

b. **Facility** - Make sure the localn you select is not in use by the syslog daemon

c. **Level** - Select Debug

d. **Message** - Make sure its in such format:

```
%TIME% %DATE% SigName=%NAME% from Sensor=%SENSOR%
ScrIP=%SIP% DstIP=%DIP% SrcPort=%SPORT% DstPort=%DPORT%
Protocol=%PROTO%
```

Step 5 Click **Save**.

Step 6 In the left menu, click **Alarm**.

Step 7 Set the **Type to Real-time** and the **Notification Rule to syslog**.

Step 8 Click **Save**.

Step 9 In the left menu, click **Deployment**.

Step 10 In the main screen, click **View Configuration**. Make sure the **localn** set in both notify syslog and alarm syslog match.

Step 11 In the main screen, click **Deploy and Reset** to confirm the configuration change.

Host-side Configuration

This section contains the following topics:

- Configure the syslog on the UNIX host, page 5-2

Configure the syslog on the UNIX host

Step 1 Log into the host as the root user.

Step 2 On the same system running the DPM or EFP, edit the file /etc/syslog.conf .

Step 3 Make sure n in localn matches the syslog entry you used on the DPM or EFP.

Step 4 Add the line:

```
localn.*          @<mars ip address>
```

Replacing *n* with the value used in Step 3 and replacing <*mars ip address* > with the IP address of the MARS Appliance.

Step 5 Restart the syslog daemon by entering:

```
/etc/rc.d/rc.syslog restart
```

MARS-side Configuration

This section contains the following topics:

- Add Configuration Information for the Enterasys Dragon, page 5-2
- Add a Dragon NIDS Device, page 5-3

Add Configuration Information for the Enterasys Dragon

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP Addresses if adding a new host.

Step 4 Click **Apply**

Step 5 Click **Reporting Applications** tab

Step 6 From the Select Application list, select **Enterasys Dragon 6.x**.

Step 7 Click **Add**.

Add a Dragon NIDS Device

Step 1 Click **Add Sensor**.

Step 2 Select existing device or **Add New Device**.

Step 3 Enter values for the following fields:

- **Device Name**—The DNS entry for this device.
- **Sensor Name**—The name as it appears in the console.
- **Reporting IP**—The IP address that the agent uses to send logs to the console.

Step 4 Add the interfaces, which important information for attack path calculation.

- For multiple interfaces, click **Add Interface**, and add the new interfaces's name, IP address and mask.

Step 5 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

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

Step 7 Click **Done** when you are done adding the sensor.

Step 8 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 6

Snort Devices

MARS can monitor Snort 2.x (2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, and 2.8) via the syslog messages generated by the devices. To enable MARS to monitor Snort devices, configure the Snort syslog plugin to publish messages to the MARS appliance, and then define the Snort device in the MARS web interface.

This chapter contains the following topics:

- MARS Expectations of the Snort Syslog Format, page 6-1
- Configure Snort to Send Syslogs to MARS, page 6-1
- Add the Snort Device to MARS, page 6-2

MARS Expectations of the Snort Syslog Format

The following example Snort syslog messages are used to illustrate the values that are parsed by the MARS Appliance:

```
<161>snort: [1:2050:1] MS-SQL version overflow attempt [Classification: Misc activity] [Priority: 3]: {UDP}
69.70.113.64:1449 -> 66.243.153.44:1434

<119>Jul 16 10:54:39 SourceFire SFIMS: [1:469:1] ICMP PING NMAP [Classification: Attempted Information Leak]
[Priority: 2] {ICMP} 210.22.215.77 -> 67.126.151.137

<161>Mar 12 18:02:22 snort: [ID 702911 local4.alert] [119:2:1] (http_inspect) DOUBLE DECODING ATTACK {TCP}
10.1.1.21:60312 -> 10.1.1.69:80
```

The MARS parser expects the pattern: “[<generator id>:<snort id>:<revision number>]" to identify the event as one originating from a Snort device. One that determination is made, MARS looks for either "{<protocol_string>} <ip>:<port> -> <ip>:<port>" or "{<protocol_string>} <ip> -> <ip>" to identify the five-tuple values.

Configure Snort to Send Syslogs to MARS

For Snort, use the syslog as your output plugin. Configure your syslogd to send copies to another host. On most older-style systems (Solaris/Linux), you need to edit ***/etc/syslog.conf***. (Assuming that the system is based on syslogd, and not any of the newer system logging facilities. The newer logging facilities are not supported by Snort.)

To configure Snort to send syslog messages to the MARS Appliance, follow these steps:

Step 1 Make Snort's output go to syslog with log facility local4 in snort.conf (you can pick any local facility that's unused.)

```
output alert_syslog: LOG_LOCAL4 LOG_ALERT
```

snort.conf is normally in /etc/snort.

Step 2 Add a redirector in your /etc/syslog.conf on your Snort box to send syslog to MARS.

```
local4.alert @IPAddrOffMarsbox
```

Step 3 Restart the Snort daemon and the syslogd daemon on your Snort box.

Add the Snort Device to MARS

To add the Snort device to MARS, follow these steps:

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**

Step 5 Click **Reporting Applications** tab.

Step 6 From the Select Application list, select **Snort Snort 2.0**.

Currently, the Snort Snort 2.0 option applies to the following versions: 2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, and 2.8

Step 7 Click **Add**

Step 8 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

Step 9 To save your changes, click **Submit**.

Step 10 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 7

McAfee IntruShield

To configure McAfee IntruShield (formerly known as IntruVert IntruShield) in MARS, you must perform the following tasks:

1. Generate CSV file that identifies each of the IntruShield senor hosts by logging into the database to which IntruShield Manager writes and performing and saving a database query.
2. Configure the IntruShield Manager to send SNMP traps to the MARS Appliance
3. Define a host that represents the management console (McAfee IntruShield Security Manger) in MARS web interface.

Note Beginning in 6.x, MARS discovers the IntruShield sensors from the IntruShield Security Manager SNMP traps. Therefore, you are not required to define the network sensors manually or via a seedfile.

4. (Optional) From that host in the MARS web interface, import the IntruShield network sensor seed file to identify the IntruShield sensors running on other hosts.

This chapter contains the following topics:

- Configure McAfee IntruShield 4.1 to Send SNMP Traps to MARS, page 7-1
- Add the IntruShield Manager Host to MARS, page 7-2
- Add IntruShield Sensors in MARS using Seed Files, page 7-4

Configure McAfee IntruShield 4.1 to Send SNMP Traps to MARS

Using the IntruShield Security Manager interface, you can identify the MARS appliance as a target for SNMP traps and specify what types of event data to forward to MARS.

To configure IntruShield to forward SNMP traps to MARS, follow these steps:

Step 1 Log in to the IntruShield Security Manager 4.1.

Step 2 Click **Configure**.

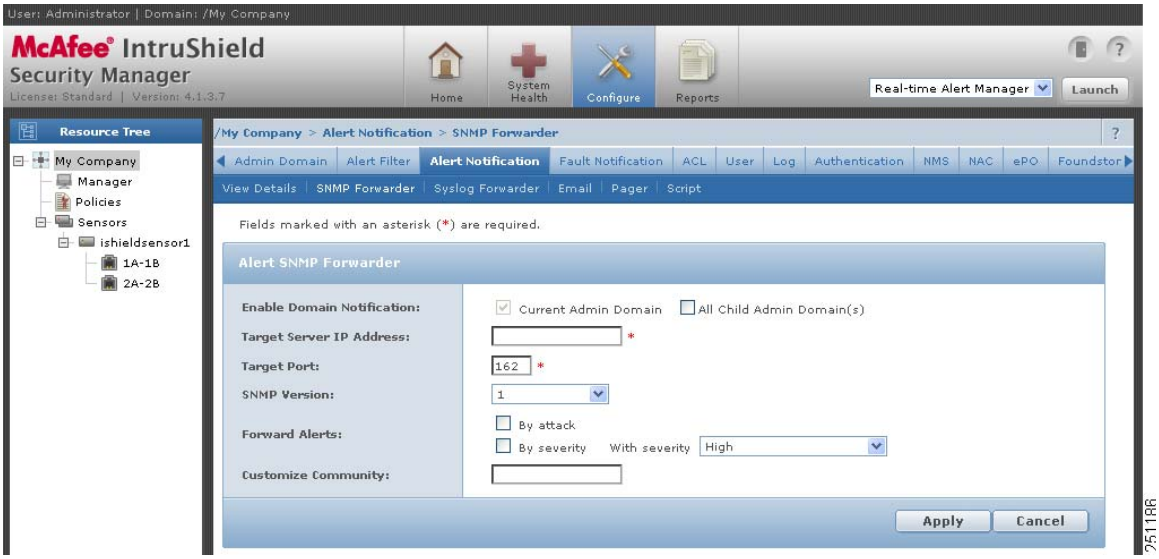
Step 3 In the Resource Tree, click **My Company**.

Step 4 Click the **Alert Notification** tab, and then click the **SNMP Forwarder** sub-tab..

Step 5 Verify the **Yes** option is selected for Enable SNMP Forwarder.

Step 6 To define an new SNMP target, click **Add**.

The Alert SNMP Forwarder page appears.



Step 7 Specify values for the following fields:

- **Enable Domain Notification**—Verify that both the Current Admin Domain and All Child Admin Domain(s) check boxes are selected.
- **Target Server IP Address**—Specify the IP address of the target Local Controller as it appears to IntruShield.
- **Target Port**—Enter ***162*** to identify the SNMP port on which the Local Controller listens for SNMP messages.
- **SNMP Version**—Select **1**. This value identifies the version of SNMP running on the target Local Controller.
- **Forward Alerts**—Verify that both the By attack and By severity check boxes are selected. Continue defining the severity level as follows:
  - **With severity**—Select the **Informational and above** option.
- **Customize Community**—Specify the SNMP community string that allows MARS to access your protected IntruShield data.

Step 8 Click **Apply** and exit the program.

Add the IntruShield Manager Host to MARS

To define the host and represent the management console for IntruShield, follow these steps:

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click **Reporting Applications** tab.

Step 6 Select **McAfee IntruShield 4.1** from the Select Application list.

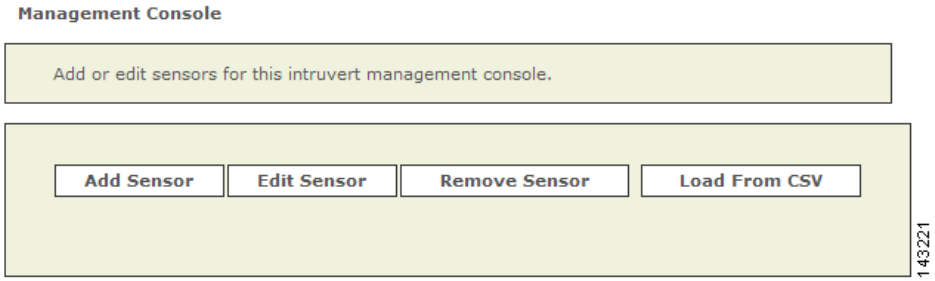
Step 7 To complete the definition of this console, click **Add**.

Note MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps.

Step 8 (Optional) To manually define sensors that the console manages, you can use on of two methods:

- Add IntruShield Sensors Manually, page 7-3
- Add IntruShield Sensors in MARS using Seed Files, page 7-4

Figure 7-1 Add IntruShield Sensors



Step 9 To save your changes, click **Submit**.

Step 10 To enable MARS to start sessionizing events from this application, click **Activate**.

Add IntruShield Sensors Manually

While MARS discovers IntruShield sensors over time, you may want to know if an undiscovered device is not reporting via the standard device not reporting messages that MARS issues. To ensure that this functionality is operational, you may chose to add a sensor manually.

Note MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps; therefore, this procedure is not required.

To add sensors manually, follow these steps:

Step 1 Click **Add Sensor**.

Step 2 Specify the following values:

- **Device Name**—The DNS entry for this device.
- **Sensor Name**—The name as it appears in the console.
- **Reporting IP**—The IP address that the agent uses to send logs to the console.

Step 3 Add the interface information.

Step 4 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

Step 5 To save your changes, click **Submit**.

Step 6 To enable MARS to start sessionizing events from this module, click **Activate**.

Add IntruShield Sensors in MARS using Seed Files

Adding an IntruShield sensors manually using a seed file has two distinct steps. First, extract sensor information from the IntruShield Security Manager host. Second, import that seedfile into the MARS web interface.

This section contains the following topics:

- Extracting IntruShield Network Sensor Information from the IntruShield Security Manager, page 7-4
- Add IntruShield Sensors Using a Seed File, page 7-5

Extracting IntruShield Network Sensor Information from the IntruShield Security Manager

IntruShield sensor information is saved in a database on the IntruShield Security Manager host. When you configure the MARS to add IntruShield sensors, you can manually add the mapping of each IntruShield sensor name or you can extract them as a seed file from the database on the IntruShield Manager.

Note MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps; therefore, this procedure is not required.

Note The instructions apply for McAfee IntruShield version 1.5. IntruShield supports both MySQL and Oracle.

To create a CSV file for McAfee IntruShield, follow these steps:

Step 1 Log in to the database.

Step 2 Perform the query:

```
use lf; select name, ip_address from iv_sensor where ip_address is not NULL;
```

Step 3 Store the query result into a file, remove the header, trailer, and separator lines, and edit the result to a CSV format.

For example, the query result could be:

```
+------------+------------+
| name       | ip_address |
+------------+------------+
| intruvert  | 0A010134   |
| intruvert1 | 0A010135   |
+------------+------------+
2 row in set (0.00 sec)
```

You would then edit the above file to appear as:

```
intruvert,0A010134
intruvert1,0A010135
```

Step 4 Save the edited CSV file, move the file to an FTP server from which you can load the seed file using the MARS web interface.

Add IntruShield Sensors Using a Seed File

To add sensors using a seed file, follow these steps:

Step 1 Click **Load From CSV**.

Step 2 Enter the FTP server information and location of the CSV (comma separated values) file.

- If you need to generate the IntruShield sensors CSV file, Extracting IntruShield Network Sensor Information from the IntruShield Security Manager, page 7-4.

Step 3 Click **Submit**.

The list of sensors appears on the management console page.

Step 4 For each sensor that appears in the management console page, select the check box next to the sensor and click Edit Sensor.

Step 5 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.

- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

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

Step 7 To save the changes made to this management console and the sensors it manages, click **Submit**.

Step 8 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 8

Symantec ManHunt

This chapter contains the following topics:

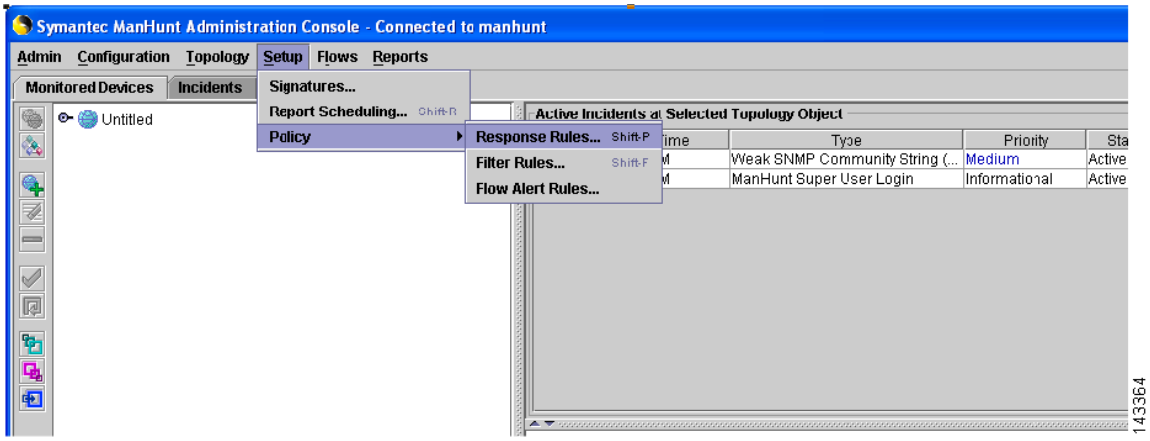
- Symantec ManHunt Side Configuration, page 8-1
- MARS Side Configuration, page 8-2

Symantec ManHunt Side Configuration

Step 1 Login to the Symantec ManHunt with appropriate username and password.

Step 2 In the main screen, click **Setup > Policy > Response Rules**, then Response Rules window will appear.

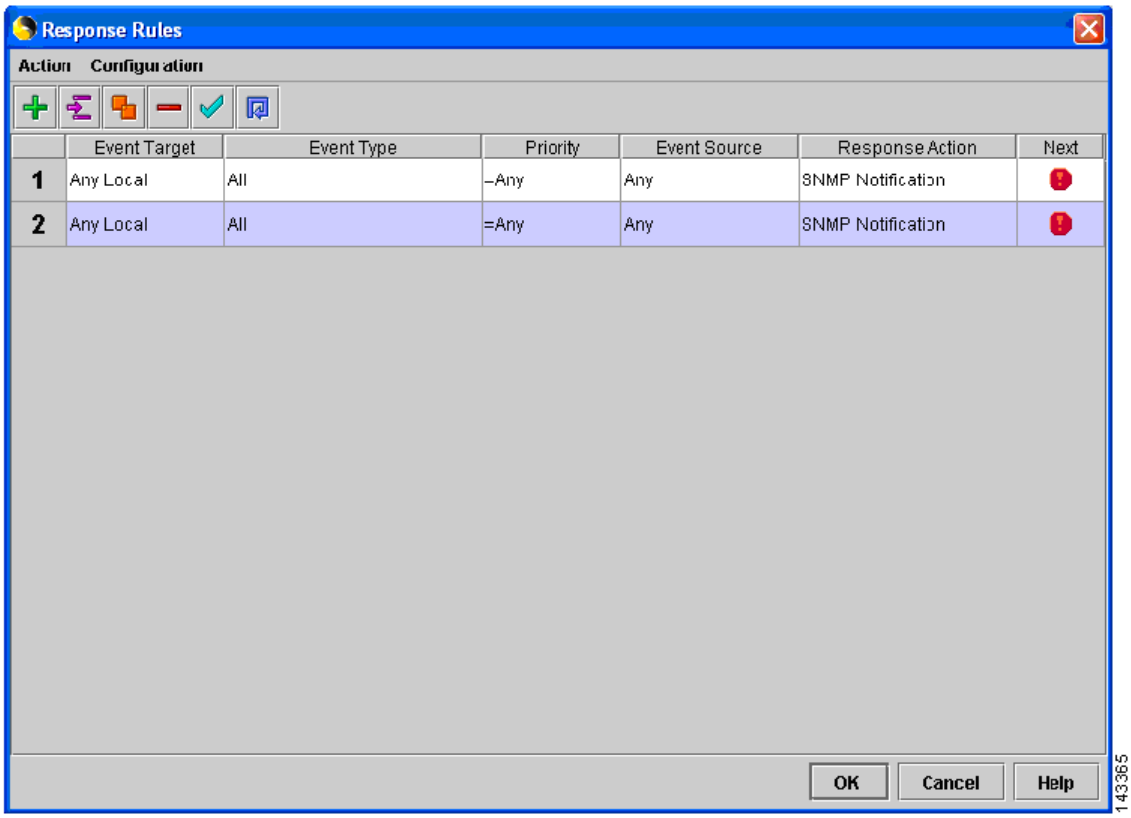
Figure 8-1 ManHunt Configuration



Step 3 In the Response Rules window, click **Action > Add Response Rules**.

Step 4 Click in the field of Response Action

Figure 8-2 ManHunt Response Rule Config



Step 5 In the left menu, click **SNMP Notification** and enter the following information:

- **SNMP Manager IP address**—Reporting IP address of MARS
- **Maximum number of SNMP notification**—(Example: 100000).
- **Delay between SNMP notification (mins)**—(Example: 1 min)

Step 6 Click **OK** to return to main screen.

MARS Side Configuration

This section contains the following topics:

- Add Configuration Information for Symantec ManHunt 3.x, page 8-2

Add Configuration Information for Symantec ManHunt 3.x

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**

Step 5 Click **Reporting Applications** tab

Step 6 From the Select Application list, select **Symantec ManHunt 3.x**

Step 7 Click **Add**.

Step 8 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

Step 9 To save your changes, click **Submit**.

Step 10 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 9

Cisco IPS Modules

MARS can monitor Cisco IPS modules installed in Cisco switches and Cisco ASA appliances. To prepare these modules, you must perform the following tasks:

- Define the base module, either the router, switch, or Cisco ASA, as defined in Chapter 17, "Cisco Routers", Chapter 15, "Cisco Switch Devices", and Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1.
- Bootstrap the base module to enable SDEE traffic on the Cisco IPS module, to forward events to the MARS Appliance, and to enable MARS to access the SDEE events stored on the modules. Module access enables MARS to retrieve trigger packets and IP log information.
- Add the IPS feature set t the base module previously defined in the web interface.

The following topic also supports the configuration of the Cisco IPS modules:

- Verify that MARS Pulls Events from a Cisco IPS Device, page 4-6

This chapter contains the following topics:

- Enable SDEE on the Cisco IOS Device with an IPS Module, page 9-1
- Add an IPS Module to a Cisco Switch or Cisco ASA, page 9-2

Enable SDEE on the Cisco IOS Device with an IPS Module

In addition to enabling either Telnet or SSH for configuration discovery on a Cisco IOS device, you must also enable SDEE on the device that supports IPS module. SDEE is used to publish events to MARS about signatures that have fired.

To enable SDEE protocol on the Cisco IOS device that supports IPS module, perform the following steps:

Step 1 Log in to the Cisco IOS device using the enable password.

Step 2 Enter the following commands to enable MARS to retrieve the events from the IPS module:

```
Router(config)#ip http secure-server
Router(config)#ip ips notify sdee
Router(config)#ip sdee subscriptions 3
Router(config)#ip sdee events 1000
Router(config)#no ip ips notify log
```

Note The “no ips notify log” causes the IPS modules to stop sending IPS events over syslog.

Add an IPS Module to a Cisco Switch or Cisco ASA

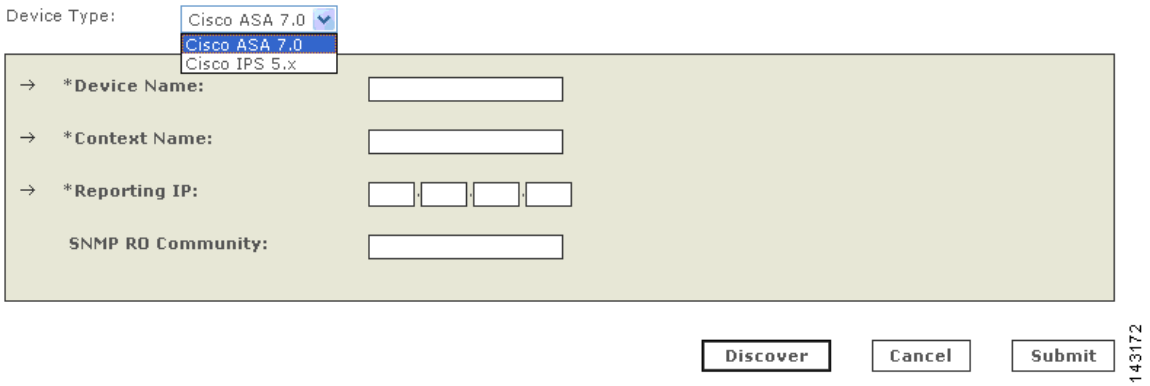
You can enable in-line IPS functionality and signature detection in multi-purpose Cisco platforms. You can identify an IDS-M2 running in a Cisco Switch or an ASA-SSM running in a Cisco ASA. To represent either of these modules, you must define the settings for the module as part of the base platform, which must be previously defined under Admin > System Setup > Security and Monitor Devices.

To add an IPS module to a Cisco Switch of Cisco ASA, follow these steps:

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

Step 2 From the list of devices, select the Cisco switch or Cisco ASA to which you want to add the IPS module and click **Edit**.

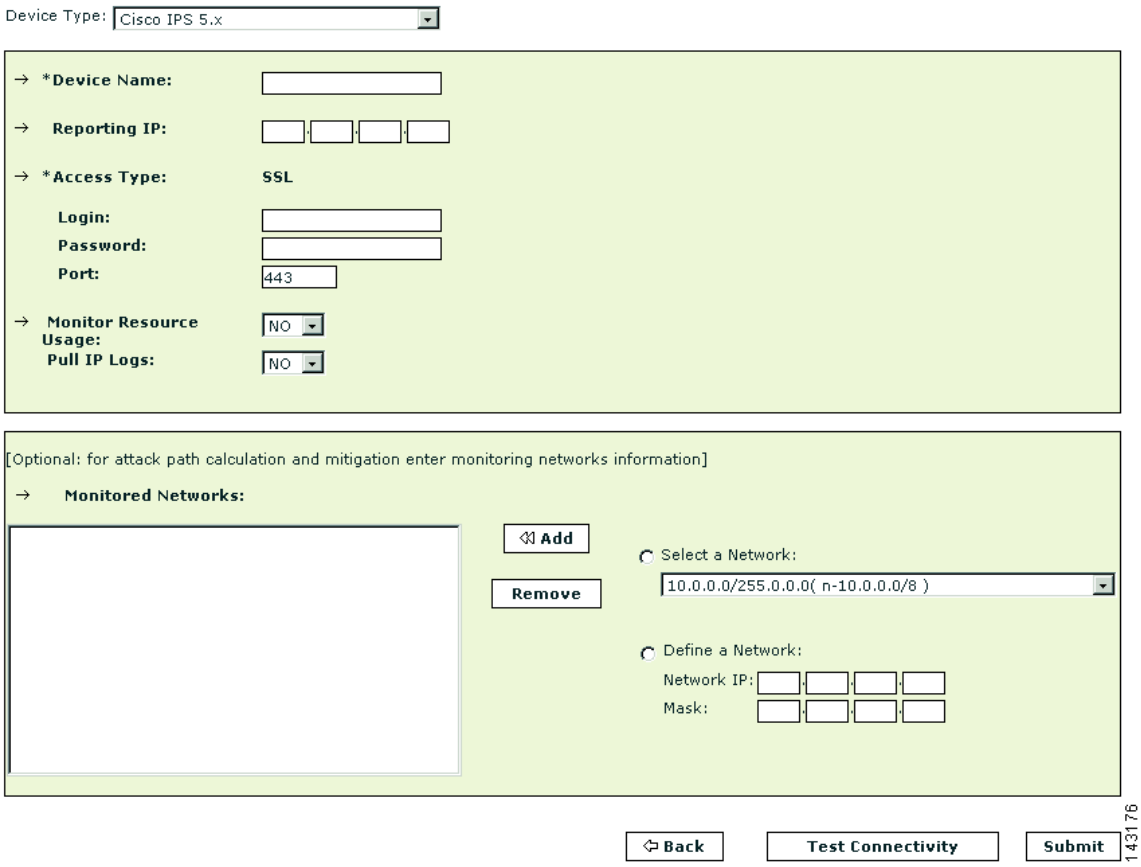
Step 3 Click **Add Module**.



Step 4 Select **Cisco IPS 5.x**or **Cisco IPS 6.x** in the Device Type list.

For Cisco switches, you can also add a Cisco IPS 4.0 module. You configure these modules just as you would a standalone sensor. For instructions on configuring these modules, refer Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1.

Figure 9-1 Configure Cisco IPS 5.x or 6.x



Step 5 Enter the hostname of the sensor in the Device Name field.

Step 6 Enter the administrative IP address in the Reporting IP field.

Step 7 The Reporting IP address is the same address as the administrative IP address.

Step 8 In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.

Step 9 In the Password field, enter the password associated with the username specified in the Login field.

Step 10 In the Port field, enter the TCP port on which the webserver running on the sensor listens.

The default HTTPS port is 443.

Note While it is possible to configure HTTP only, MARS requires HTTPS.

Step 11 (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.

a. Enter the network address in the Network IP field.

b. Enter the corresponding network mask value in the Mask field.

c. Click **Add** to move the specified network into the Monitored Networks field.

d. Repeat as needed.

Step 12 (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.

a. Select a network from in the Select a Network list.

b. Click **Add** to move the specified network into the Monitored Networks field.

c. Repeat as needed.

Step 13 Click **Test Connectivity** to verify the configuration.

Step 14 To save your changes, click **Submit**.

Step 15 To enable MARS to start sessionizing events from this module, click **Activate**.

CHAPTER 10

IBM Proventia Management/ISS SiteProtector 2.0

This chapter contains the following topics:

- IBM Proventia Management/ISS SiteProtector to Define Global Event Policies, page 10-1
- IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device, page 10-5

IBM Proventia Management/ISS SiteProtector to Define Global Event Policies

To define SiteProtector as a reporting device, see IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device, page 10-5.

Note This topic describes how to use Site Protector to configure the ISS NIDS and HIDS; Site Protector is not a device type that can be monitored or used as an aggregation point for ISS event data from the perspective of MARS. Prior to 4.3.1 and 5.3.1, MARS could not parse event data from Site Protector, unless you developed a custom event parser for each event type.

MARS supports ISS NIDS and HIDS event retrieval via SNMP. However, when configuring ISS RealSecure sensors (NIDS) and hosts (HIDS), you must configure each active signature to send an alert to the MARS Appliance. This task can be very tedious as it must be done for each sensor and after each signature upgrade, as it resets the redirect configuration. One approach to simplifying this task is to use the SiteProtector management console to define these changes globally and apply them to each sensor.

SiteProtector 2.0 allows you to centrally manage SNMP alert destinations, such as the MARS Appliance, for group policies. You can then push these group policies to all desired host and network sensors. For each ISS signature update, you must specify the MARS Appliance as an SNMP alert destination before you apply the downloaded signatures to sensors using Site Protector.

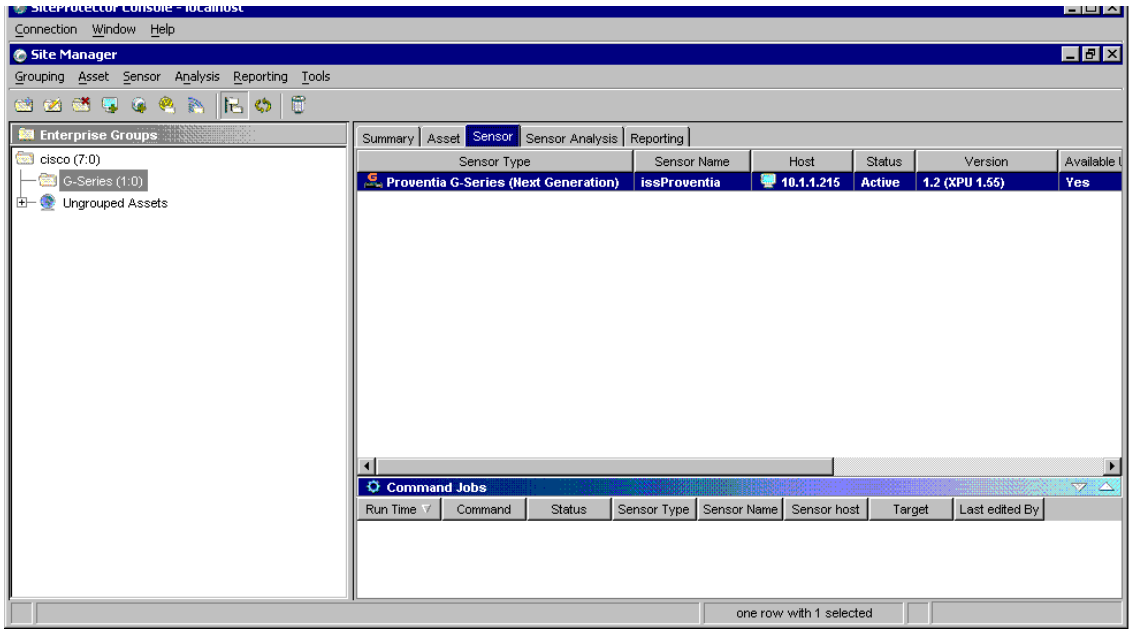
Note By default, the group policy response configuration is supported only on Proventia G400 and G2000 models. For all other models, including the G100 mentioned, a firmware upgrade is required. See the documentation that came with SiteProtector for more information.

To perform the major configuration steps required to use Site Protector to forward the SNMP alerts generated by sensors to MARS Appliance, follow these steps:

Step 1 Using the Add Sensor Wizard, register the sensor to Site Protector Console.

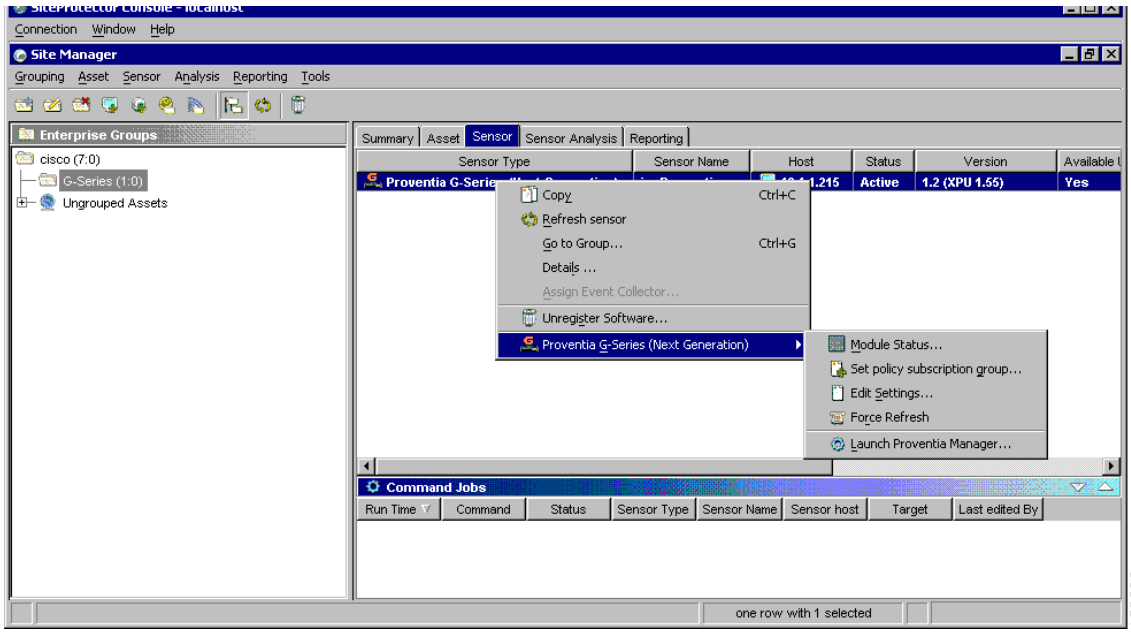
Other methods exist for registering sensors in Site Protector. For more information on using the Wizard as well as these other methods, see *Chapter 9, Registering Software Managed by SiteProtector,* on page 105 at the following URL:

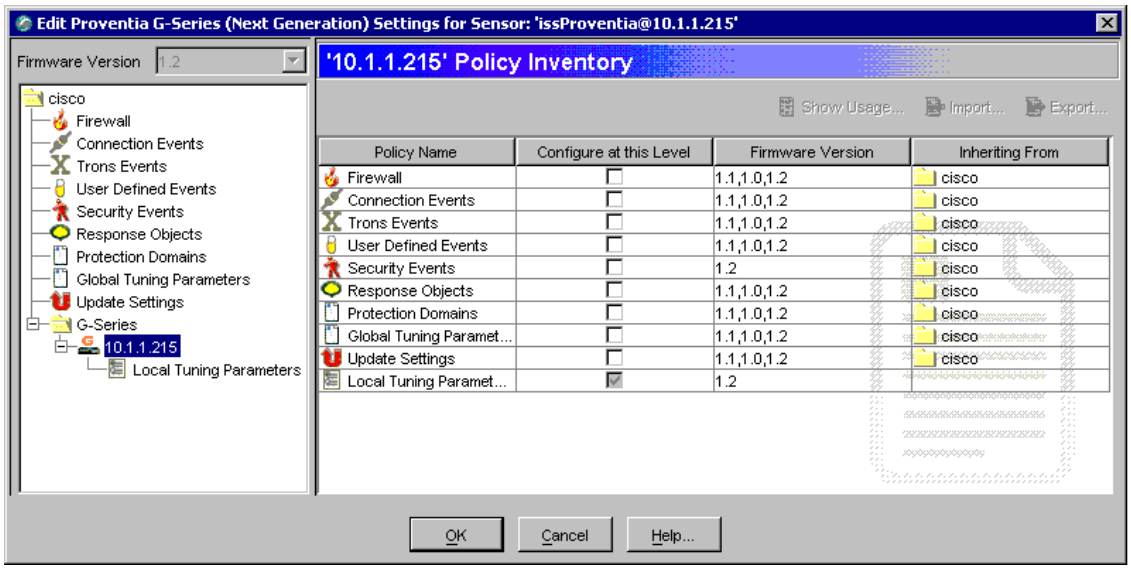
http://documents.iss.net/literature/SiteProtector/SPUserGuideforSecurityManagers20SP52.pdf



Step 2 Right-click the sensor to edit, and click **Edit Settings** on the shortcut menu.

The Edit Settings dialog appears.



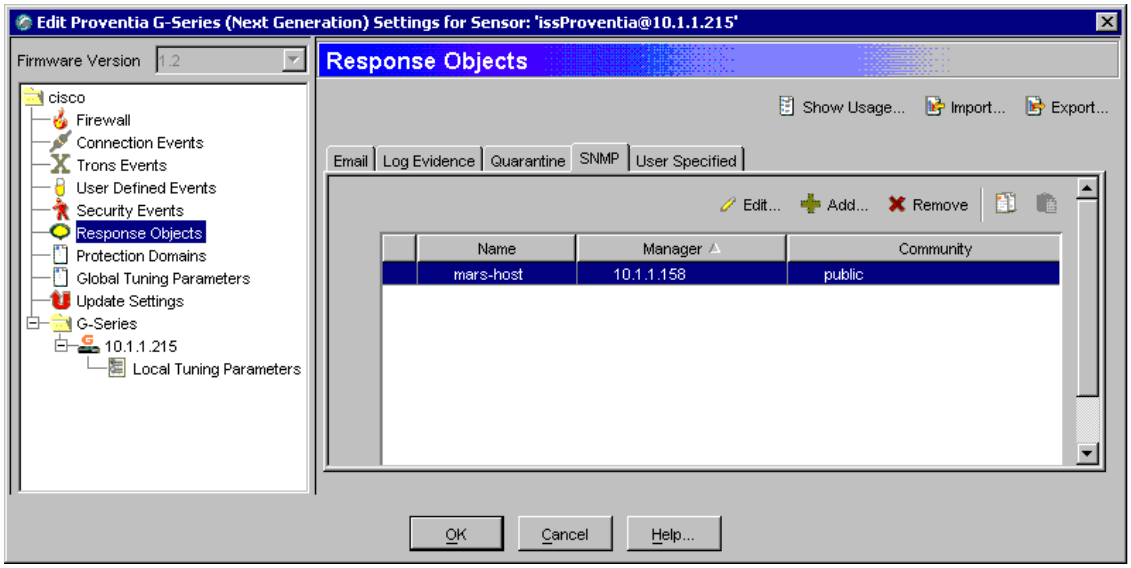


Step 3 Create a new SNMP response that sends messages to the IP address of the MARS Appliance:

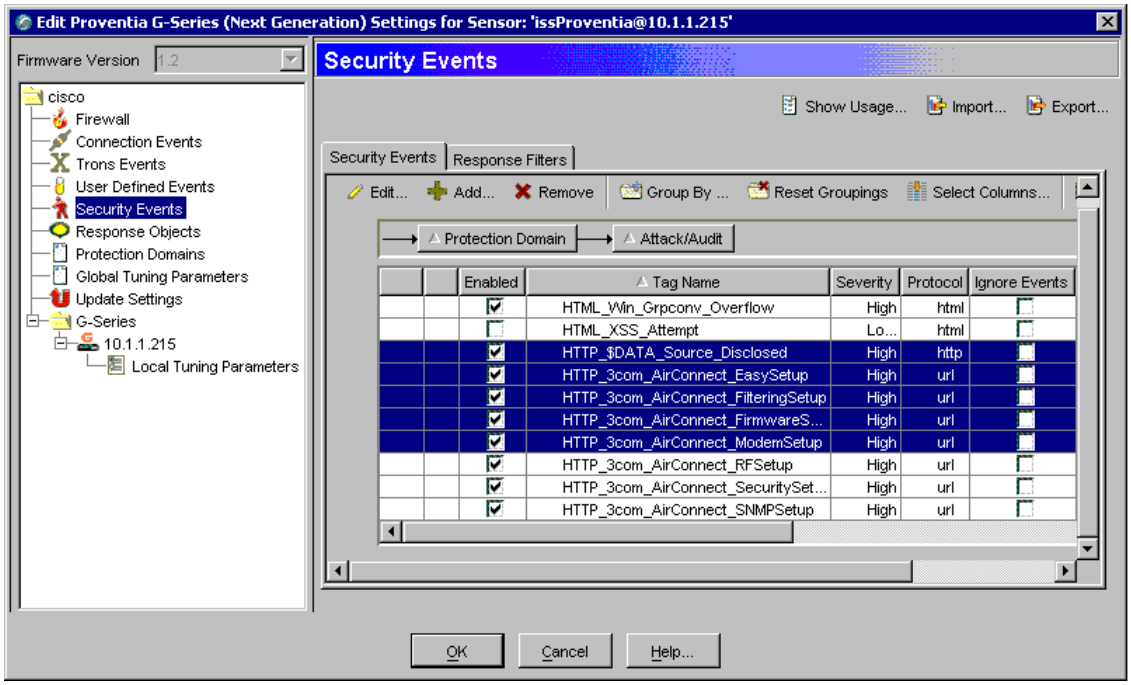
a. Select **Response Objects** from the settings tree.

b. Select the **SNMP** tab.

c. Click **Add** to create a new SNMP response object using the IP address of the MARS Appliance.



Step 4 Select the Security Events to configure new SNMP destination.



a. Select **Security Events** under the sensor folder.

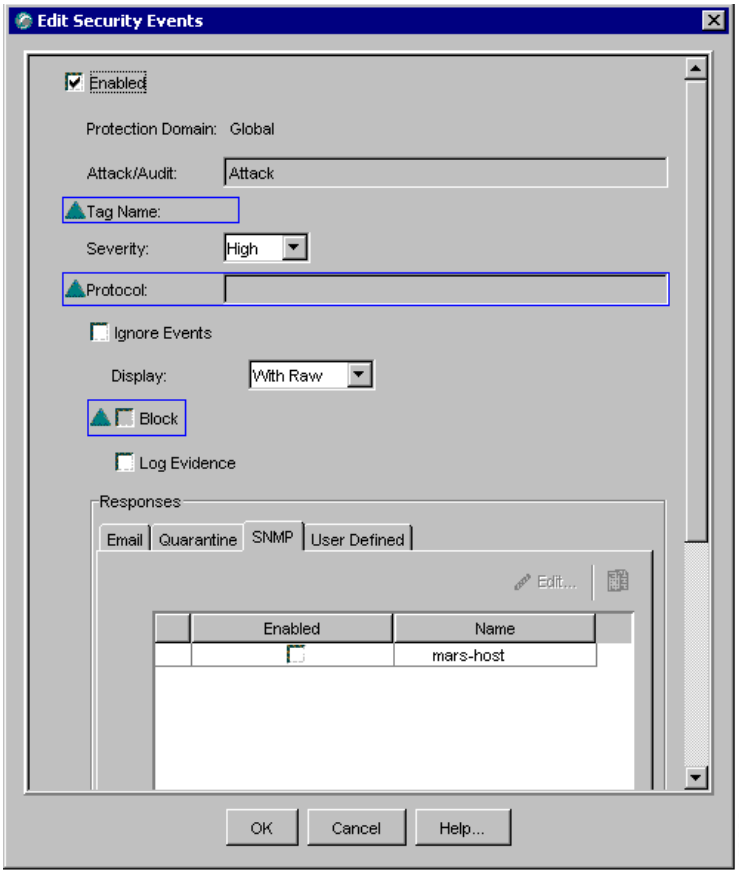
b. Select the required security events from the Security Events tab.

The Group By button allows you to group policies using any number of parameters.

Note You can also select policies and edit them at the group level.

c. Click **Edit** to configure SNMP response of all the selected policies.

Step 5 Select the MARS Appliance on SNMP tab.



a. Enable all the security events by selecting the **Enabled** checkbox located at the top of the Edit Security Events dialog box.

b. Select the **SNMP** tab under Responses, and then select the **Enabled** checkbox next to the name of MARS Appliance created in Step 3.

c. Click **OK**.

The security events and updated response target are applied to the selected sensor during the next synchronization.

IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device

MARS supports ISS NIDS and HIDS event retrieval via SNMP. However, when configuring ISS RealSecure sensors (NIDS) and hosts (HIDS), you must configure each active signature to send an alert to the MARS Appliance. This task can be very tedious as it must be done for each sensor and after each signature upgrade, as it resets the redirect configuration. Two approaches that simplify this task exist:

- **Use the SiteProtector management console to define these changes globally and apply them to each sensor.** In this case, MARS parses SNMP event data from the managed ISS NIDS and HIDS devices.

  SiteProtector 2.0 allows you to centrally manage SNMP alert destinations, such as the MARS Appliance, for group policies. You can then push these group policies to all desired host and network sensors. For each ISS signature update, you must specify the MARS Appliance as an SNMP alert destination before you apply the downloaded signatures to sensors using Site Protector.

  By default, the group policy response configuration is supported only on Proventia G400 and G2000 models. For all other models, including the G100 mentioned, a firmware upgrade is required. See the documentation that came with SiteProtector for more information.

- **Define Site Protector as a reporting device**. It acts as an aggregation point for ISS NIDS and HIDS event data . In this case, MARS parses SNMP event data from Site Protector.

This topic describes how to configure and define Site Protector as a reporting device. To enable SiteProtector as a reporting device in MARS, define the SiteProtector console as the reporting device. The SiteProtector receives alerts from the ISS agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the ISS agent that originally triggered the event, rather than the SiteProtector that forwarded it. Therefore, MARS requires host definitions for each of the ISS agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the SiteProtector console.

MARS discovers ISS agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the ISS agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the SiteProtector as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the SiteProtector; however, you are not required to define each agent. The default topology presentation for discovered ISS agents is within a cloud.

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

This section contains the following topics:

- Configure SiteProtector to Forward SNMP Notifications to MARS, page 10-6
- Add and Configure a SiteProtector Device in MARS, page 10-10

Configure SiteProtector to Forward SNMP Notifications to MARS

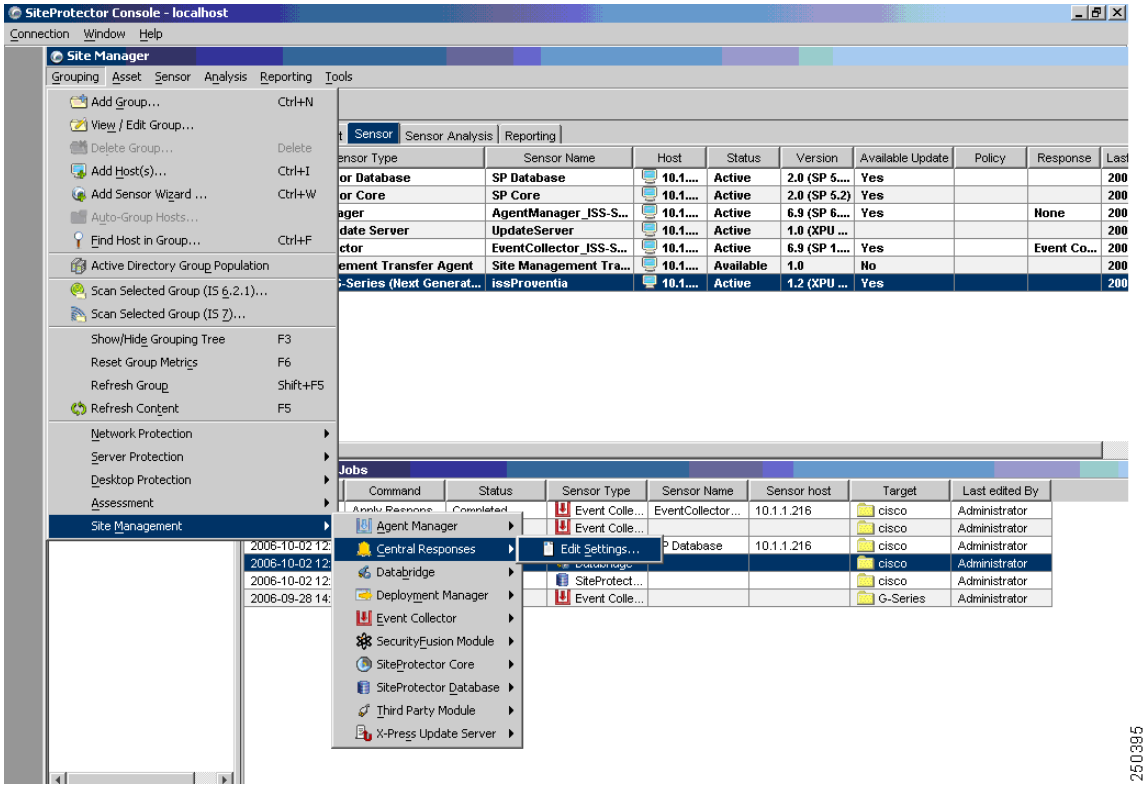
The only required configuration is to ensure that SiteProtector forwards the SNMP notifications that it receives from agents to MARS. From these notifications, MARS is able to discover the agent and its relevant settings. It is also from these events that MARS learns about the host-level activities transpiring on your network.

To forward all notifications to the MARS Appliance, follow these steps:

Step 1 Log in to the Site Protector console.

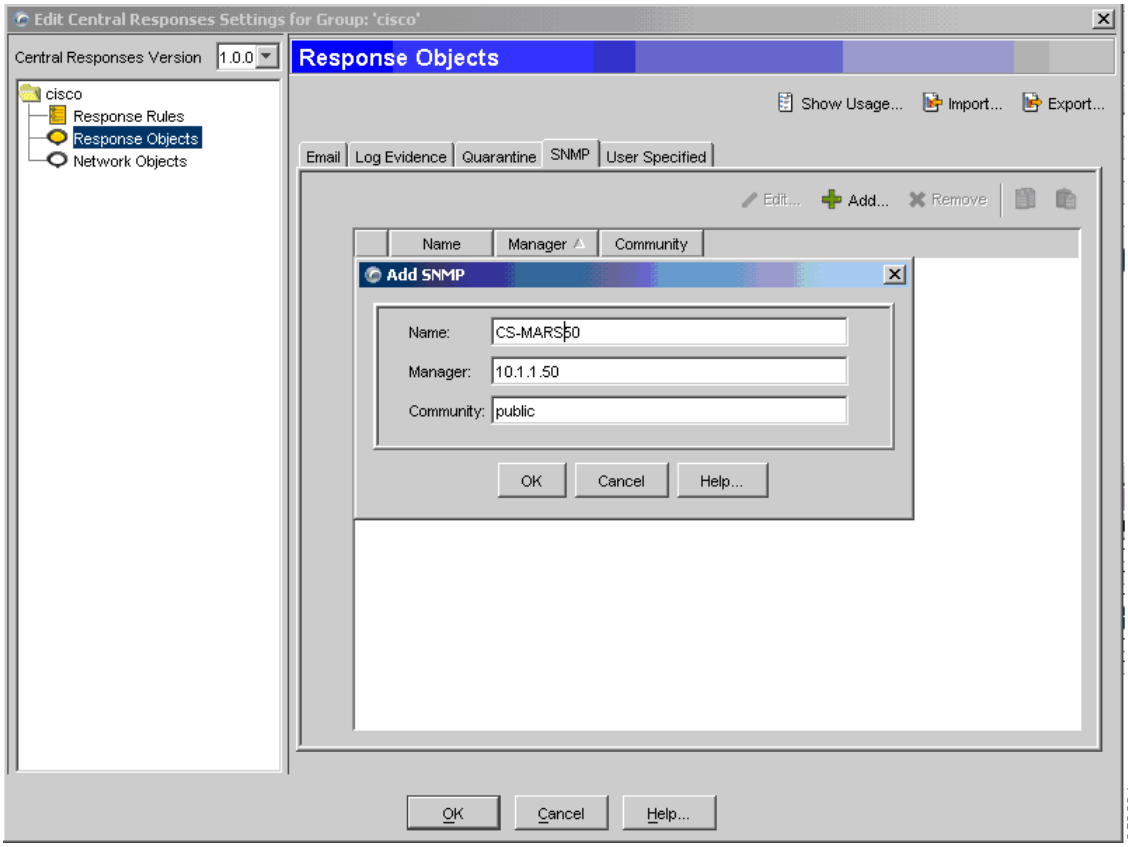
Step 2 Click **Grouping > Site Management > Central Responses > Edit settings**.

The Edit Central response Settings Window appears.



Step 3 Click **Response Objects > SNMP > Add** to add a new response object that represents the MARS Appliance to which events should be forwarded.

The Add SNMP dialog box appears.



Step 4 Enter values for the following fields that correspond to the MARS Appliance:

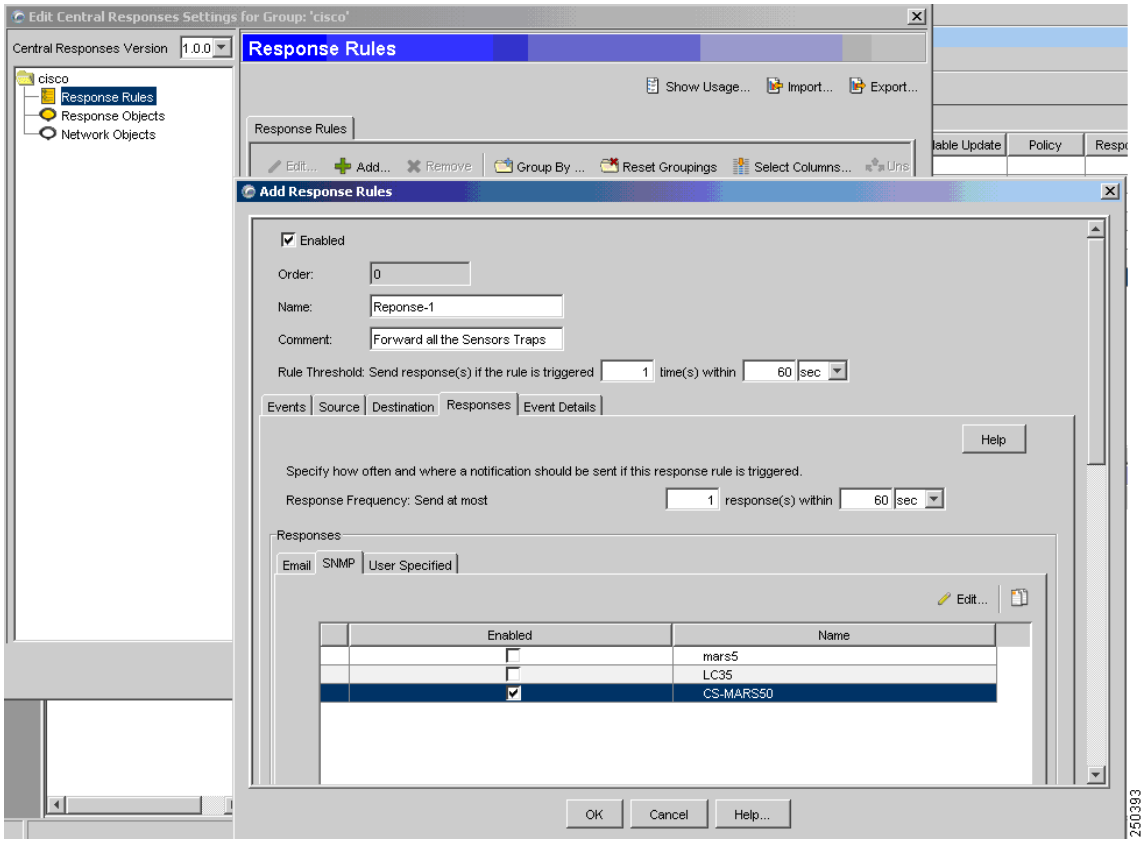
- **Name**—(hostname)
- **Manager**—(IP address)
- **Community**—(public)

Step 5 Click **OK.**

The MARS Appliance appears as a response object. You can now define response rules forward SNMP traps to this object. The default SNMP port is 612. One ore more response object is associated with each response rule. Therefore, the response object is not used until it is associated with an enabled response rule.

Step 6 To add a response rule, click **Response Rules > Add**.

The Add Response Rules dialog box appears.



Step 7 Specify the following value:

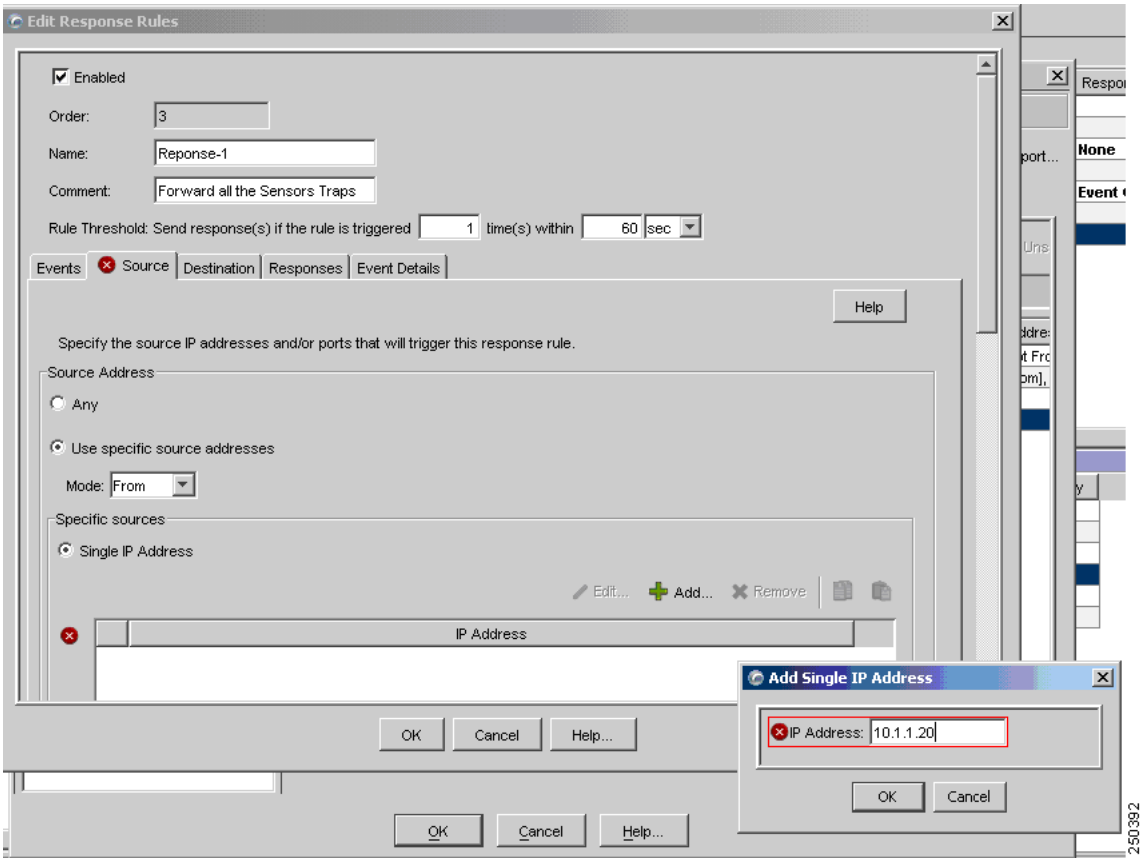
- **Enable**—When selected, it enables the response rule.
- **Name**—Identifies the name of the response rule.
- **Comments**—Provides a description of the response rule.

Step 8 Click the SNMP tab, and under the Enabled column, select the checkbox next to the response object defined inStep 4.

Note Multiple response objects can be enabled for each response rule.

Step 9 Click on **OK** to save the rule, enable it, and enable the response object that represents the MARS Appliance.

Step 10 (Optional) (Optional) By default, a rule matches on any source or destination IP addresses. To refine the rule to match on a specific source IP address, modify the rule, and then select the Source tab.



Specify the following values:

- **Use specific source addresses**—Select this option to restrict the rule based on IP address of the source.
- **Mode**—Specify that the rule should either be From or Not From the IP address.
- **Click Add**—Define one or more IP addresses to clarify the rule's scope.

Similarly, you can modify the rule depending on the destination IP addresses.

Step 11 Close the program.

Add and Configure a SiteProtector Device in MARS

Before you can identify the agents, you must add the SiteProtector to MARS. All ISS agents forward notifications to the SiteProtector, and the SiteProtector forwards SNMP notifications to MARS. Once you define the SiteProtector and activate the device. MARS can discover the agents that are managed by that SiteProtector. However, you can also chose to manually add the agents.

To add a SiteProtector to MARS, follow these steps:

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click **Reporting Applications** tab.

Step 6 From the Select Application list, select **ISS SiteProtector 2.x**.

Step 7 Click **Add**.

The Management Console page appears.

Step 8 Do one of the following:

- To save your changes and allow the ISS agents to be discovered automatically, click **Submit**, and then click **Done**.

  Note Discovered agents are named Generic Real Secure agent, as no version information is contained in the SNMP events.

- To add a single ISS RealSecure NIDS or ISS RealSecure HIDS agent manually, continue with Add an ISS Agent Manually, page 10-11.

Add an ISS Agent Manually

MARS automatically discovers ISS agents when it receives an event from the agent. Discovered agents are named Generic Real Secure agent, as no version information is contained in the SNMP events. However, you can manually add a ISS Agent (ISS RealSecure NIDS or ISS RealSecure HIDS devices) as a child of the SiteProtector device. This feature allows you to represent all of your agents, even if they have not generated any notifications. In turn, this definition allows you to identify devices that are not reporting results.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

To add ISS Agents manually, follow these steps:

Step 1 Click **Admin > Security and Monitoring Devices**.

Step 2 From the list of devices, select the host running SiteProtector, and click **Edit**.

Step 3 Click the **Reporting Applications** tab, select **ISS SiteProtector** in the Device Type list, and click **Edit**.

Step 4 Click the **Add Agent**.

Step 5 Do one of the following:

- Select the existing device, click **Edit Existing**, and continue with Step 8.

  A page displays with the values pre-populated for hostname, reporting IP address, and at least one interface.

- Click **Add New**, and continue with Step 6.

Step 6 In the Device Name field, enter the hostname on which this ISS Agent resides.

This value should reflect the DNS entry for this device.

Step 7 In the Reporting IP field, enter the IP address that the agent uses to send logs to the SiteProtector.

Step 8 Define each interface that is configured for this host by specifying the interface name, IP address, and network mask. To add a new interface, click **Add Interface**.

The interface settings are used for attack path calculation. It is very important that you identify any dual-homed hosts by defining each interface.

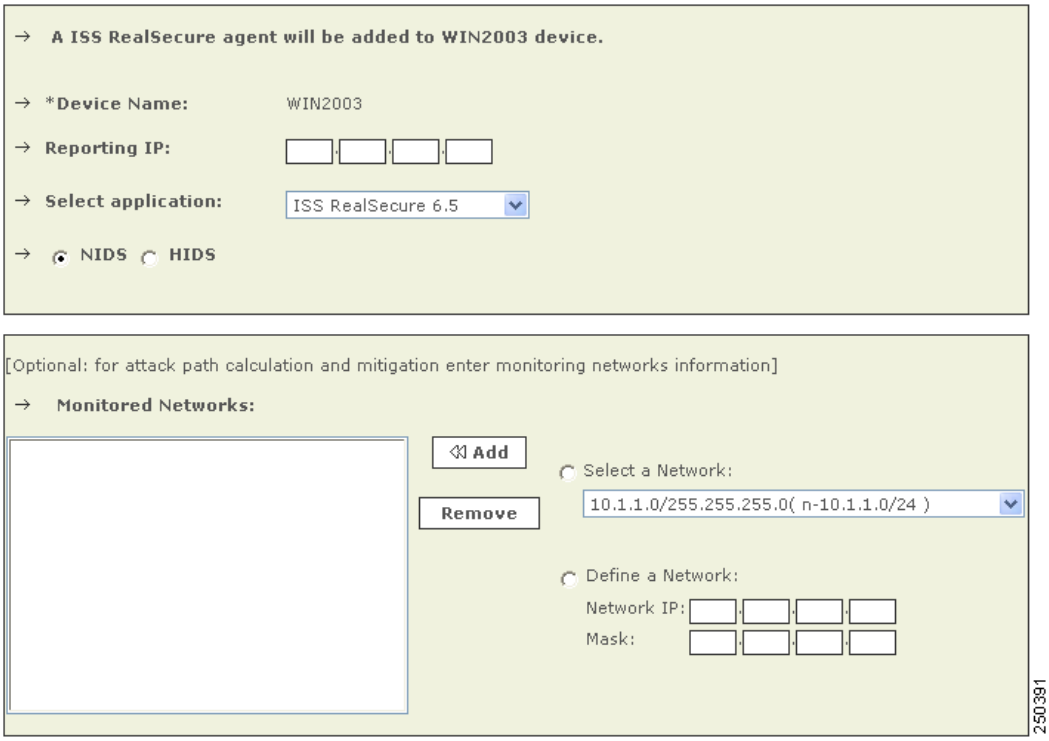
Step 9 In the Device Application field, select one of the following values:

- **ISS RealSecure 6.5**
- **ISS RealSecure 7.0**

Step 10 Select either the **NIDS** or **HIDS** option.

If you select HIDS, the Monitored Networks field disappears.

Step 11 If you selected NIDS, continue with Step 12. Otherwise, continue with Step 14.



Step 12 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

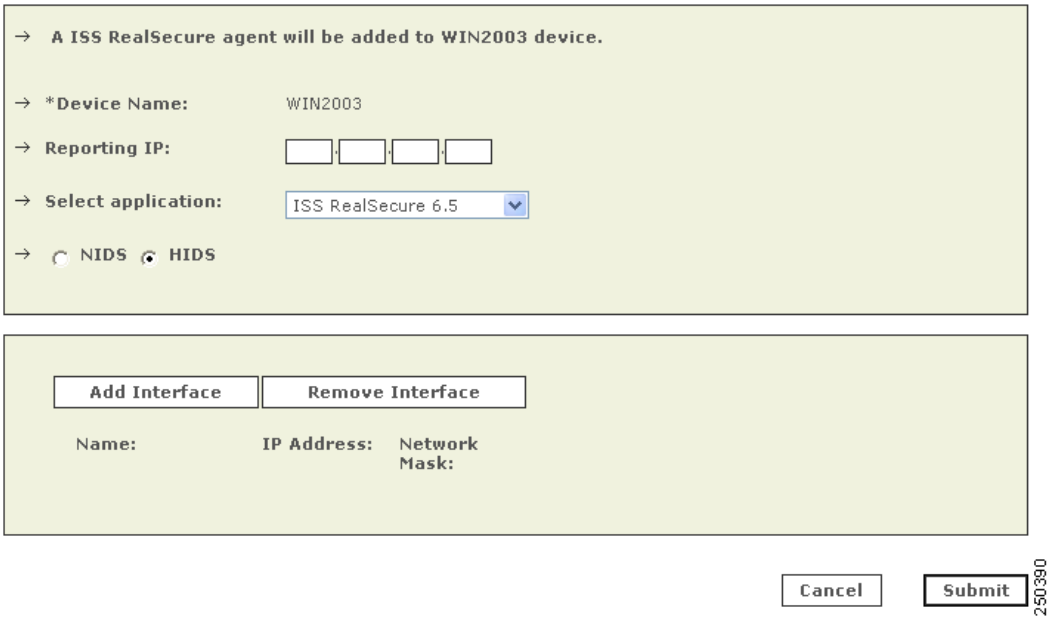
- To manually define the networks, select the **Define a Network** radio button.
  - **a.** Enter the network address in the Network IP field.
  - **b.** Enter the corresponding network mask value in the Mask field.
  - **c.** Click **Add** to move the specified network into the Monitored Networks field.
  - **d.** Repeat as needed.

- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

Step 13 Continue with Step 16.

Step 14 For multiple interfaces, click on **Add Inerfaces**, and specify the new interfaces' name, IP address, and network mask.

Figure 10-1 Adding Multiple Interfaces



Step 15 Click **Apply**.

Step 16 Click **Submit**, and then click **Done**.

Step 17 To activate this device, click **Activate**.

CHAPTER 11

ISS RealSecure 6.5 and 7.0

To configure ISS RealSecure, you must perform the following four tasks:

1. Prepare each ISS sensor as follows:
   - Edit the ***common.policy*** files to point to the MARS Appliance as an SNMP target.
   - Modify the ***current.policy*** files to configure each signature so that the SNMP notification is a default response when triggered.
   - Edit the ***response.policy*** files to specify the IP of the SNMP manager (MARS Appliance) and the community string.
   - Restart the ISS daemon for the changes to take effect.

   For more information, see Configure ISS RealSecure to Send SNMP Traps to MARS, page 11-1.
2. Add the ISS sensor to MARS as a network-based IDS device. For more information, see Add an ISS RealSecure Device as a NIDS, page 11-3.
3. Click **Activate** to enable proper processing of received events.

This chapter contains the following topics:

- Configure ISS RealSecure to Send SNMP Traps to MARS, page 11-1
- Add an ISS RealSecure Device as a NIDS, page 11-3
- Add an ISS RealSecure Device as a HIDS, page 11-4

Configure ISS RealSecure to Send SNMP Traps to MARS

To configure an ISS RealSecure sensor, follow these steps:

Step 1 Log into the sensor.

Step 2 Locate the common.policy files in these directories:

- Microsoft Windows

```
Program Files\ISS\issSensors\server_sensor_1
Program Files\ISS\issSensors\network_sensor_1
```

- Linux

```
/opt/ISS/issSensors/server_sensor_1
/opt/ISS/issSensors/network_sensor_1
```

Step 3 Open the ***common.policy*** files in a text editor.

Step 4 Change the line that reads:

```
Manager =S
```

to:

```
Manager =S <MARS's IP address>
```

If MARS Appliance's IP address is NATed, you may need to use the NATed address. If you use the MARS Appliance's IP address as the destination IP address, make sure the SNMP trap can reach MARS Appliance.

Step 5 Save these edited files and exit the editor.

Step 6 Locate the ***current.policy*** files in these directories:

- Microsoft Windows

```
Program Files\ISS\issSensors\server_sensor_1
Program Files\ISS\issSensors\network_sensor_1
```

- Linux

```
/opt/ISS/issSensors/server_sensor_1
/opt/ISS/issSensors/network_sensor_1
```

Step 7 Open the ***current.policy*** files in a text editor.

Edit each signature to have SNMP as one of its responses, and set the choice for SNMP trap as default. For example, in this original signature:

```
[\template\features\AOLIM_File_Xfer\Response\];
[\template\features\AOLIM_File_Xfer\Response\DISPLAY\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\LOGDB\];
Choice =S LogWithoutRaw;
```

Insert the following bolded lines to make it look similar to the following:

```
[\template\features\AOLIM_File_Xfer\Response\];
[\template\features\AOLIM_File_Xfer\Response\DISPLAY\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\SNMP\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\LOGDB\];
Choice =S LogWithoutRaw;
```

Step 8 Save these edited files and exit the editor.

Step 9 Locate the ***response.policy*** files in these directories:

- Microsoft Windows

```
Program Files\ISS\RealSecure SiteProtector\Console
```

- Linux

```
/opt/ISS/RealSecure SiteProtector/Console
```

Step 10 Edit the response.policy files to specify the IP of the SNMP manager (MARS Appliance) and the community string:

```
SMTP_HOST=S;
addr_1=S;
[\Response\SNMP\];
[\Response\SNMP\Default\];
Manager=S;
Community=Spublic;
```

to:

```
Manager =S <MARS's IP address> ;
Community = S <string> public;
```

If MARS Appliance's IP address is NATed, you may need to use the NATed address. If you use the MARS Appliance's IP address as the destination IP address, make sure the SNMP trap can reach MARS Appliance.

Step 11 Save these edited files and exit the editor.

Step 12 Restart the ISS daemon.

- For sensors installed on Microsoft Windows, restart it in the Services menu.
- For sensors installed on Linux, run:

```
/etc/init.d/RealSecure stop
/etc/init.d/RealSecure start
```

Add an ISS RealSecure Device as a NIDS

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name.

Step 4 Click **Apply**.

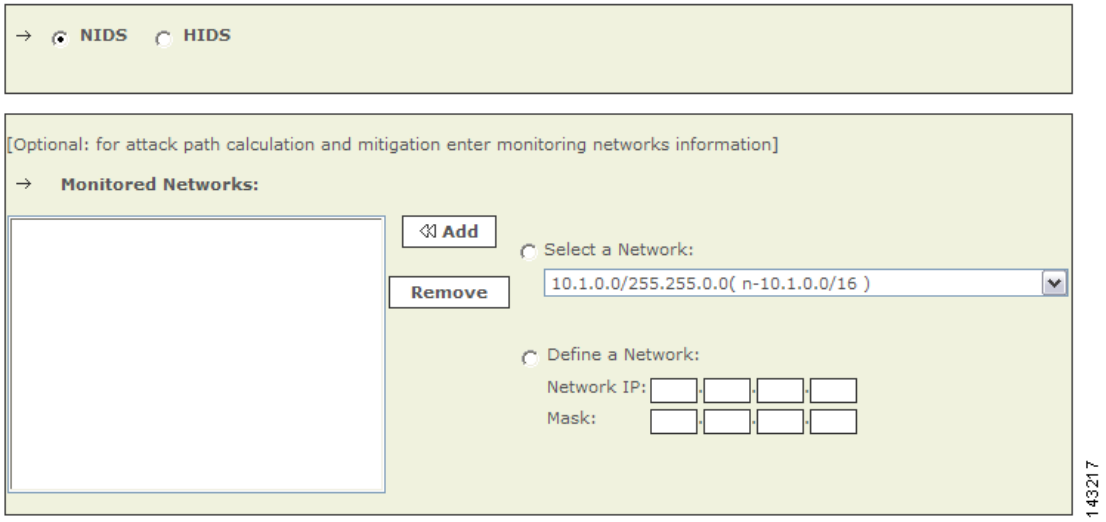
Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select **ISS RealSecure 6.5** or **ISS RealSecure 7.0**.

Step 7 Click **Add**.

Step 8 Click the **NIDS** radio button, if it is not already selected.

Figure 11-1 Configure ISS Real Secure NIDS



Step 9 For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:

- To manually define the networks, select the **Define a Network** radio button.
  a. Enter the network address in the Network IP field.
  b. Enter the corresponding network mask value in the Mask field.
  c. Click **Add** to move the specified network into the Monitored Networks field.
  d. Repeat as needed.
- To select the networks that are attached to the device, click the **Select a Network** radio button.
  a. Select a network from in the Select a Network list
  b. Click **Add** to move the specified network into the Monitored Networks field.
  c. Repeat as needed.

Step 10 To save your changes, click **Submit**.

Step 11 To enable MARS to start sessionizing events from this module, click **Activate**.

Add an ISS RealSecure Device as a HIDS

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name.

Step 4 Click **Apply**.

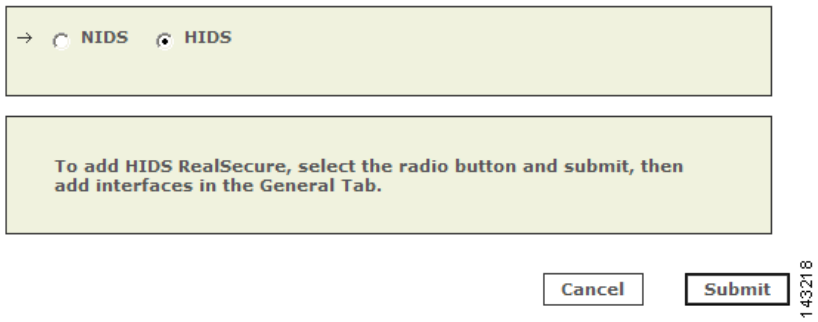
Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select **ISS RealSecure 6.5** or **ISS RealSecure 7.0**.

Step 7 Click **Add**.

Step 8 Click the **HIDS** radio button.

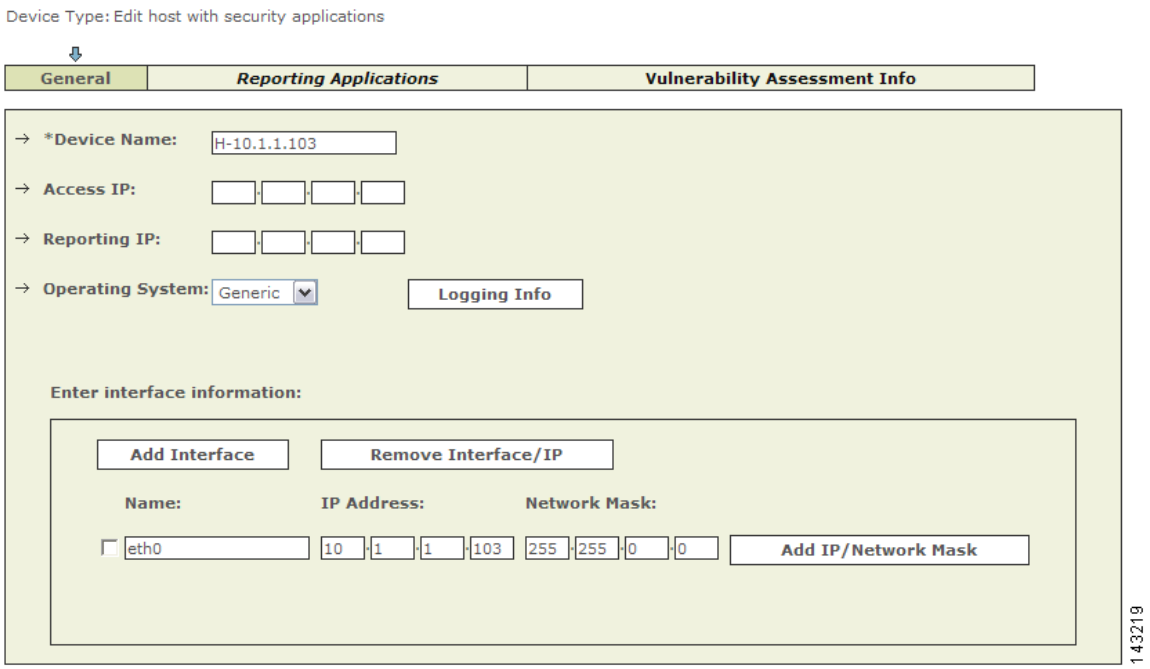
Figure 11-2 Configure ISS Real Secure HIDS



Step 9 Click **Submit**.

Step 10 For multiple interfaces, click the **General** tab, and add the new interfaces' name, IP address, and network mask.

Figure 11-3 Adding Multiple Interfaces



Step 11 Click **Apply**.

PART 3

Vulnerability Assessment

CHAPTER 12

Qualys QualysGuard Devices

In MARS, a QualysGuard device represents a specific report query to the QualysGuard API Server, which is the central API server hosted by Qualys. The only one that you configure to work with MARS is the QualysGuard API Server. You want to ensure that the QualysGuard API Server can provide reports about the devices on the network segments that you are monitoring with the MARS Appliance, as each MARS Appliance is responsible for identifying false positives for the network segments it monitors.

If you have a subscription to the QualysGuard service, MARS can pull VA data from the QualysGuard database using the QualysGuard XML API. To configure MARS to pull this data, you must perform three tasks:

- Configure QualysGuard to collect the required data, ensuring that the data is current.
- Add the QualysGuard device that represents a report query to MARS using the web interface.
- Schedule the interval at which the QualysGuard device data is pulled by MARS.

Note If a proxy server resides between the QualysGuard server and the MARS Appliance, the settings defined on the Admin > System Parameters > Proxy Settings page are used. For more information, see Specify the Proxy Settings for the Global Controller or Local Controller of the " Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 5.3.x."

This chapter contains the following topics:

- Configure QualysGuard to Scan the Network, page 12-1
- Add and Configure a QualysGuard Device in MARS, page 12-2
- Schedule the Interval at Which Data is Pulled, page 12-3
- Troubleshooting QualysGuard Integration, page 12-4

Configure QualysGuard to Scan the Network

MARS uses the QualysGuard XML API and password-based authentication over SSL (TCP port 443) to retrieve scan reports from the QualysGuard API Server. As such, you do not need to configure the QualysGuard server to accept connections from MARS. The only required configuration is that you have an active account and Qualys subscription that is configured correctly to scan your network.

By default, MARS assumes that you want to retrieve the most recent scan report saved on the QualysGuard server. Depending on the number of IP addresses analyzed, the QualysGuard scan takes from a few seconds to several minutes. You need to estimate this time so that you can schedule automated

scans of your network with a frequency that ensures a recent saved scan report is available. Using the QualysGuard administrative interface, you can determine how long a scan takes and set the schedule accordingly.

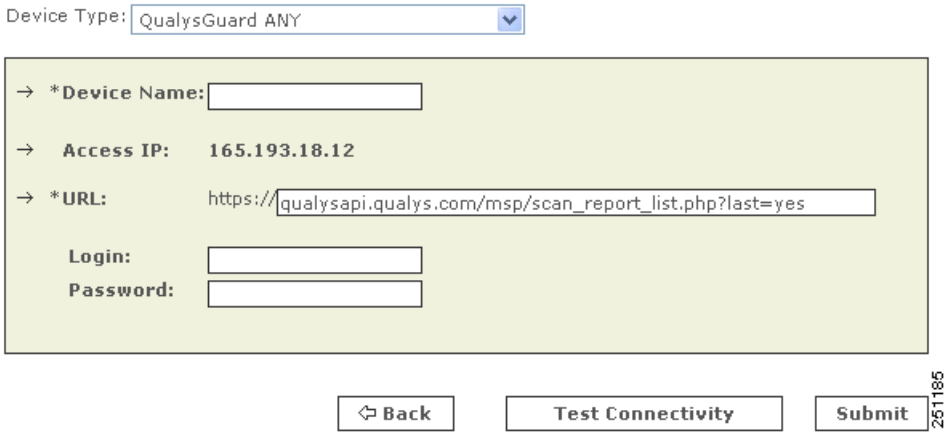
Add and Configure a QualysGuard Device in MARS

Adding an internal QualysGuard device as a reporting device entails identifying the QualysGuard API Server, which is the central API server hosted by Qualys, from which the reports are pulled and providing credentials that MARS can use to log in to the device to pull the reports. You can specify whether you want to pull saved scan reports that are run on a schedule or whether you want to initiate and retrieve an on-demand scan report. Each reporting device identifies a unique query to the QualysGuard API Server.

To add a QualysGuard device, follow these steps:

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

Step 2 Select **QualysGuard ANY** from the Device Type list.



Step 3 Enter the name of the Qualys device in the Device Name field.

This name is used to identify the Qualys device uniquely within MARS. It is used in reports and query results to identify this device.

The IP addressfield is read only. The value is also fixed at 165.193.18.12, which is significant because you can only define one schedule for pulling all report queries defined as Qualys devices on the Local Controller. However, you can define unique schedules across different Local Controllers. For more information, see Scheduling Topology Updates, page 1-18.

Step 4 Enter the URL that identifies the device and report type in the **URL** field.

The URL provides the following information:

- **Server**—Identifies the server from which the report should be pulled. This value can be specified as a hostname or IP address that identifies the primary Qualys server.
- **Report type**—Real-time vs. Last Saved. The default value.
  - *Real-time Report*. qualysapi.qualys.com/msp/scan.php?ip=[addresses]

  IP addresses may be entered as multiple IP addresses, IP ranges, or a combination of the two. Multiple IP addresses must be comma separated, as shown below:

```
123.123.123.1,123.123.123.4,123.123.123.5
```

An IP address range specifies a start and end IP address separated by a dash (-), as shown below:

```
123.123.123.1-123.123.123.8
```

A combination of IP addresses and IP ranges may be specified. Multiple entries must be comma separated, as shown below:

```
123.123.123.1-123.123.123.5,194.90.90.3,194.90.90.9
```

The addresses attribute specifies the target IP addresses for the scan request.

Note You must use a Scanner Appliance to scan private IP addresses on your internal network.

- *Last Saved Report*. qualysapi.qualys.com/msp/scan_report_list.php?last=yes

Step 5 Enter the username of the account that MARS will use to access the Qualys device in the **Login** field.

Step 6 Enter the password that corresponds to the account identified in Step 5 in the **Password** field.

Step 7 (Optional) To verify that the settings are correct and that the MARS Appliance can communicate with this Qualys device, click **Test Connectivity**.

Note The URL used to test connectivity cannot be changed. This operation verifies that the username/password is accepted and that the Qualys Server can be reached. A scan is not initiated.

If you receive error messages during this test, refer to Troubleshooting QualysGuard Integration, page 12-4.

Step 8 To add this device to the MARS database, click **Submit**.

Once you activate this device (click Activate in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Schedule the Interval at Which Data is Pulled, page 12-3.

Schedule the Interval at Which Data is Pulled

Once you activate one or more Qualys devices (where each device represents a report query run on the QualysGuard API Server), you must define the schedule at which MARS pulls data from them. The schedule, or update rule, that you define is the same for all Qualys devices. This update rule is based on the fixed IP address of 165.193.18.12, which is the Qualys Access IP. When you define an update rule using this address, all Qualys devices are updated based on that schedule. Even if you have more than one Qualys device on your network, you cannot stagger when MARS queries those Qualys devices. However, you can define unique schedules across different Local Controllers.

For more information on the broader use of update rules, see Scheduling Topology Updates, page 1-18.

To define the rule by which all Qualys devices will be discovered, 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 *Qualys Devices* or another meaningful value in the Name field.

This name identifies the rule in the list of rules that appears on the Topology/Monitored Device Update Scheduler page.

Step 4 Select the **Network IP** radio button, and enter 165.193.18.12. and 255.255.255.255 in the Network IP and Mask fields respectively.

Step 5 Click **Add** to move the device into the selected field.

Step 6 In the Schedule table, select **Daily**, and select a time value from Time of Day list.

We recommend that you pull this data daily, during off-peak hours, however, you can define any interval required by your organization.

Step 7 Click **Submit**.

The update rule appears in the list on the Topology/Monitored Device Update Scheduler page.

Step 8 Click **Activate**.

Tip To perform this discovery on demand, select the check box next to the rule you just defined and click **Run Now**

.

Troubleshooting QualysGuard Integration

Table 12-1 identifies possible errors and likely causes and solutions.

Table 12-1 Error Table for QualysGuard and MARS Integration

Error/Symptom	Workaround/Solution
Test connectivity failed. Click the View Errors button for more information. Server unavailable.	This error means that MARS was unable to connect to the Qualys device. Four possible issues can account for this message: • You have entered an invalid hostname or IP address in the URL field. Verify the value was entered correctly. • The traffic may be blocked by either a proxy server or firewalls and gateways on your network. Enable SSL traffic (TCP port 443) to traverse between the MARS Appliance and the Qualys device. Enter the correct settings for your proxy server on the Admin > System Parameters > Proxy Setting page.

Table 12-1 Error Table for QualysGuard and MARS Integration (Continued)

Fail to parse scan report.	This error means that MARS was unable to parse the scan report that it pulled from the Qualys device. Two possible issues can account for this message: • Data corruption on the QualysGuard device. • Format changes to the report due to an issue on the QualysGuard device or due to a software upgrade on the QualysGuard device. Verify that the QualysGuard device is running a supported version and that the device data is not corrupted.
Invalid user credentials.	This error means that MARS was unable to authenticate to the Qualys device. Two possible issues can account for this message: • The provided login credentials are incorrect. Verify these values were entered correctly, and verify that the provided account has sufficient privileges. • Your account has expired. Renew your subscription services with Qualys.
Test connectivity failed for qualys. Unknown host: qualysapi.qualys.com Please make sure that, • Proxy settings are configured correctly, If there is no direct connection exists from CS-MARS to Qualys server • The hostname specified in the URL string is correct • Login name and Password is valid.	Make sure that the DNS server is configured correctly for the MARS Appliance. For more information on these DNS settings, see Specifying the DNS Settings.

CHAPTER 13

eEye REM 1.0

To configure MARS to pull this REM data, you must perform three tasks:

1. Configure eEye REM to correlate the required data, ensuring that the data is current.
2. Add the eEye REM server to MARS using the web interface.
3. Schedule the interval at which the eEye REM server data is pulled by MARS.

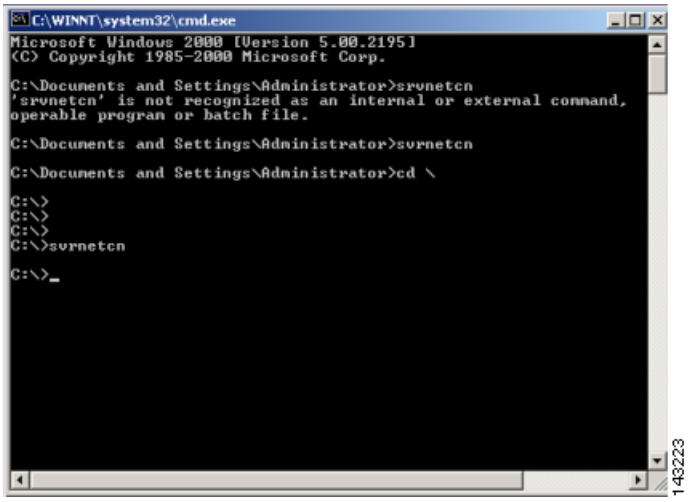
This chapter contains the following topics:

- Configure eEye REM to Generate Required Data, page 13-1
- Add and Configure the eEye REM Device in MARS, page 13-2

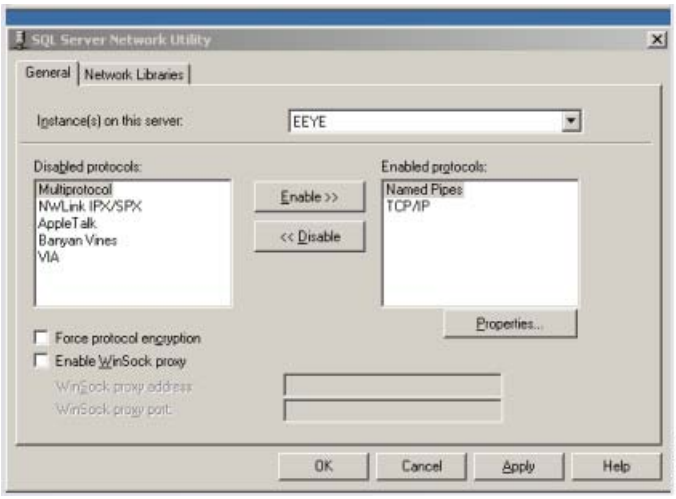
Configure eEye REM to Generate Required Data

To configure eEye REM to provide the correct data to MARS, follow these steps:

Step 1 Run command **svrnetcn** at the DOS prompt on the host where eEye REM 1.0 is installed.



Step 2 In the SQL Server Network Utility dialog box, enable TCP/IP by moving **TCP/IP** from the Disabled Protocols list to Enabled Protocols list.



Step 3 Click **Apply**.

Add and Configure the eEye REM Device in MARS

To add the eEye REM device in MARS, follow these steps:

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

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

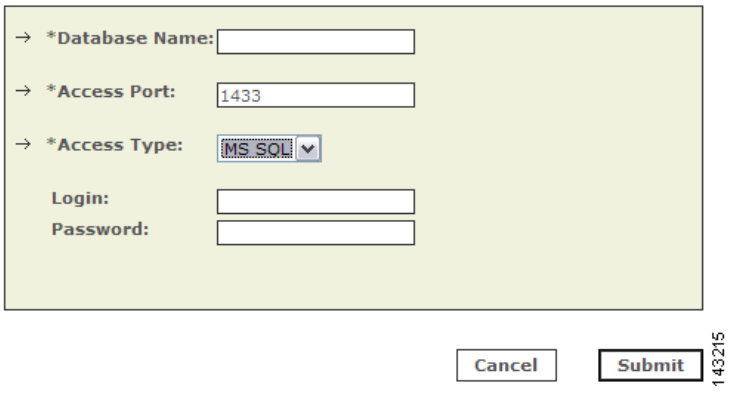
Step 3 Enter the device name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select **eEye REM 1.0.**

Step 7 Click **Add**.



Step 8 Enter the following information:

- **Database Name**—The name for this database.
- **Access Port**—The default access port is 1433.
- **Login**—The login information for the database.
- **Password**—The password information for the database.

Step 9 Click **Submit**.

Step 10 Click **Apply**.

Once you activate this device (click Activate in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Scheduling Topology Updates, page 1-18.

CHAPTER 14

McAfee Foundstone

To configure MARS to pull data from McAfee Foundstone (formerly known as Foundstone FoundScan), you must perform three tasks:

1. Configure McAfee Foundstone to enable data retrieval by MARS.
2. Add the McAfee Foundstone server to MARS using the web interface.
3. Schedule the interval at which the McAfee Foundstone server data is pulled by MARS.

This chapter contains the following topics:

- Enable McAfee Foundstone 5.x and later to Use TCP/IP, page 14-1
- Enable McAfee Foundstone (versions prior to 5.0) to Use TCP/IP, page 14-2
- Add and Configure a McAfee Foundstone Device in MARS, page 14-3

Enable McAfee Foundstone 5.x and later to Use TCP/IP

To enable TCP/IP on Foundstone 5.0 and 6.0, use the SQL Server Configuration Manager. As part of this configuraiton, you must disable the secure communications.

To enable the TCP/IP network protocol, perform the following steps:

Step 1 On the **Start** menu, choose **All Programs**, point to **Microsoft SQL Server** and then click **SQL Server Configuration Manager**.

Tip Optionally, you can open Computer Manager by right-clicking **My Computer** and choosing **Manage**. In Computer Management, expand **Services and Applications**, expand **SQL Server Configuration Manager.**

Step 2 Expand **SQL Server Network Configuration**, and then click **Protocols for***InstanceName*.

Step 3 In the list of protocols, right-click the **TCP/IP** protocol, and then click **Enable**.

The icon for the protocol changes to show that the protocol is enabled.

Step 4 In the right pane, enable the IP address of the Local Controller that is monitoring this Foundstone server.

Step 5 Click **Apply**.

Step 6 Right-click on **Protocols for***InstanceName*, and select **Properties**.

Step 7 In the Force Protocol Encryption box, verify the **OFF** option is selected.

This option disables secure communications between the MARS appliance and the Foundstone Server.

Step 8 Click **OK** to close Properties.

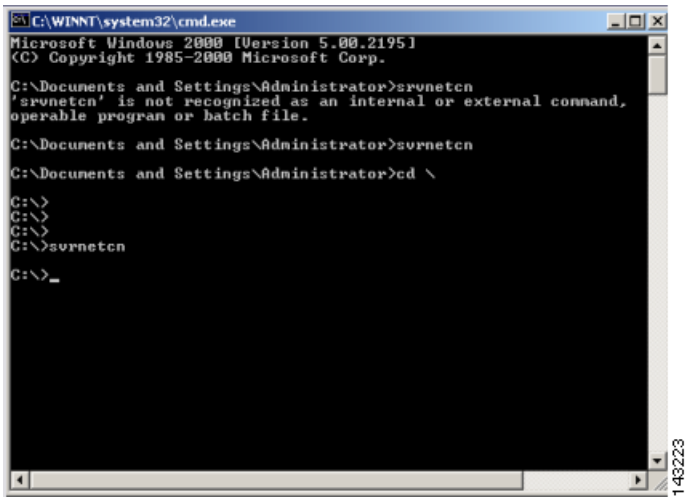
Step 9 Click **OK** to close SQL Server Configuration Manager.

Enable McAfee Foundstone (versions prior to 5.0) to Use TCP/IP

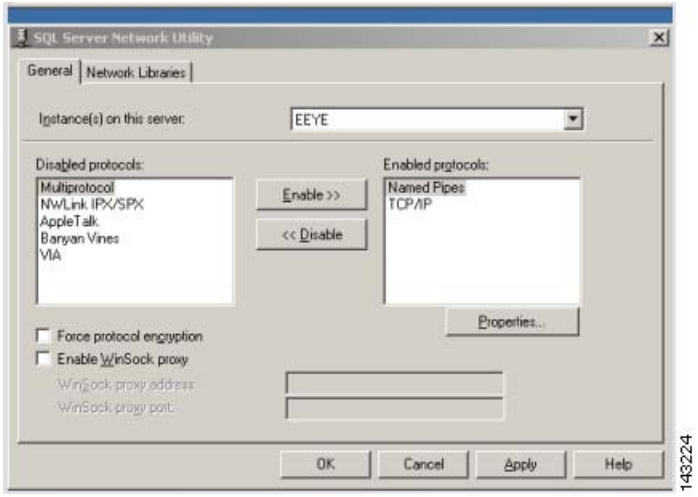
Note This procedure is only required for Foundstone versions prior to 5.0.

To configure McAfee Foundstone to provide data to MARS, follow these steps:

Step 1 Run command **svrnetcn** at the DOS prompt on the host where McAfee Foundstone is installed.



Step 2 In the SQL Server Network Utility dialog box, enable TCP/IP by moving **TCP/IP** from the Disabled Protocols list to Enabled Protocols list.



Step 3 Verify that the **Force protocol encryption** checkbox is cleared.

Step 4 Click **Apply**.

Step 5 Click **OK** to close SQL Server Network Utility.

Add and Configure a McAfee Foundstone Device in MARS

To add a McAfee Foundstone device in MARS, follow these steps:

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

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

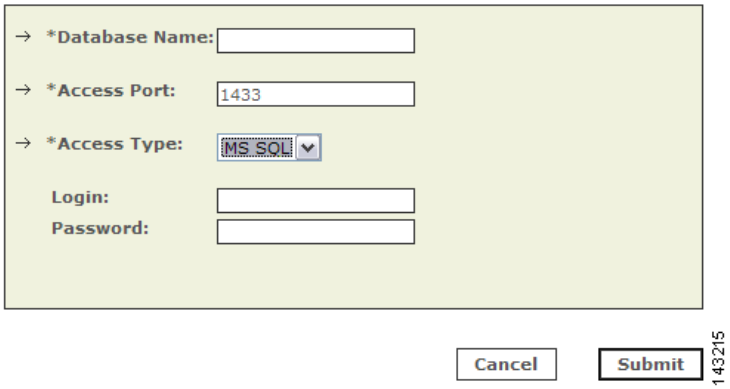
Step 3 Enter the device name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click the **Reporting Application** tab.

Step 6 From the Select Application list, select **McAfee Foundstone ANY**.

Step 7 Click **Add**.



Step 8 Enter the following information:

- **Database Name**—The name for this database.
- **Access Port**—The default access port is 1433.
- **Access Type**—Verify the value is MS SQL.
- **Login**—The login information for the database.
- **Password**—The password for the database.

Step 9 Click **Submit**.

Step 10 Click **Apply**.

Once you activate this device (click **Activate** in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Scheduling Topology Updates, page 1-18.

PART 4

Switches

CHAPTER 15

Cisco Switch Devices

You can manage Cisco switches that run either CatOS or Cisco IOS Software Release 12.2 or later. The configuration of the switch varies between these two operating system, as does the addition of the device in MARS. Adding a Cisco switch involves three steps:

1. Configure the switch to enable MARS to discover the its settings.
2. Configure the switch to generate the data required by MARS.
3. Add and configure the switch in MARS.
4. Add modules to the switch.

To prepare a Cisco switch running Cisco IOS Software Release 12.2 or later, refer to the following procedures:

- Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later, page 17-1
- Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data, page 17-2

To prepare a Cisco switch running CatOS, refer to the following procedures:

- Enable Communications Between Devices Running CatOS and MARS, page 15-1
- Configure the Device Running CatOS to Generate Required Data, page 15-3

Adding a Cisco switch running to MARS has two distinct steps. First, you add the base module of the switch, providing administrative access to that device. Second, you add any modules that are running in the switch. For instructions on performing these two steps, refer to the following topics:

- Add and Configure a Cisco Switch in MARS, page 15-6
- Adding Modules to a Cisco Switch, page 15-8

Enable Communications Between Devices Running CatOS and MARS

Before you add a Cisco switch running CatOS to MARS, make sure that you have enabled SNMP, Telnet, SSH, or FTP access to the swtich. First, you must configure the MARS Appliance as an IP address that is permited to access the switch.

For information on permitting IP addresses and specifying the access type, see the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/ip_perm.html

Next, you must ensure that your switch is configured to enable the correct access method.

This section contains the following topics:

- Enable SNMP Administrative Access, page 15-2
- Enable Telnet Administrative Access, page 15-2
- Enable SSH Administrative Access, page 15-2
- Enable FTP-based Administrative Access, page 15-2

Enable SNMP Administrative Access

To enable configuration discovery using SNMP access to the Cisco switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Configure SNMP

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/snmp.html

Enable Telnet Administrative Access

To enable configuration discovery using Telnet access to the Cisco switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Enable SSH Administrative Access

To enable configuration discovery using SSH access to the Cisco router or switch, refer to your device documentation or the following URL:

IP Access

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/ip_perm.html

Enable FTP-based Administrative Access

To enable configuration discovery using FTP access, you must place a copy the Cisco router's or switch's configuration file on an FTP server to which the MARS Appliance has access. This FTP server must have user authentication enabled.

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

You must copy the running configuration from the Cisco switch. For information on copying the running configuration, refer to your device documentation or the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/cli.html#wp10227391

Configure the Device Running CatOS to Generate Required Data

You can configure the following message types:

- Syslog message
- SNMP RO or RW strings
- NAC messages (802.1x)
- L2 discover settings

This section contains the following topics:

- Enable Syslog Messages on CatOS, page 15-3
- Enable SNMP RO/RW Strings on CatOS, page 15-4
- Enable NAC-specific Messages, page 17-4
- Enable L2 Discovery Messages, page 15-6

Enable Syslog Messages on CatOS

To configure a Cisco switch running CatOS to send syslog information to MARS, follow these steps:

Step 1 To enable the syslog server on the switch, enter:

```
set logging server enable
```

Step 2 To identify the MARS Appliance as a destination for syslog messages, enter the following command:

```
set logging server <IP address of MARS Appliance>
```

Step 3 The remaining commands tell the switch what kinds of logging information to provide and at what level. The commands in the following example can be changed to suit your requirements.

```
set logging level cdp 7 default
set logging level mcast 7 default
set logging level dtp 7 default
set logging level dvlan 7 default
set logging level earl 7 default
set logging level fddi 7 default
set logging level ip 7 default
set logging level pruning 7 default
set logging level snmp 7 default
set logging level spantree 7 default
set logging level sys 7 default
set logging level tac 7 default
set logging level tcp 7 default
set logging level telnet 7 default
set logging level tftp 7 default
set logging level vtp 7 default
set logging level vmps 7 default
set logging level kernel 7 default
```

```
set logging level filesys 7 default
set logging level drip 7 default
set logging level pagp 7 default
set logging level mgmt 7 default
set logging level mls 7 default
set logging level protfilt 7 default
set logging level security 7 default
set logging server facility SYSLOG
set logging server severity 7
set logging buffer 250
set logging timestamp enable
```

Enable SNMP RO/RW Strings on CatOS

If the supervisor SNMP server is not configured, you must perform this procedure.

To configure the supervisor SNMP server and enabled SNMP traps on the Catalyst switch, follow these steps:

Step 1 Enter configuration mode:

```
switch> enable
Enter password: <password>
switch> (enable)
```

Step 2 Set the SNMP read community string as follows:

```
switch> (enable) set snmp community read-only <read community>
```

Step 3 Set the SNMP write community string as follows:

```
switch> (enable) set snmp community read-write <write community>
switch> (enable) set snmp community read-write-all <write community>
```

Step 4 To collect RMON Ethernet statistics, RMON data collection must be enabled in the CatOS agent (this is not required in Native IOS). To enable RMON collection, enter the following:

```
switch> (enable) set snmp rmon enable

switch> (enable) set snmp rmon enable
```

Step 5 Exit configuration mode as follows:

```
switch> (enable) exit
```

Enable NAC-specific Messages

Cisco routers and switches that are running Cisco IOS Software release 12.2 and later or CatOS can enable network Admission Control (NAC) specific data. This data includes:

- **Client logs.** These logs relate the activities of the client software.
- **RADIUS server logs.** These logs relate the authorization communications between clients and the posture validation servers.

- **Network access device logs.** These logs relate connection attempts by clients and final authorizations provided by the AAA server enforcing the NAC policies.

For more information on the events that are logged as part of NAC, see the *Monitoring and Reporting Tool Integration into Network Admission Control* white paper at the following URL:

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_white_paper0900aecd801dee49.shtml

This section contains the topics that address the NAC configuration settings specific to each device type.

This section contains the following topics:

- Enable NAC Support in Cisco Switches, page 15-5

Enable NAC Support in Cisco Switches

NAC Phase II enables Cisco switches to act as network access devices. To support this new feature, you must configure the Cisco switch to initiate 802.1x authentication when the link state changes from down to up and periodically if the port remains up but unauthenticated. NAC requires that hosts use 802.1x supplicants, or clients, to authenticate to the Cisco Secure ACS server before gaining access to network services. Enabling the 802.1x messages on your network helps you troubleshoot supplicant failures becauise connection attempts are logged, which you can analyze.

Configuring the Cisco switch to act as proxy between the Cisco Secure ACS server and the 802.1x supplicants is a multi-step process. First, the e switch must be defined as a AAA client (RADIUS) in the Cisco Secure ACS server. For information on defining a AAA client, see Define AAA Clients, page 26-6. Second, the switch must be configured to use a a RADIUS server. Then, you must enable the following features on each interface installed in the switch:

- **802.1X port-based authentication.** The device requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system by using the client's MAC address.
- **802.1x reauthentication.** The device re-authenticates the supplicants after the reauthentication timeout value is reached, which is 3600 seconds by default.
- **802.1x accounting.** The device logs authentication successes and failures, as well as link down events and users logging off. The switch publishes these audit records to the Cisco Secure ACS server for logging.
- **DHCP snooping.** The device filters DHCP requests, safeguarding against spoof attacks. This feature ensures that MARS receives reliable data and identifies the port number of the 802.1x supplicant.

The following URLs detail how to configure these features:

Dot1x and Radius Sever

IOS Software:
chttp://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/sw8021x.html

CatOS Software:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/8021x.html

DHCP Snooping

IOS Software:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/swdhcp82.html

CatOS Software:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/dhcp.html

After you configure the switch to act as proxy and it is defined as a AAA client in Cisco Secure ACS, you must ensure that the authentication messages are sent to the MARS Appliance. For 802.1x accounting records, you must ensure that the audit records are written to the RADIUS log on the Cisco Secure ACS server. To configure these settings, refer toConfigure Cisco Secure ACS 4.x to Generate Logs, page 26-3 or Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4.

Enable L2 Discovery Messages

To enable L2 discovery on your Cisco switches, you must enable the spanning tree protocol (STP) and provide the SNMP RO community string. All L 2 devices must support SNMP STP MIB (IETF RFC 1493). The discovered information includes interfaces, Layer 3 (L3) routes, L2 spanning trees, L2 forwarding tables, MAC addresses, and so on.

Note STP is enabled by default on all Cisco switches. Therefore, unless you have altered this setting, no changes are necessary.

For more information on configuring STP, select **Spanning Tree Protocol** in the View Documents by Topics list at the following URL:

http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod_configuration_examples_list.html

Add and Configure a Cisco Switch in MARS

MARS monitors Cisco switches running either CatOS or Cisco IOS 12.2 and later.

To add the configuration information that MARS uses to monitor a Cisco switch running Cisco IOS 12.2 and later, follow these steps:

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

Step 2 Do one of the following:

- If the switch is running any version of CatOS, select **Cisco Switch-CatOS ANY** from the Device Type list.
- If the switch is running Cisco IOS 12.2 or later, select one of the following options from the Device Type list:
  - **Cisco IOS 12.2**
  - **Cisco IOS 12.3**
  - **Cisco IOS 12.4**

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, NetFlow MIBs, or any combination of the three, 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**, **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- 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

For more information on determining 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.

Note To perform mitigation, MARS uses the SNMP Set commands, which require SNMP RW access to a Cisco router or Cisco switch. If you define an SNMP RW string in the SNMP RO Community field, then you do not also need to define an SNMP RO string, as the RW community string enables SNMP Gets (RO) as well.

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 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 9 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Step 10 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 11 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

After submitting, you can add modules. See Adding Modules to a Cisco Switch, page 15-8.

Adding Modules to a Cisco Switch

In MARS, you can represent, discover, and monitor modules that are installed in Cisco switches. These modules perform special purpose security functions for the switch, such as firewall or intrusion detection and prevention. MARS recognizes the following switch modules and versions:

- Cisco FWSM 1.1, 2.2, 2.3, 3.1, and 3.2
- Cisco IDS 3.1 and 4.0
- Cisco IPS 5.x and 6.x
- Cisco IOS 12.2, 12.3, and 12.4

To add a module, you must first add the base module, which is the Cisco switch. After the base module is defined in the web interface, you can discover the modules that are installed in the switch (click **Add Available Module**) or add them manually (click **Add Module**).

For instructions on adding and configuring a firewall services module (FWSM), see Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1.

For instructions on adding and configuring an intrusion detection or prevention services module (IDSM or IPSM), see Chapter 9, “Cisco IPS Modules”.

This section contains the following topics:

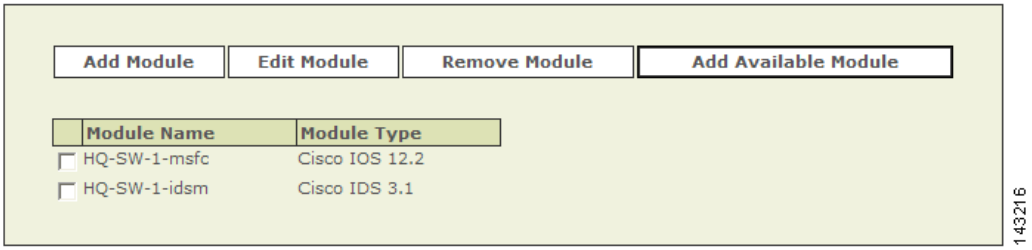
- Add Available Modules, page 15-8
- Add Cisco IOS Modules Manually, page 15-9

Add Available Modules

When you perform a discovery operation on a base module, MARS lists the discovered modules. From this list, you can select the modules to monitor using MARS.

To add available modules, follow these steps:

Step 1 Click **Add Available Module**.



If modules are installed in the switch, a list of the modules appears.

Step 2 Select a module from the Select list.

Step 3 Click **Add**.

Step 4 Repeat for other modules.

Step 5 After you add the desired modules, verify the configuration information of each. For example, verify that the SNMP RO community string matches that defined for use by MARS. To verify these settings, select a module and click **Edit Module**.

Basic guidance for editing these settings can be found in the topics that discuss manually adding these modules. See the following topics for more information:

- Add Cisco IOS Modules Manually, page 15-9
- Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1
- Chapter 9, "Cisco IPS Modules".

Step 6 To add these modules to the base module defined in 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 7 Click **Activate**.

MARS begins to sessionize events generated by this device and the selected modules and evaluate those events using the defined inspection and drop rules. Any events published by the device or its modules to MARS before activation can be queried using the reporting IP address of the device or module as a match criterion. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

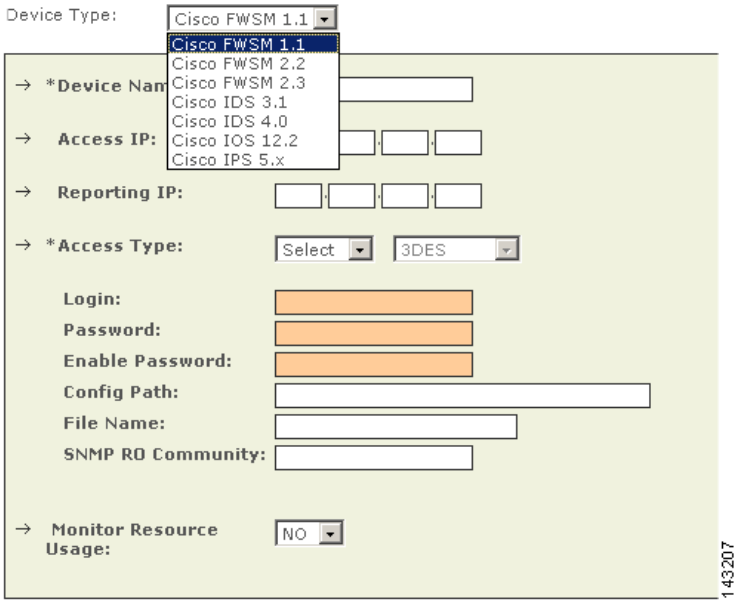
Add Cisco IOS Modules Manually

To add a module manually, follow these steps:

Step 1 Click **Add Module**.

Step 2 Select one of the following options from the Device Type list:

- **Cisco IOS 12.2**
- **Cisco IOS 12.3**
- **Cisco IOS 12.4**



Step 3 Enter the name of the module 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 modules that support the discovery operation, such as router and firewall modules, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the *hostname.domain* format.

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, NetFlow MIBs, or any combination of the three, 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**, **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- 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

For more information on determining 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.

Note To perform mitigation, MARS uses the SNMP Set commands, which require SNMP RW access to a Cisco router or Cisco switch. If you define an SNMP RW string in the SNMP RO Community field, then you do not also need to define an SNMP RO string, as the RW community string enables SNMP Gets (RO) as well.

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 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the module for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 9 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the module settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the module, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Step 10 To add this module to the device in 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.

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.

PART 5

Routers

CHAPTER 17

Cisco Routers

Revised: November 10, 2007

This chapter describes how to bootstrap routers and switches and add those reporting devices and mitigation devices to MARS. It also describes how to configure NetFlow, NAC's EAP over UDP and 802.1x logging, and the Layer 2 (L2) mitigation features of switches.

Routers and switches provide MARS with data about traffic flows and the network topology, including address translations, endpoint devices, connected networks, and accepted and rejected sessions. Routers and switches also support modules that enable features common to specialty security appliances, such as firewalls and intrusion detection or prevention systems (IDS/IPS). This chapter does not describe how to enable the features on routers and switches that enable the modules or how to configure these modules for use by MARS. Such discussions are provided in Chapter 19, "Configuring Cisco Firewall Devices", and Chapter 2, "Configuring Network-based IDS and IPS Devices".

To configure Cisco routers running Cisco IOS Software Release 12.2 and later to communicate with a MARS Appliance, you must perform three tasks.

This chapter contains the following topics:

- Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later, page 17-1
- Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data, page 17-2
- Add and Configure a Cisco Router in MARS, page 17-5

Enable Administrative Access to Devices Running Cisco IOS 12.2 and Later

You must enable administrative access by the MARS Appliance to any Cisco routers or switches running Cisco IOS Software release 12.2 and later. The type of access that you must enable depends on whether modules are installed in your Cisco router or switch and the role of the device in your network. MARS uses this administrative access to discover the device's configuration and, at times, to make changes to the device's running configuration. For information on selecting an administrative access method, see Selection of the Access Type, page 1-11.

Before you add a Cisco router to MARS, make sure that you have enabled SNMP, Telnet, SSH, or FTP access to the router. This topic contains guidance on configuring each supported access method.

This section contains the following topics:

- Enable SNMP Administrative Access, page 17-2
- Enable Telnet Administrative Access, page 17-2

- Enable SSH Administrative Access, page 17-2
- Enable FTP-based Administrative Access, page 17-2

Enable SNMP Administrative Access

To enable configuration discovery using SNMP access to the Cisco router or switch, refer to your device documentation or the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

Enable Telnet Administrative Access

To enable configuration discovery using Telnet access to the Cisco router or switch, refer to your device documentation or the following URL:

http://cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

Enable SSH Administrative Access

To enable configuration discovery using SSH access to the Cisco router or switch, refer to your device documentation or the following URL:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

Enable FTP-based Administrative Access

To enable configuration discovery using FTP access, you must place a copy the Cisco router's or switch's configuration file on an FTP server to which the MARS Appliance has access. This FTP server must have user authentication enabled.

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

You must copy the running configuration from the Cisco router or switch. For information on copying the running configuration, refer to your device documentation or the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a008020260d.shtml

Configure the Device Running Cisco IOS 12.2 and Later to Generate Required Data

Cisco routers and switches that are running Cisco IOS Software release 12.2 and later can be configured to provide different types of data to MARS:

- **Syslog messages.** The syslog messages provide information about activities on the network, including accepted and rejected sessions.

- **SNMP traffic.** SNMP RO community strings support the discovery of your network's topology.
- **NAC-specific data.** NAC logs events that are specific to its configuration, including Extensible Authentication Protocol (EAP) over UDP messages and 802.1x accounting messages.
- **Access lists or NAT statements.** You must enable SSH or Telnet access if the configuration on the Cisco router or swtich includes access lists or NAT statements.
- **Spanning tree messages** (Switch only). You must have STP (spanning tree protocol) configured correctly on the switches to enable L2 discovery and mitigation. STP provides MARS with access to the L2 MIB, which is required to identify L2 re-routes of traffic and to perform L2 mitigation. MARS also uses the MIB to identify trunks to other switches, which are used to populate VLAN information used in L2 path calculations. STP, which is enabled by default on Cisco Switches, should remain enabled, as it is required for L2 mitigation.

This section organizes the topics that describe how to configure these settings.

This section contains the following topics:

- Enable Syslog Messages, page 17-3
- Enable SNMP RO Strings, page 17-3
- Enable NAC-specific Messages, page 17-4
- Enable SDEE for IOS IPS Software, page 17-5

Enable Syslog Messages

To send syslog messages to the MARS Appliance from a device running Cisco IOS Software Release 12.2 and later, follow these steps:

Step 1 Log in to the Cisco IOS device with enabled password.

Step 2 Enter the commands:

```
Router(config)#logging source-interface <interface name>
Router(config)#logging trap <logging level desired>
Router(config)#logging <IP address of MARS Appliance>
```

Enable SNMP RO Strings

To enable SNMP RO strings for topology discovery on the Cisco IOS device, you must enable the SNMP server and define the RO community.

To configure the SNMP RO string settings, follow these steps:

Step 1 Enter configuration mode:

```
Router> enable
Password: <password>
Router#
```

Step 2 Enter the **configure terminal** command to enter configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

Step 3 Set the SNMP read community string as follows:

```
Router(config)# snmp-server community <read community>  RO <ACL name if required>
```

Note This information is required to retrieve the MAC addresses and associated L2 information.

Step 4 Set the SNMP write community string as follows:

```
Router(config)# snmp-server community <write community> RW
```

The Add and Configure a Cisco Router in MARS, page 17-5 procedure provides instructions for configuring the MARS Appliance to discover configuration and settings using these strings

Enable NAC-specific Messages

Cisco routers and switches that are running Cisco IOS Software release 12.2 and later or CatOS can enable network Admission Control (NAC) specific data. This data includes:

- **Client logs.** These logs relate the activities of the client software.
- **RADIUS server logs.** These logs relate the authorization communications between clients and the posture validation servers.
- **Network access device logs.** These logs relate connection attempts by clients and final authorizations provided by the AAA server enforcing the NAC policies.

For more information on the events that are logged as part of NAC, see the *Monitoring and Reporting Tool Integration into Network Admission Control* white paper at the following URL:

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_white_paper0900aecd801dee49.shtml

This section contains the topics that address the NAC configuration settings specific to each device type.

This section contains the following topics:

- NAC on Cisco Routers, page 17-4

NAC on Cisco Routers

This command ensures that the IOS device sends the IP address of the host that is being NAC'd in its calling-station-id attribute in all RADIUS requests to the ACS.

To configure the NAC Phase I data on a Cisco router to work with MARS, you must allow EAP over UDP and allow an IP address in the AAA station-id field of the packets. (Cisco Secure ACS includes this detail in its logs. MARS presents this data in reports and queries that dispay the host IP addresses.) In addition, you must enable logging of these events, which are published as syslog messages.

To enable the NAC-specific data on a Cisco router, enter the following commands:

Router(config)#eou allow ip-station-id Router(config)#eou logging

For more information on these commands and related commands, review the Network Admission Control feature document at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html

Enable SDEE for IOS IPS Software

Before you enable SDEE, you must enable either Telnet or SSH as the access type for configuration discovery on a Cisco IOS device. You must also enable SDEE on the device that supports the IOS IPS software feature. SDEE is used to publish events to MARS about signatures that have fired.

To enable SDEE protocol on the Cisco IOS device that supports IOS IPS, follow these steps:

Step 1 Log in to the Cisco IOS device using the enable password.

Step 2 Enter the following commands to enable MARS to retrieve events from the IOS IPS software:

```
Router(config)#ip http secure-server
Router(config)#ip ips notify sdee
Router(config)#ip sdee subscriptions 3
Router(config)#ip sdee events 1000
Router(config)#no ip ips notify log
```

Note The “no ips notify log” causes the IOS IPS software to stop sending IPS events over syslog.

Add and Configure a Cisco Router in MARS

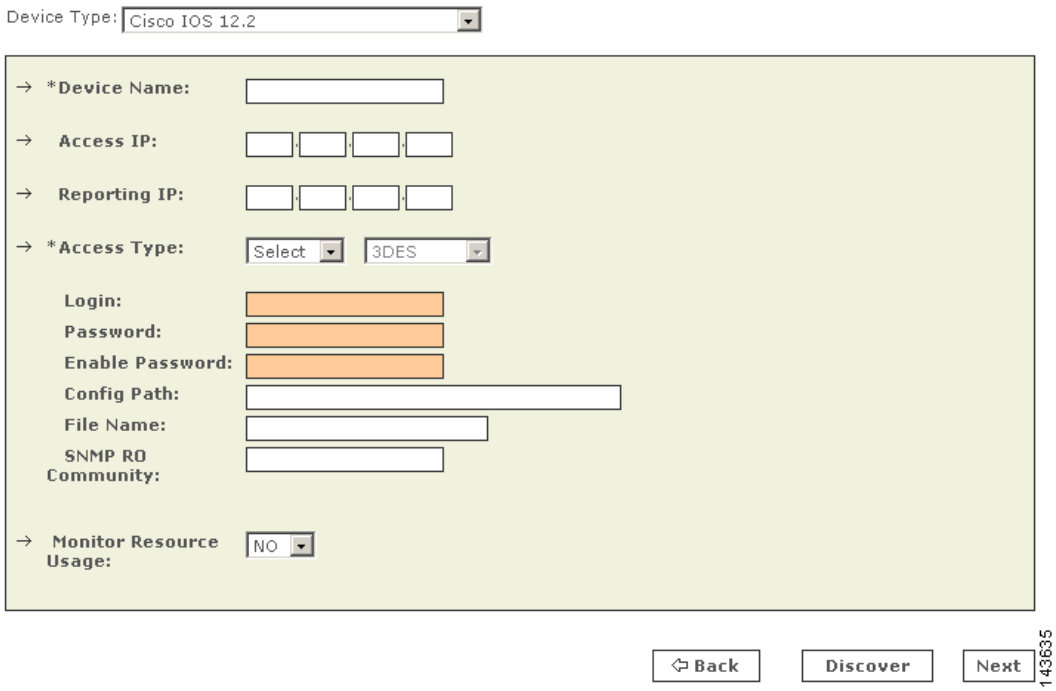
Cisco routers provide data about the network and its activities in the form of syslog messages and SNMP RO MIBs. In addition, MARS can discover settings, such as network address translations, attached networks, and active access rules, that improve the accuracy of false positive identification, attack path analysis, and L3 network discovery.

To add a Cisco router running Cisco IOS 12.2 and later, follow these steps:

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

Step 2 Select one of the following options from the Device Type list:

- **Cisco IOS 12.2**
- **Cisco IOS 12.3**
- **Cisco IOS 12.4**



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, NetFlow MIBs, or any combination of the three, 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**, **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- 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

For more information on determining 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.

Note To perform mitigation, MARS uses the SNMP Set commands, which require SNMP RW access to a Cisco router or Cisco switch. If you define an SNMP RW string in the SNMP RO Community field, then you do not also need to define an SNMP RO string, as the RW community string enables SNMP Gets (RO) as well.

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.

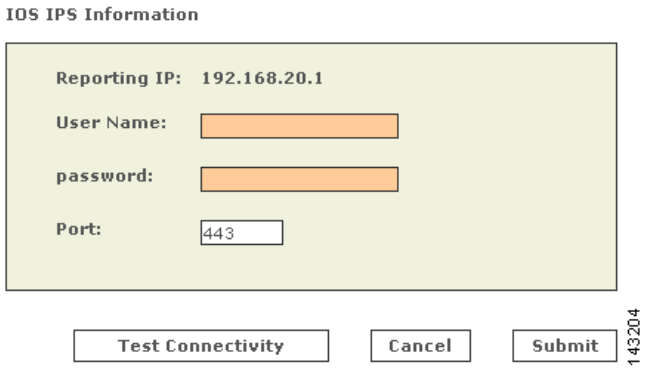
Step 8 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 9 (Optional) If this router has the IOS IPS feature and SDEE access enabled and you have configured the router to accept HTTPS connections from the MARS Appliance, click **Add IPS** to provide the username and password required to pull SDEE events.

Note IOS IPS does *not* refer to an IPS module. It refers to a software feature in the IOS software.

Result : The IOS IPS Information page appears.



a. Enter the username that has HTTPS access to this device in the User Name field.

b. Enter the corresponding password in the Password field.

c. In the Port field, verify the port used for SDEE communications with this device.

MARS pulls data using SDEE over HTTPS. The default port number for HTTPS/SDEE is 443. This access allows MARS to retrieve XML files that contain the events generated by the IOS IPS feature.

MARS can query the router for SDEE events.

Step 10 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings, including the IOS IPS settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Step 11 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 12 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

CHAPTER 18

Generic Router Device

You can add any L2 or L3 device to the MARS as long as SNMP is enabled on the device. A generic router refers to any L2 or L3 device that is not listed in the *Supported Devices and Software Versions for CS-MARS Local Controller*.

Add and Configure a Generic Router in MARS

To add and configure a generic router device in MARS, follow these steps:

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

Step 2 Select **Generic Router version unknown** 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.

PART 6

Firewalls

CHAPTER 19

Configuring Cisco Firewall Devices

Revised: July 31, 2008

This chapter describes how to bootstrap Cisco firewall devices and add them to MARS as reporting devices. Firewall devices come in several form factors: hardware appliances, software applications running on a host, modules that are installed in switches and routers, and modules that install in multifunction security devices.

Multifunction security devices, such as the Cisco Adaptive Security Appliance (ASA), also support non-firewall modules, such as intrusion detection or prevention systems (IDS/IPS) and Content Security and Control Security Services (CSC-SSM). This chapter does not focus on configuring non-firewalling modules. Instead, they are discussed in Chapter 9, "Cisco IPS Modules" and Chapter 32, "Cisco CSC SSM".

This chapter contains the following topics:

- Cisco Firewall Devices (PIX, ASA, and FWSM), page 19-1
- Failover Considerations for PIX, ASA, and Modules in ASA, page 19-21

Cisco Firewall Devices (PIX, ASA, and FWSM)

MARS support for Cisco firewall devices includes the following:

- PIX Security Appliance
- Cisco Adaptive Security Appliance (ASA)
- Cisco Firewall Services Modules (FWSM)

For the complete list of supported software releases by platform, refer to the latest *Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller* document.

Because these PIX software is mostly backward compatible, the commands required to bootstrap PIX security appliance remain consistent across the releases. In addition, Cisco ASA and FWSM have much in common with PIX command set.

The taskflow required to configure MARS to monitor a Cisco firewall device is as follows:

1. Configure the Cisco firewall device to accept administrative sessions from MARS (to discover settings).

   For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types, you configure the admin context to accept these sessions.

Note To be monitored by MARS, the Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types have the following two requirements: each context requires a unique routable IP address for sending syslog messages to MARS, and each context must have a unique name (hostname+ domain name).

2. Configure the Cisco firewall device to publish its syslog events to MARS.

   For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types, you must configure the admin context and each security context.

   Note MARS uses syslog events to discover information about the network topology. It uses SNMP to discover CPU utilization and related information.

3. Within MARS, define the Cisco firewall device by providing the administrative connection information.

   Note Before you can add an FWSM module in a switch, you must add and configure the base module (the Cisco switch) in MARS. For more information, Chapter 15, "Cisco Switch Devices".

   For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM, the basic device type represents the admin context. However you must also define or discover each security context and any installed Advanced Inspection and Prevention (AIP) modules running IPS 5.0.

To configure MARS to accept syslog event data and to pull device configurations settings from a Cisco firewall device, you must perform the following tasks:

- Bootstrap the Cisco Firewall Device, page 19-2
- Add and Configure a Cisco Firewall Device in MARS, page 19-14

Bootstrap the Cisco Firewall Device

You should configure your Cisco firewall devices to act as reporting devices and manual mitigation devices because they perform multiple roles on your network. MARS can benefit from the proper configuration of specific features:

- **IDS/IPS signature detection.** While it does not boast the most efficient or comprehensive set of signatures, the built-in IDS and IPS signature matching features of the Cisco firewall device can be critical in detecting an attempted attack.
- **Accept/Deny Logs.** The logging of accepted as well as denied sessions aids in false positive analysis.
- **Administrative Access.** Administrative access ensure MARS access to several key pieces of data:
  - *Route and ARP tables*, which aid in network discovery and MAC address mapping.
  - *NAT and PAT translation tables*, which aid in address resolution and attack path analysis, exposing the real instigator of attacks.
  - *OS Settings*, from which MARS determines the correct ACLs to block detected attacks, which paste into a management session with the Cisco firewall device.

To bootstrap the Cisco firewall device, you must identify the MARS Appliance as an administrative host Enabling administrative access allows MARS to discover the Cisco firewall device configuration settings. To enable administrative access, you must make sure that the MARS Appliance is granted Telnet or SSH administrative access to the firewall device. If you use FTP access type, make sure that you have added its configuration file to an FTP server to allow MARS access to the FTP server.

In addition to configuring specific event types and administrative access, syslog messages should be sent to the MARS Appliance. To prepare the Cisco firewall device to send these messages to the MARS Appliance, you must configure the logging settings associated with each firewall device on your network. To prepare a firewall device to generate the syslog messages and direct them to a specific MARS Appliance, you must:

1. Enable logging on the firewall device.

   Before a firewall device can generate syslog messages, you must enable logging for one or more interfaces. In addition, if you configured your firewall device in a failover pair, you can specify the standby firewall device to generate syslog messages as well. You can enable the device to ensure that the standby unit's syslog messages stay synchronized if failover occurs. However, this option results in twice as much traffic on the MARS Appliance.

2. Select the log facility and queue size.

   To generate meaningful reports about the network activity of a firewall device and to monitor the security events associated with that device, you must select the appropriate logging level. The logging level generates the syslog details required to track session-specific data. After you select a logging level, you can define a syslog rule that directs traffic to the MARS Appliance.

3. Do one of the following:

   – Select the log level to debug, or

   – Change the severity level of required events to a level other than debug and select that log level.

   The debug log level generates syslog messages that assist you in debugging. it also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. It includes all emergency, alert, critical, error, warning, notification, and information messages. Alternatively, you can change the severity level of the required messages using the **logging message** command described in Device-Side Tuning for Cisco Firewall Device Syslogs, page 19-6.

   Note Full URLs, such as `www.cisco.com/foo.html`, are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

4. Identify the target MARS Appliance and the protocol and port pair that it listens on.

   By directing syslog messages generated by a firewall device to MARS, you can process and study the messages.

Tip When monitoring a failover pair of Cisco firewall devices, you should designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

To enable administrative connections to the firewall device, select from the following options:

- Enable Telnet Access on a Cisco Firewall Device, page 19-4
- Enable SSH Access on a Cisco Firewall Device, page 19-4
- Send Syslog Files From Cisco Firewall Device to MARS, page 19-4

To configure log settings, see Send Syslog Files From Cisco Firewall Device to MARS, page 19-4.

Enable Telnet Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
telnet <MARS IP address> <netmask of MARS IP address> <interface name>
```

where *interface name* can be inside, outside, DMZ.

Enable SSH Access on a Cisco Firewall Device

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 Enter the command:

```
ssh <MARS IP address> <netmask of the MARS IP address> <interface name>
```

where *interface name* can be inside, outside, DMZ.

Send Syslog Files From Cisco Firewall Device to MARS

To send syslog messages to the MARS Appliance, you must enable logging, select the log facility and queue size, and specify the log level to debug.

Before You Begin

When preparing a Cisco firewall device to publish syslog messages, consider the following restrictions:

- In releases prior to 4.2.1, do not customize the priority of any syslog messages. If you do, MARS fails to parse those messages.
- **Do not** configure EMBLEM format for syslog messages. Make sure that the format EMBLEM extension is not used on the following command in the configuration:

```
logging host <interface name> <PN-MARS's IP address> format EMBLEM
```

To configure the firewall device to forward syslog message to MARS, follow these steps:

Step 1 Log in to the Cisco firewall device with administrator's privileges.

Step 2 To enable logging, enter one of the following commands:

- (PIX and Cisco ASA) **logging enable**
- (FWSM) **logging on**

Step 3 To specify the MARS Appliance as a target logging host, enter the following command:

```
logging host <interface name> <MARS IP address>
```

Step 4 To set the log level to debug, which ensures that HTTP and FTP session logs are generated, enter the following command:

```
logging trap debugging
```

Tip Alternatively, you can tune the event settings as defined in Device-Side Tuning for Cisco Firewall Device Syslogs, page 19-6.

The debug messages contain the HTTP URL address information. Therefore, you can create keyword-based rules matching against the firewall message itself. For example, if the debug messages are enabled and users were logging to "http://mail.cisco.com", you could create keyword-based rules that matched against "mail.yahoo.com."

Note Full URLs, such as `www.cisco.com/foo.html` , are included in HTTP session logs and FTP command data is logged only if web filtering (N2H2\SecureComputing or WebSense) is enabled on the reporting device. If web filtering is not enabled, then the HTTP session log does not include the hostname (although the destination host's IP and the Request-URI are included, such as `192.168.1.1:/foo.htm`) and FTP command data is not logged at all. Caveats exist with HTTP session logging, such as if the HTTP session request is broken across packets, then the hostname data might not be included in the log data.

Debug messages are also preferred for troubleshooting. You can define inspection rules that match on on debug-level keywords, which send notifications to the appropriate group. Refer to PIX debug messages for interesting keywords.

Cisco recommends enabling debug for optimal use of your STM solution. If a Cisco firewall device is unable to sustain debug-level messages due to performance reasons, the informational level should be used. In non-debug mode, the URL information is not available; only the 5 tuple is available for queries and reports.

Step 5 For FWSM, enter the following command:

```
logging rate-limit <eps rate desired> 1
```

Step 6 For Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM, repeat Step 2 through Step 5 for each context defined, admin and security.

Step 7 (Cisco ASA only) If an Advanced Inspection and Prevention (AIP) module is installed, you need to prepare that module as you would any IPS 5.0 module. For more information, see Chapter 9, "Cisco IPS Modules".

Device-Side Tuning for Cisco Firewall Device Syslogs

The default level for many of the events that are studied by MARS is the debug level, which can generate a high volume of additional events that are not used by MARS. If you are experiencing an influx of these other events, you can use the **logging message** command to either turn off events or change the severity level of the event to a level that generates required messages but not as many as debug.

This topic identifies the commands to use to change the log level from the command line, as well as identifies those messages consumed by MARS and their default severity level.

Logging Message Command

The following references provide details for using the **logging message** command on the appropriate firewall device:

Cisco ASA and Cisco PIX

- "Changing the Severity Level of a System Log Message" in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065731
- "Disabling a System Log Message" in *Cisco Security Appliance Command Line Configuration Guide, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/monitor.html#wp1065706
- "Logging Message Command" in *Cisco Security Appliance System Log Messages, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/l2_72.html#wp1689570
- *Cisco Security Appliance System Log Messages, Version 7.2*

  http://www.cisco.com/en/US/docs/security/asa/asa72/system/message/logmsgs.html

Cisco FWSM

- "Changing the Severity Level of a System Log Message" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm32/configuration/guide/monitr_f.html#wp1099894
- "Disabling a System Log Message" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/monitr_f.html#wp1099869
- "Logging Message Command" in *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/command/reference/l2.html#wp1565791
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/system/message/fwsm_log.html

List of Cisco Firewall Message Events Processed by MARS

The following list of events are processed by MARS. By changing the severity level for these events to ensure they are within the logging level you have selected, you can typically reduce the load on your firewall logging by 5-15%. However, the primary consumer of resources will remain the session detail events, which are processed and analyzed by MARS.

Starting with MARS version, the system can correctly parse syslogs at customized logging levels. Therefore, you can move the syslogs processed by MARS to a lower level and then set the log to that level, for example *logging level 6*. Use the command **logging message***message-id* level *level* on the ASA, or PIX, to move a syslog message to a new level.

The following syslog message IDs are those required for proper sessionization. If you change the logging level of the firewall, ensure that the following messages IDs are generated at the new level so the MARS Appliance receives them.

Note The syslog message IDs listed below are required for sessionization. However, other logs at the debug or informational levels may exist that you may require for other purposes. for example, a specific URL accessed by one user if you are doing URL filtering on the security appliance. Refer to the Logging Message Command, page 19-6 for pointers to the full message list for each firewall device type.

- 101001-101005
- 102001
- 103001-103007
- 104001-104004
- 105001-105011
- 105020-105021
- 105031-105032
- 105034-105040
- 105042-105048
- 106001-106002
- 106006-106007
- 106010-106027
- 106100-106101
- 107001-107003
- 108002-108003
- 108005
- 108007
- 109001-109003
- 109005-109008
- 109010-109014
- 109016-109034
- 110001-110003
- 111001

- 111003-111005
- 111007-111009
- 111111
- 112001
- 113001
- 113003-113023
- 114001-114021
- 199001-199003
- 199005-199009
- 199011
- 199012
- 199907-199908
- 201002-201006
- 201008-201013
- 202001
- 202005
- 202011
- 208005
- 209003-209005
- 210001-210003
- 210005-210008
- 210010
- 210020-210022
- 211001
- 211003
- 212001-212006
- 213001-213006
- 214001
- 215001
- 216003
- 216004
- 217001
- 218001-218004
- 219002
- 302001
- 302003-302004
- 302007-302010
- 302012-302023

- 302033
- 302034
- 302302
- 303002-303005
- 304001-304009
- 305005-305012
- 308001-308002
- 311001-311004
- 312001
- 313001
- 313003-313005
- 313008
- 314001-314006
- 315004
- 315011
- 316001
- 316002
- 317001-317006
- 318001-318009
- 319001-319004
- 320001
- 321001-321004
- 322001-322004
- 323001-323006
- 324000-324007
- 324300-324301
- 325001-325003
- 326001-326002
- 326004-326017
- 326019-326028
- 327001-327003
- 328001
- 329001
- 331001-331002
- 332001-332004
- 333001-333010
- 334001-334009
- 335001-335014

- 336001-336011
- 400000-400050
- 401001-401005
- 402101-402103
- 402106
- 402114-402120
- 402121-402127
- 403101-403104
- 403106-403110
- 403500-403507
- 404101-404102
- 405001-405002
- 405101-405107
- 405201
- 405300-405301
- 406001-406002
- 407001-407003
- 408001-408003
- 409001-409013
- 409023
- 410001-410004
- 411001-411004
- 412001-412002
- 413001-413006
- 414001-414002
- 415001-415020
- 416001
- 417001
- 417004
- 417006
- 417008-417009
- 418001
- 419001-419002
- 420001-420006
- 421001-421007
- 422004-422006
- 423001-423005
- 424001-424002

- 425001-425006
- 428001
- 431001-431002
- 446001
- 450001
- 500001-500004
- 501101
- 502101-502103
- 502111-502112
- 503001
- 504001-504002
- 505001-505016
- 506001
- 507001-507002
- 508001-508002
- 509001
- 602101-602104
- 602201-602203
- 602301-602304
- 603101-603109
- 604101-604104
- 605004-605005
- 606001-606004
- 607001-607002
- 608001-608005
- 609001-609002
- 610001-610002
- 610101
- 611101-611104
- 611301-611323
- 612001-612003
- 613001-613003
- 614001-614002
- 615001-615002
- 616001
- 617001-617004
- 620001-620002
- 621001-621003

- 621006-621010
- 622001
- 622101-622102
- 634001
- 701001-701002
- 702201-702212
- 702301-702303
- 702305
- 702307
- 703001-703002
- 709001-709007
- 710001-710006
- 711001-711002
- 713004
- 713006
- 713008-713010
- 713012
- 713014
- 713016-713018
- 713020
- 713022
- 713024-713037
- 713039-713043
- 713047-713052
- 713056
- 713059-713063
- 713065-713066
- 713068
- 713072-713076
- 713078
- 713081-713086
- 713088
- 713092
- 713094
- 713098-713099
- 713102-713105
- 713107
- 713109

- 713112-713124
- 713127-713149
- 713152
- 713154-713172
- 713174
- 713176-713179
- 713182
- 713184-713187
- 713189-713190
- 713193-713199
- 713203-713206
- 713208-713226
- 713228-713251
- 713254
- 713900-713906
- 714001-714007
- 714011
- 715001
- 715004-715009
- 715013
- 715019-715022
- 715027-715028
- 715033-715042
- 715044-715072
- 715074-715079
- 716001-716056
- 717001-717049
- 718001-718081
- 718082-718088
- 719001-719026
- 720001-720073
- 721001-721019
- 722001-722041
- 723001-723014
- 724001-724002
- 725001-725015
- 726001
- 730001

- 730002-730005
- 730010
- 731001-731003
- 732001-732003
- 733100
- 733102
- 733103
- 734002-734004

Add and Configure a Cisco Firewall Device in MARS

The process of adding a PIX security appliance, Cisco ASA, or FWSM to MARS involves many of the same steps, regardless of the version of software that is running. The process is exactly the same for PIX software versions 6.0, 6.1, 6.2, and 6.3. However, Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM provide the ability to define multiple security contexts, or virtual firewalls.

Adding a Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM to MARS has two distinct steps. First, you must define the settings for the admin context. Then, if multiple context mode is enabled, you define or discover the settings for its security contexts. These Cisco firewall device have two type of contexts: one admin context, which is used for configuration of the device itself, and one or more security contexts. For Cisco ASA, you can also define or discover any modules that are installed in the appliance.

To be monitored by MARS, the Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM device types have the following additional requirements:

- each context requires a unique routable IP address for sending syslog messages to MARS
- each context must have a unique name (hostname+ domain name)

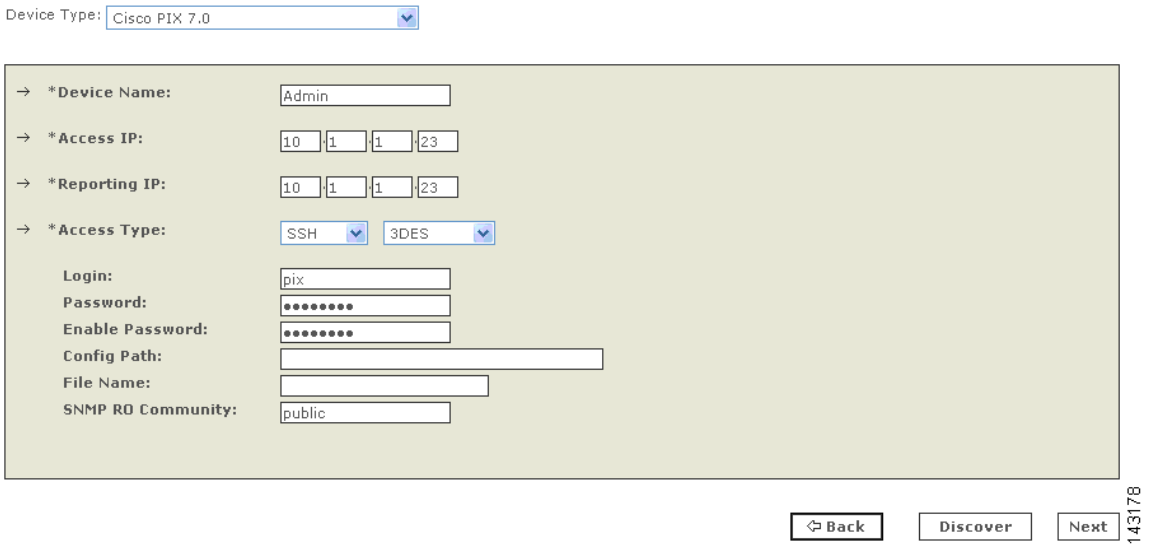
Note The Cisco ASA, PIX 7.0, 7.2, and 8.0, and FWSM can run in single context mode, which means that the system context acts as both the admin context and a security context.

To add and configure a Cisco firewall device, follow these steps:

Step 1 Do one of the following:

- If you are adding an FWSM, you must be on the main page of the Cisco switch to which you are adding it. On that page, click **Add Module**, and select one of the following options from the Device Type list:
  - Cisco FWSM 1.1
  - Cisco FWSM 2.2
  - Cisco FWSM 2.3
  - Cisco FWSM 3.1
  - Cisco FWSM 3.2
- If you are adding a PIX security appliance or a Cisco ASA, an Select **Admin > System Setup > Security and Monitor Devices > Add**, and select one of the following options from the Device Type list:

- Cisco ASA 7.0
- Cisco ASA 7.2
- Cisco ASA 8.0
- Cisco PIX 6.0
- Cisco PIX 6.1
- Cisco PIX 6.2
- Cisco PIX 6.3
- Cisco PIX 7.0
- Cisco PIX 7.2
- Cisco PIX 8.0



Step 2 Enter the name of the firewall 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 3 (Optional) To enable MARS to discover settings from this firewall device, enter the administrative IP address in the Access IP field.

Note If the device is running Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, this address corresponds to IP address from which the syslog messages of the admin context are sent.

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 4 Enter the IP address of the interface that publishes syslog messages or SNMP notifications, or both in the Reporting IP field.

Note If the device is running Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, this address corresponds to the address from which the admin context syslog messages are published.

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 5 If you entered an address in the Access IP field, select **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- 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

Note If you select the FTP access type and you are defining a Cisco ASA, PIX 7.0, 7.2, and 8.0, or FWSM, you cannot discover the non-admin context settings. Therefore, this access type is not recommended.

For more information on determining the access type, see Selection of the Access Type, page 1-11.

Step 6 (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.

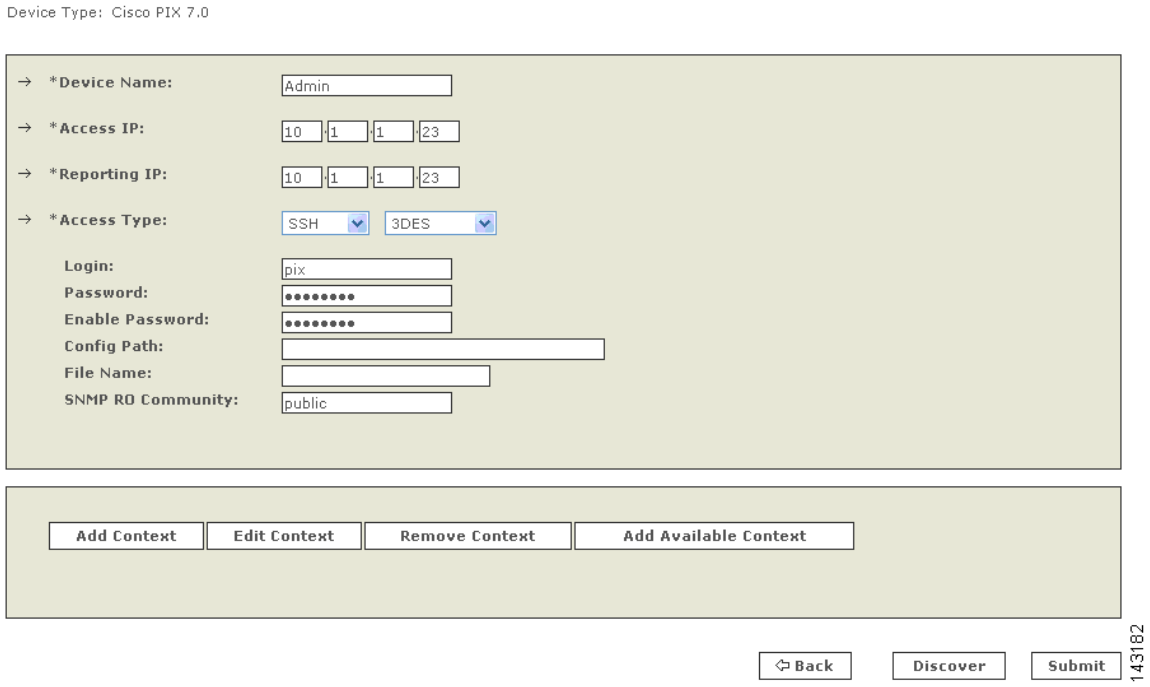
Step 7 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 8 (Cisco ASA, FWSM, and PIX 7.0, 7.2, and 8.0 Only) do one of the following:

- Click **Discover** to let MARS contact the device and conduct a topology and context configuration discovery. Information about the security contexts is presented in the Context section of the main page. To edit discovered contexts, continue with Edit Discovered Security Contexts, page 19-20.
- Click **Next** to commit your changes and allow for manual definition of security contexts or modules. Continue with Add Security Contexts Manually, page 19-17, Add Discovered Contexts, page 19-19, or Add an IPS Module to a Cisco Switch or Cisco ASA, page 9-2.

For PIX and FWSM, you can add one or more security contexts. For Cisco ASA, you can add one or more security contexts or Advanced Inspection and Prevention (AIP) modules, running the Cisco IPS 5.x software.



Step 9 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings, including any security contexts and their settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Step 10 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 11 Click **Activate**.

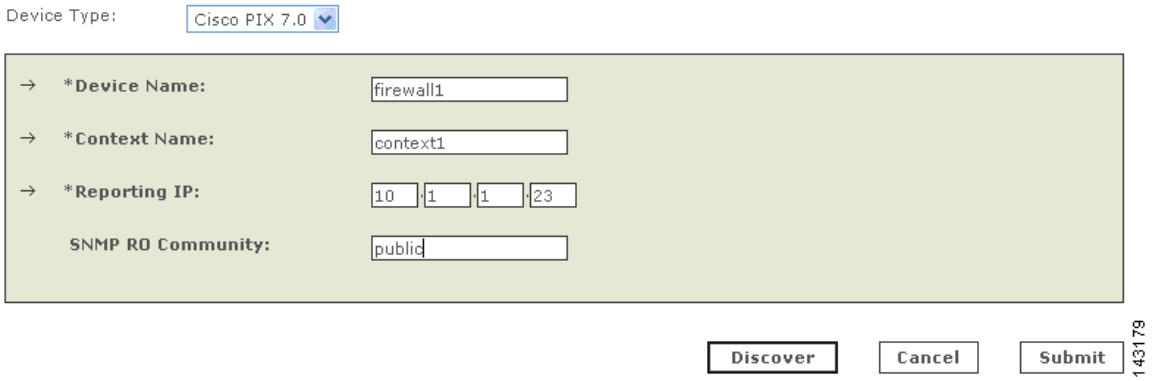
MARS begins to sessionize events generated by this device and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Add Security Contexts Manually

You can manually define security contexts in PIX 7.0, 7.2, and 8.0, Cisco ASA, or FWSM.

Step 1 Do one of the following:

- (PIX 7.0, 7.2, and 8.0 and FWSM) Click **Add Context**.
- (Cisco ASA) Click **Add Module**.



Step 2 In the Device Type list, do one of the following:

- For Cisco ASA, select **Cisco ASA 7.0**, **Cisco ASA 8.0**, or **Cisco ASA 8.1**.
- For PIX, select **Cisco PIX 7.0**, **Cisco PIX 7.2**, or **Cisco PIX 8.0**.
- For FWSM, select **Cisco FWSM *x.y***, where *x.y* is the version number of the software running on the module.

Step 3 Enter the name of the firewall 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 Enter the name of the security context in the Context Name field.

This name must exactly match the context name defined on the device.

Step 5 Enter the IP address of the security context from which syslog messages or SNMP notifications, or both are published 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 (Optional) To enable MARS to retrieve MIB objects for this security context, 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 security context's CPU usage, network usage, and device anomaly data and to discover device and network settings.

Step 7 To discover the settings of the defined context click **Discover**.

This discovery collects all of the route, NAT, and ACL-related information. In addition, the name of the device may change to the *hostname.domain* format if it was not already entered as such.

Step 8 To save your changes, click **Submit**.

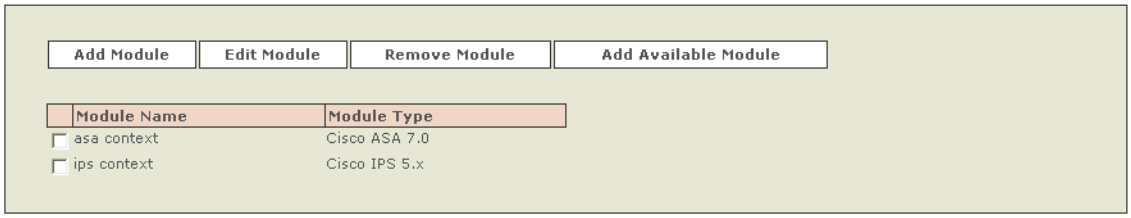
Add Discovered Contexts

When you select Discover on a Cisco ASA, PIX 7.0, 7.2, and 8.0 or FWSM, MARS discovers the contexts that are defined for that firewall device. However, you must still manually add discovered contents.

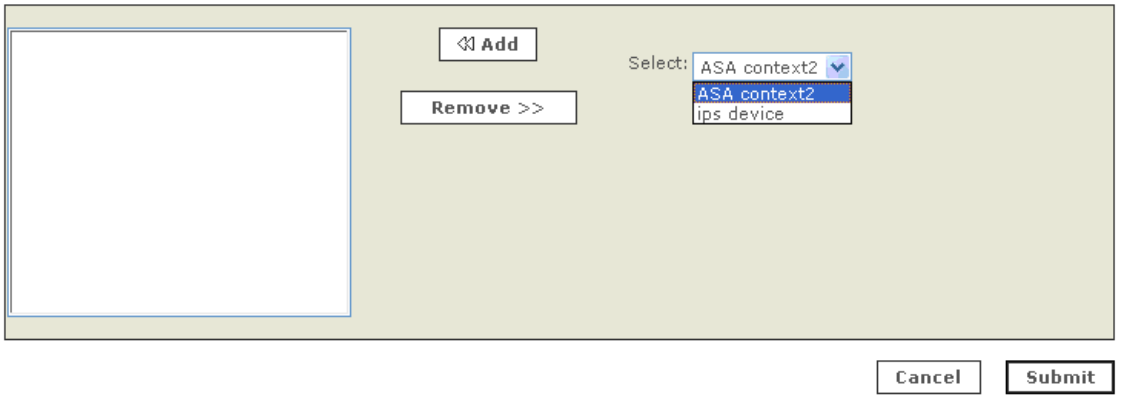
Note You cannot discover a module install in a Cisco ASA; you must manually define IPS modules. However, the discovered contexts do appear under the Module area on the main page.

Step 1 Do one of the following:

- (PIX 7.0, 7.2, and 8.0 and FWSM) Click **Add Available Context**.
- (Cisco ASA) Click **Add Available Module**.



Step 2 Select a security context from the Select list.



Step 3 Click **Add**.

Step 4 Repeat for other contexts.

Step 5 To save your changes, click **Submit**.

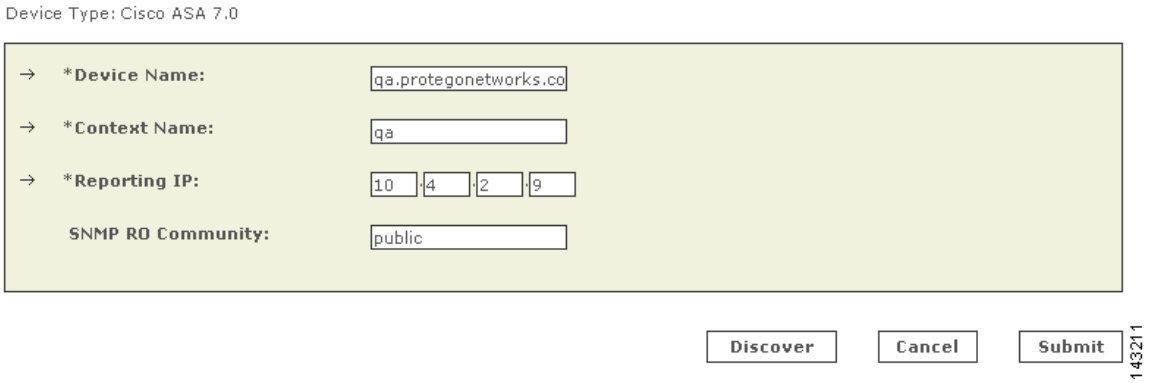
After you add discovered contexts, you must edit them to provide the contact information required by MARS. Continue with Edit Discovered Security Contexts, page 19-20.

Edit Discovered Security Contexts

Note You must edit all discovered contexts to specify the reporting IP address and the SNMP RO community string.

Step 1 From the list of discovered contexts, select the one that you want to edit and select the action appropriate to the device type:

- (PIX 7.0, 7.2, and 8.0) Click **Edit Context**.
- (Cisco ASA and FWSM) Click **Edit Module**.



Step 2 Enter the IP address from which the syslog messages of the security context are sent in the Reporting IP field.

Step 3 (Optional) To enable MARS to retrieve MIB objects for this context, 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 4 (Optional) To enable MARS to monitor this context for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 5 To save your changes, click **Submit**.

Step 6 Repeat for each discovered context.

Failover Considerations for PIX, ASA, and Modules in ASA

When monitoring a failover pair of Cisco firewall devices (PIX or ASA), you should designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

While this is true for the actual firewalls, it is not true for AIP-SSM modules. AIP-SSM modules do not swap IP addresses in the event of a failover. Therefore, to ensure that MARS receives uninterrupted IPS event data, you must configure both the primary and secondary AIP-SSM modules as child modules of the same ASA device that represents the Active/Standby pair. In this configuration, MARS will likely generate "Inactive Reporting Device" messages on the hour for the non-active AIP-SSM module.

CHAPTER 20

Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x and 8.2.x with NetFlow

Revised: October 14, 2008, OL-16778-01

Contents

This chapter describes how to add the Cisco ASA, Versions 8.1.x or 8.2.x to the Local Controller as reporting devices, and how to configure NetFlow Security Event Logging (NSEL) between the Cisco ASA 5580, Version 8.1.x or 8.2.x and the MARS Local Controller.

Configuration procedures for firewall syslog monitoring and for adding other versions of the Cisco ASA to MARS are described in, "Configuring Cisco Firewall Devices."

This chapter contains the following sections:

- Information About Configuring the Cisco ASA Version 8.1.x with NSEL, page 1
- Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS, page 3
- Configuring NSEL for MARS on the Cisco ASA 5580, page 10
- Additional References, page 13

Information About Configuring the Cisco ASA Version 8.1.x with NSEL

NetFlow Security Event Logging (NSEL) is an efficient logging method for high-speed environments. Before Cisco ASA Release 8.1, Cisco ASA events were exported exclusively through system log (syslog) messages and SNMP traps. NSEL can transmit much of the same syslog information in a less CPU-intensive, more secure, and more bandwidth-efficient way. NSEL is an adaptation of NetFlow version 9.

To implement NSEL, the MARS Local Controller is configured as a NetFlow collector on the Cisco ASA 5580. When the Cisco ASA is configured in multi-mode, each context can report to its own MARS Appliance—if the contexts are on separate networks. The MARS Local Controller can use the Cisco ASA NSEL information as follows:

- Create topology-aware sessionization of NetFlow events with non-NetFlow events

- Perform rule correlation and incident firing from NetFlow events
- Retrieve collected NetFlow data with queries and non-scheduled reports
- View incoming Netflow events with the Real-time Event Viewer
- Configure drop rules against incoming NetFlow events
- Use NetFlow-derived events in Scheduled reports results (For example, Top N reports)

Note Syslog-based anomaly detection is still supported for all versions of the Cisco ASA.

For information on NetFlow anomaly detection on MARS, see the, *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*, Understanding NetFlow Anomaly Detection on MARS.

For detailed information on NSEL, configuring the Cisco ASA Security Appliance, and descriptions of how NSEL and SYSLOG events compare, see the following publications:

- All Cisco ASA 5500 Series Adaptive Security Appliances documentation:
  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco ASA 5580 Adaptive Security Appliance Command Reference (8.1, 8.2)
  http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/refgd.html

  http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html
- Monitoring the Cisco ASA Security Appliance (8.1, 8.2):
  http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html#wp1099818

  http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_syslog.html
- Cisco ASA 5580 Implementation Note for NetFlow Collectors (8.1 and 8.2):
  http://www.cisco.com/en/US/docs/security/asa/asa81/netflow/netflow.html

  http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html

Taskflow for Configuring NSEL on MARS

The taskflow for configuring the Cisco ASA, Version 8.1.x and 8.2.x with MARS NetFlow Security Event Logging is as follows:

1. Identify the Cisco ASA contexts and modules on which to enable NSEL.
2. Disable syslog reporting to MARS on those devices.
3. Enable NSEL on each Cisco ASA reporting device and direct the NetFlow data to the MARS Appliance responsible for that network segment.
4. Verify that all the Cisco ASA reporting devices are defined in the MARS web interface.
5. Enable NetFlow processing in the MARS web interface.
6. Configure Networks for Traffic Anomaly Detection in the MARS web interface (if necessary)
7. Allow MARS to study traffic for a week to develop a usage baseline before it begins to generate incidents based on detected anomalies.

Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS

Prerequisites

The following prequisites are required for MARS-ASA interoperability:

- MARS is permitted administrative access to ASA
- MARS is configured as a NetFlow collector for the ASA.
- MARS is configured with the same NTP server as the Cisco ASA

For details on configuring the Cisco ASA, Version 8.1.x for MARS, See the *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide, Version 8.1, Appendix F,* section *Configuring NSEL for MARS on the ASA 5580* at the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/csmars.html

For details on configuring the Cisco ASA, Version 8.2.x for MARS, See the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2* at the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ref_csmars.html

Procedures for configuring administrative access on the Cisco ASA, Version 7.x and 8.0.x are also described in this guide, in the chapter, "Configuring Cisco Firewall Devices."

See also, Related Documents, page 13.

SUMMARY STEPS

1. Navigate to Admin > System Setup > Security and Monitor Devices.
2. Select Cisco ASA, Version 8.1 or Cisco ASA, Version 8.2 from the Device Type drop-down list.
3. Complete the configuration fields on the device configuration page.
4. Click Submit.
5. Click Activate.

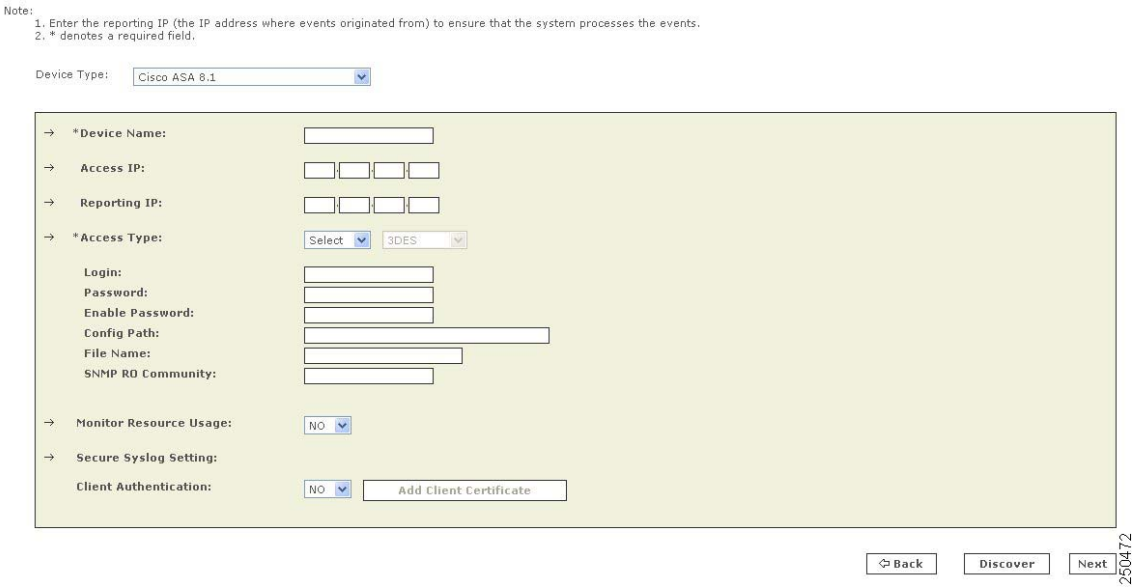
DETAILED STEPS

Step 1 Navigate to **Admin > System Setup > Security and Monitor Devices**.
The Security and Monitoring Information page appears.

Step 2 Click **Add**.
The Device Configuration page appears.

Step 3 Select **Cisco ASA 8.1** or **Cisco ASA 8.2** from the Device Type drop-down list.
The ASA 8.1 Configuration page appears, as shown in Figure 20-1.

Figure 20-1 Add the Cisco ASA, Version 8.1.X to MARS (Admin > Security and Monitor Devices > Add > Device Type> ASA 8.1)



Step 4 Complete the configuration fields as described in Table 20-1.

Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields

ASA 8.x Device Configuration Field	Description
Device Name	Name of the Cisco ASA device. 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 value specified in this field.
Access IP	ASA Administrative IP address—allows MARS to discover settings of the ASA. The Access IP address must be reachable from MARS.
Reporting IP	The IP address of the interface that sends NetFlow data. The Reporting IP is seen in MARS as the sender IP in an ASA syslog or netflow packet. The Reporting IP address does not have to be reachable from MARS or be the IP address of the ASA admin context (because separate NetFlow collectors can be configured from each context).

Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields (Continued)

ASA 8.x Device Configuration Field	Description
Access Type	If you entered an address in the Access IP field, select TELNET, SSH, or FTP from the Access Type list, and continue with the procedure that matches your selection: **To configure Telnet access for devices in MARS:** • In the Login field, enter the username of the administrative account to use when accessing the reporting device. **Note** The username filed is optional for a telnet connection. It is required only when AAA is configured for the telnet access. • In the Password field, enter the password associated with the username specified in the Login field. • Enter the Cisco ASA enable password in the Enable Password field. **To configure SSH access for Cisco ASA in MARS:** • 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. • In the Login field, enter the username of the administrative account to use when accessing the reporting device. • In the Password field, enter the password associated with the username specified in the Login field. • If this device supports an enable mode, enter that password in the Enable Password field. **To configure FTP access for devices in MARS:** • In the Login field, enter the username of the FTP server account to use when accessing the configuration file of the reporting device. • In the Password field, enter the password associated with the username specified in the Login field. • 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. • In the File Name field, enter the name of the reporting device's configuration file residing on the FTP server.
Login	See Access Type.
Password	See Access Type.

Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields (Continued)

ASA 8.x Device Configuration Field	Description
Enable Password	See Access Type.
Config Path	See Access Type, "To configure FTP access."
File Name	See Access Type, "To configure FTP access."
SNMP RO Community	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 the Cisco ASA's CPU usage, network usage, device anomaly data and to discover device and network settings.
Monitor Resource Usage	Optional. To enable MARS to monitor this device for anomalous resource usage, select Yes from the Monitor Resource Usage list. MARS monitors the ASA for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports.
Secure Syslog Setting: Client Authentication (not relevant to NSEL)	Optional. The Cisco ASA 8.0 and 8.1 can be configured to send secure syslogs, that is, syslogs over an SSL connection. **No**—No client authentication is necessary. **Yes**—Perform the following tasks: • Click **Add Client Certificate.** • Copy and paste the certificate into the Update Client Certificate pop-up window that appears. • Click **Accept.** **Note** NSEL is transported by UDP.

Step 5 Do one of the following:

- Click **Discover** to let MARS contact the device and conduct a topology and module configuration discovery. Information about the security modules is presented on the Security and Monitoring Information page.

  To edit discovered contexts, continue with Edit Discovered Security Contexts.
- Click **Next** to commit your changes and manually configure Cisco ASA modules.

For the Cisco ASA, you can add one or more security contexts or Advanced Inspection and Prevention (AIP) modules. The following sections in this guide describe how to manually add or edit Cisco ASA modules:

- Defining a CSC SSM in MARS
- Add Security Contexts Manually
- Edit Discovered Security Contexts

Step 6 Click **Submit**.

End of the procedure, "Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS"

What to Do Next

To enable NSEL on the MARS Appliance, go to the procedure, "Enabling NSEL Processing on the MARS Appliance"

Enabling NSEL Processing on the MARS Appliance

This procedure is valid only for the Cisco ASA, Version 8.1.x and 8.2.x

SUMMARY STEPS

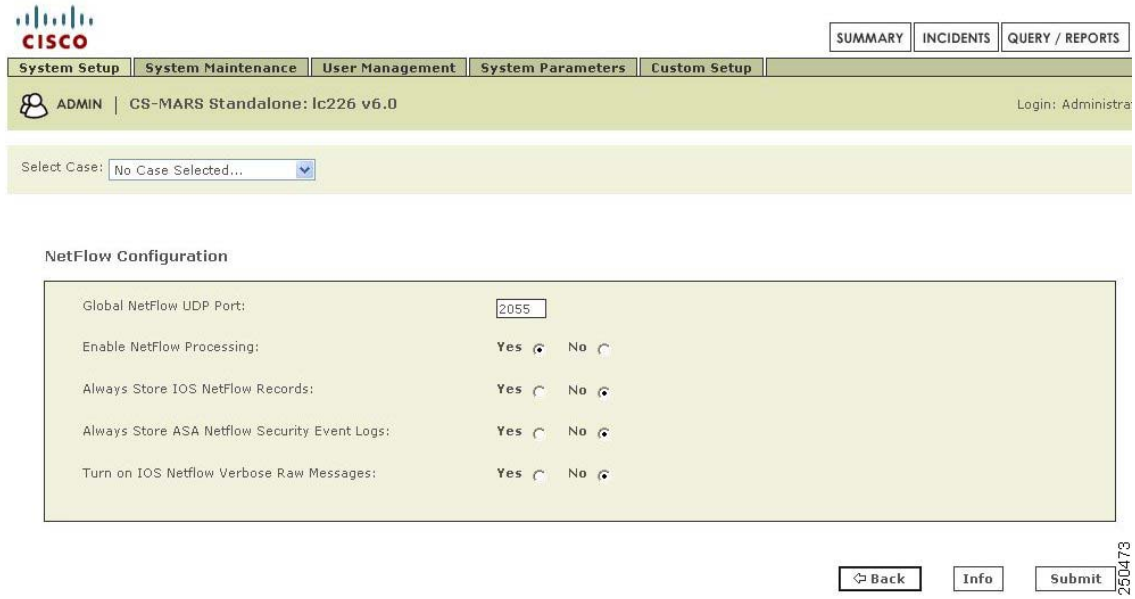
1. Navigate to Admin > System Setup > NetFlow Config Info.
2. Complete the configuration fields on the Netflow Configuration Page.
3. Click Submit.
4. Navigate to Admin > System Setup > Networks for Traffic Anomaly Detection.
5. Configure the Networks for Traffic Anomaly Detection Page
6. Click Submit.
7. Click Activate.

DETAILED STEPS

Before enabling NetFlow on MARS, you must enable NetFlow Security Event Logging on the Cisco ASA with MARS as the NetFlow collector. See–Configuring NSEL for MARS on the Cisco ASA 5580 later in this document.

Step 1 Navigate to **Admin > System Setup > NetFlow Config Info**. The NetFlow configuration page appears, as shown in Figure 20-2.

Figure 20-2 NetFlow Configuration Page (Admin > System Setup > NetFlow Config Info)



Step 2 Type the Cisco ASA NetFlow Security Event Logging port in the Global NetFlow UDP Port field. The default is 2055.

Note This value must match the value configured with the **ip flow-export destination** command on the ASA. Verify that you have enabled traffic on this port on all intermediate network devices between the ASA and MARS.

Step 3 Configure **Enable NetFlow Processing**.

- **Yes**—Configures MARS to process the NetFlow logs.
- **No**—Disables the processing of NetFlow data into the MARS.

Step 4 Configure **Always Store ASA Netflow Security Event Logs**.

- **Yes** —Enables MARS to use Cisco ASA Netflow Security Event Logs to do the following:
  - Topology-aware sessionization of NetFlow events with non-NetFlow events
  - Rule correlation and incident firing from NetFlow events
  - Retreival of NetFlow reported data using queries and non-scheduled reports
  - View incoming Netflow events with the Real-time Event Viewer
  - Configure drop rules against incoming NetFlow events
  - Use NetFlow-derived events in Scheduled reports results (For example, Top N reports)
- **No (default)**—Configures MARS to store only anomalies. MARS detects anomalies by using two dynamically generated watermarks comparing the previous data against current data. When the data breaches the first watermark, MARS starts to save that data. When the data rises above the second watermark, MARS creates an incident.

  No limits the use of Cisco ASA Netflow Security Event Logs to the following:
  - View incoming Netflow events with the Real-time Event Viewer
  - Configure drop rules against incoming NetFlow events

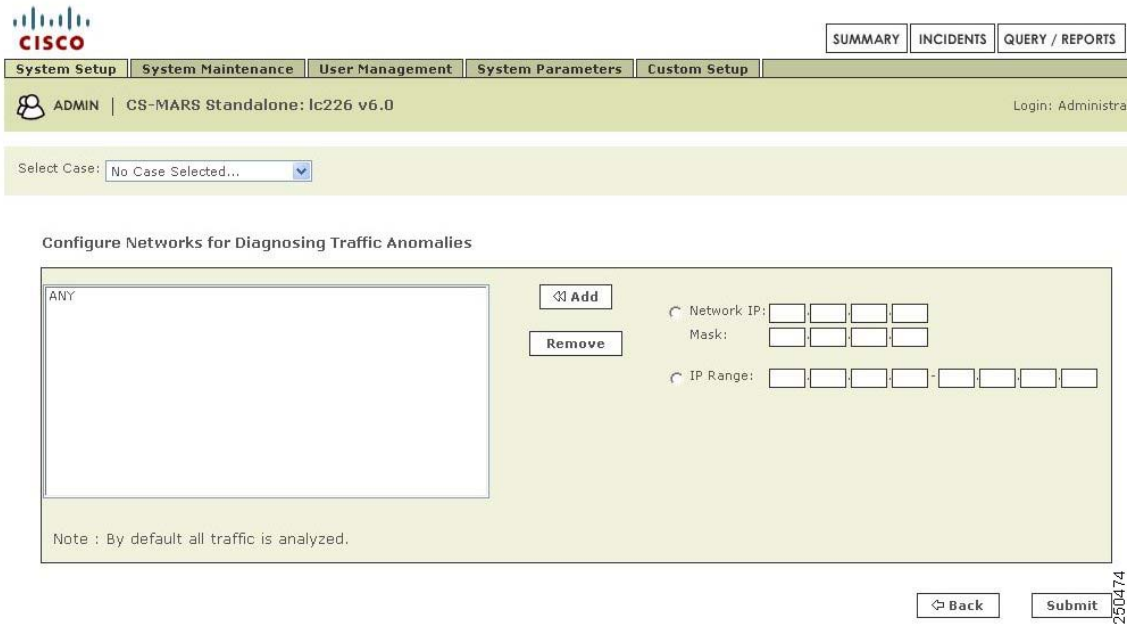
- Use NetFlow-derived events in Scheduled reports results (for stored incident data)

Step 5 Click **Submit**.

If you wish to restrict traffic anomaly processing to specific networks go to Step 6, otherwise go to Step 9. To restrict logging, configure drop rules as needed.

Step 6 Navigate to **Admin > System Setup > Networks for Traffic Anomaly Detection**.
The Configure Networks page appears, as shown in Figure 20-3.

Figure 20-3 Networks for Traffic Anomaly Detection Page (Admin > System Setup > Networks for Traffic Anomaly Detection)



Step 7 In the Configure Networks for Diagnosing Traffic Anomalies window, enter the addresses of networks you want to monitor and use the << Add button to add them.

- Specifying one or more networks causes MARS to generate NetFlow-based incidents that occur only on the specified networks. The default is to examine all data from all networks for anomalies. If the Local Controller is monitoring a specific zone (as defined by the Global Controller-Local Controller relationship), then this field should include only those networks for which this Local Controller is responsible. This interface restricts traffic anomaly processing for Cisco ASA NetFlow and Cisco IOS NetFlow.

Note To reduce the memory usage and increase performance of the appliance, you can configure MARS to profile hosts belonging to a set of valid networks.

Step 8 Click **Submit** to save your changes.

Step 9 To enable NetFlow processing by the MARS Appliance, click **Activate**.

Before MARS can start detecting anomalies based on NetFlow data, it must first develop a baseline for network behavior. It takes a full week, including the weekend, for MARS to develop a baseline. After a baseline is created, MARS can generate incidents based on NetFlow's anomaly detection.

Step 10 Verify NetFlow configuration by observing raw messages from the Cisco ASA with the MARS real-time event viewer.

End of Procedure, "Configuring NSEL for MARS on the Cisco ASA 5580."

What to Do Next

To enable NSEL on a Cisco ASA, Version 8.1.x, go to the procedure, "Configuring NSEL for MARS on the Cisco ASA 5580."

Configuring NSEL for MARS on the Cisco ASA 5580

For detailed information on configuring the Cisco ASA Security Appliance, see the section, Related Documents, later in this chapter.

Note The Cisco ASA interface to MARS in the following examples is configured as "cs-mars" with the Cisco ASA **name** command.

SUMMARY STEPS

1. configure terminal
2. ntp server
3. clear configure flow-export.
4. flow-export enable.
5. flow-export destination
6. flow-export template timeout-rate
7. logging flow-export-syslogs disable
8. logging trap 6
9. logging host
10. logging enable
11. exit
12. show running-config logging
13. show running-config flow-export

DETAILED STEPS

	ASA Command	Explanation
Step 1	**configure terminal** **Example:** asa# configure terminal	Enters Cisco ASA global configuration mode from privileged EXEC mode.
Step 2	**ntp server** *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**] **Example:** asa(config)# ntp server 171.68.10.80 key 1 source inside prefer	Configure an NTP server to ensure accurate time stamps. This enables better correlation by MARS because it ensures the time on both the ASA and MARS are the same.
Step 3	**clear configure flow-export** [*destination*] **Example:** asa(config)# clear configure flow-export 192.168.1.1	Clear the flow-export configurations associated with NetFlow data only for the specified IP adddress —in this example, previous configurations associated with the MARS IP address 192.168.1.1.
Step 4	**flow-export enable** **Example:** asa(config)# flow-export enable	Enable export of NetFlow security event log messages. When flow-export is enabled, the template records are sent to all configured NetFlow collectors. When disabled, any pending, cached NetFlow records are deleted from all collectors.
Step 5	**flow-export destination** *interface-name ipv4-address | hostname udp-port* **Example:** asa(config)# flow-export destination inside cs-mars 2055	Configure the Cisco ASA to export the flow cache entries to a destination system (MARS). The example configures the Cisco ASA interface on which the MARS appliance can be reached, the name associated with the IP address of the MARS appliance, and the UDP port on which MARS is listening for NetFlow traffic
Step 6	**flow-export template timeout-rate** *minutes* **Example:** asa(config)# flow-export template timeout-rate 1	Set the interval at which the template information is sent to NetFlow collectors. Use 1 minute for MARS.
Step 7	**logging flow-export-syslogs** {**enable | disable**} **Example:** asa(config)# logging flow-export-syslogs disable	Disable the redundant system log messages. The syslog messages report the same events as the NetFlow security event logging.
Step 8	**logging trap** [*logging_list | level*] **Example:** asa(config)# logging trap informational	Set the logging trap level to informational. You can also specify “6”.

	ASA Command	Explanation
Step 9	**logging host** *interface_name syslog_ip* **Example:** asa(config)# logging host cs-mars	Define MARS as a syslog server. The example sets the logging host to the user-defined IP address of the CS-MARS appliance using the name command on the ASA.
Step 10	**logging enable** **Example:** asa(config)# clear configure flow-export cs-mars_ip	Enable logging to CS-MARS
Step 11	**exit** **Example:** asa(config)# exit	Log out of global configuration mode into Priveleged Exec mode.

Step 12	**show running-config** [**all**] **logging** [**level** | **disabled**]
	Example:
	asa# show running-config logging
		Display the status of the system logs, for example:
		`ASA81-Single# show running-config logging`
		`logging enable`
		`logging monitor debugging`
		`logging host outside 10.2.3.58`
		`logging host outside 10.2.4.101`
		`logging host outside 10.2.4.113`
		`no logging message 106015`
		`no logging message 313001`
		`no logging message 313008`
		`no logging message 106023`
		`no logging message 710003`
		`no logging message 106100`
		`no logging message 302015`
		`no logging message 302014`
		`no logging message 302013`
		`no logging message 302018`
		`no logging message 302017`
		`no logging message 302016`
		`no logging message 302021`
		`no logging message 302020`

Step 13	**show running-config flow-export** [**destination** | **enable** | **template**]
	Example:
	asa# show running-config flow-export
		Display the status of the flow exports, for example:
		`ASA81-Single# show running-config flow-export`
		`flow-export destination outside 10.2.3.226 2055`
		`flow-export destination outside 10.2.3.42 2055`
		`flow-export template timeout-rate 1`
		`flow-export enable`

Additional References

The following sections provide references related to configuring the Cisco ASA Adaptive Security Appliances.

Related Documents

Related Topic	Document Title
Understanding NetFlow Anomaly Detection on MARS	User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x: http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/cfgOver.html#wp872012
All Cisco ASA 5500 Series Adaptive Security Appliances documentation	Cisco ASA 5500 Series Adaptive Security Appliancs Support Documentation http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
Cisco ASA 5580 command line interface explanations.	Cisco ASA 5580 Adaptive Security Appliance Command Reference (8.1, 8.2) http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/refgd.html http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html
Information on Syslog, SNMP, and NetFlow monitoring for the Cisco ASA.	Monitoring the Cisco ASA Security Appliance (8.1, 8.2): http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html#wp1099818 http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_syslog.html
Configuring NetFlow (NSEL) Collectors for the Cisco ASA 5580	Cisco ASA 5580 Implementation Note for NetFlow Collectors (8.1, 8.2): http://www.cisco.com/en/US/docs/security/asa/asa81/netflow/netflow.html http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html

CHAPTER 21

Check Point Devices

The Check Point security product family can be distributed and tiered. As such, you must understand the deployment method, components, and release versions of this product family, their relationships, and how MARS interacts with them. You must also understand the many acronyms and abbreviations associated with this product family. Table 21-1 lists the abbreviations and acronyms used in the topics that follow.

Table 21-1 Check Point Abbreviations and Acronyms

Abbreviation	Expansion	Additional Information
ASYMSSLCA	Secure Sockets Layer Certificate Authority using an asymmetric key cipher	Communications protocol used for establishing secure sessions.
CLM	Customer Log Modules	Standalone log server for collecting log data from the Check Point enforcement modules.
CMA	Customer Management Add-ons	A a virtual instance of SmartCenter and only exists within the context of a Provide-1/SiteManager-1 infrastructure.
CPMI	Check Point Management Interface	Communications protocol used for configuration discovery.
LEA	Log Export API	Communications protocol used for retrieving audit and firewall logs.
MDG	Multi Domain GUI	GUI used for managing Provider-1/ SiteManager-1 deployments. The MDG is the parent GUI that can launch specific SmartDashboard GUIs for a CMA.
MDS	Multi Domain Server	Is the umbrella manager for the CMA instances in a Provider-1/SiteManager-1 deployment.

Table 21-1 Check Point Abbreviations and Acronyms (Continued)

MLM	Multi Domain Log Module	Usually found in Provider-1/ SiteManager-1 deployments and provides the ability to create multiple instances of a CLM on a single logging server.
NG AI	Next Generation with Application Intelligence	All current trains of Check Point are released under the NG AI umbrella with specific release numbers, such as NG AI R55 and NG AI R60.
NG FP3	Next Generation Feature Pack 3	—
NGX	Next Generation eXtension	NGX is also NG AI R60
OPSEC	Open Platform for Security	An alliance, certification and integration methodology for products and solutions that integrate into a Check Point infrastructure.
P-1	Check Point Provider-1	—
SSLCA	Secure Sockets Layer Certificate Authority, using a symmetric key cipher (protocol)	—
SIC	Secure Internal Communication	—
SIC DN	SIC Distinguished Name	—
VIPs	Virtual IP Addresses	Usually used in a Provider-1/ SiteManager-1 deployment to assign unique IP addresses for CMA instances.
VPN-1	Check Point VPN-1 Pro and Edge	VPN-1 Pro is the Check Point enforcement gateway that does the inspection, firewalling, VPN encryption and QoS tagging. VPN-1 Edge is treated as a normal enforcement point.

To understand what MARS supports, we must first clarify the product terminology used by Check Point. NG refers to the 5.x product family, and it included three feature packs: FP1, FP2, and FP3. NG is different from NG AI in that NG AI improved upon, and renamed, the SmartDefense feature set that was introduced in NG FP2. NG AI also provides a larger number of application-aware inspections,; hence the name Application Intelligence. NG AI included releases R54 and R55. NGX refers to the 6.x product family and began with the R60 release.

MARS supports and has been tested with the following releases:

- NG FP3
- NG AI (R55)
- NGX (R60)

The different security platforms, Provider-1, SiteManager-1, SmartCenter, and SmartCenter Pro are bundles of the technologies released under the NG, NG AI, and NGX release trains. From this perspective, MARS works with any of the security platforms as long as it belongs to one of the supported release trains.

Check Point Provider-1 is a security management system for the managed security service providers (MSSP) and multi-site enterprises, respectively. Service providers are able to manage the Check Point gateways (firewall and VPN gateways) on their customer sites. The security policies and the system configurations are stored on the MDS. Each per-customer security policy is managed through a CMA, which also reside on the MDS. The Provider-1 system allows the service provider and the end customers to maintains separate log servers, using the MLM and CLM respectively. The user interface for Provider-1 is called the MDG. This system also support a tiered fault-tolerant configuration via redundancy at the gateway, CMA, or MDS level.

The Provider-1 system ensures secure and private communication between its components and Check Point gateways. Each CMA has its own internal certificate authority that issues certificates for secure communication between the CMA, log servers, and its own network. All communication between MDSs is authenticated and secured, and every MDS communicates securely with the CMAs that it houses.

The SiteManager-1 system operates much the same as Provider-1; however, it is targeted toward large enterprise customers. The Check Point components are the same as those found in Provider-1.

SmartCenter and SmartCenter Pro are security management systems also targeted toward enterprise customers. They can support the Provider-1 system, serving as a backup server at the CMA level. However, their primary function is to provide centralized security and VPN policy and security event management through SmartDashboard, which is the user interface for both systems. From the MARS perspective, SmartCenter has the ability to extend the view of the network by managing the policies and events associated with gateway and desktop nodes:

- VPN-1 perimeter security gateways,
- InterSpect internal security gateways
- Connectra Web security gateways
- SecureClient, a personal firewall running on desktops and servers.

MARS monitors the primary management servers, such as the MDS in Provider-1 and SiteManager-1 and the SmartCenter Server in SmartCenter and SmartCenter Pro. These management servers are where the actual security and audit policies are centrally managed and stored. If the Check Point deployment requires, MARS also monitors those components managed by the management stations, such as individual firewalls, VPN gateways, and log servers. Whether you configure MARS to monitor these remote components depends on whether their security event logs are propagated to the centralized management servers (SmartCenter or CMA). If the logs are not forwarded to the primary management server, then you must define where the log repository exists, whether local to the enforcement module, or forwarded to a separate logging module (CLM).

In addition to understanding the components, it is important to understand how Check Point components use Secure Internal Communications (SIC) to securely communicate with each other and with third-party OPSEC applications. SIC is the process by which MARS Appliance authenticates to the SmartCenter Server and other Check Point components. SIC uses a shared secret as the seed for negotiating session keys. This shared secret is referred to as an activation key. The authentication and communication setup works as follows:

1. Using a username and password pair, MARS authenticates to the SmartCenter Server and other Check Point components, such as remote log servers, using TCP port 18210.
2. If authenticated, the peers swap the activation key and each other's SIC using TCP port 18190.

3. If each peer validates the authenticity of the other, the Check Point component establish an encrypted session over TCP port 18184 with the MARS Appliance. It is over this channel that the Check Point components to sends encrypted log data to MARS.

The following topics support the integration of MARS into a Check Point environment:

- Determine Devices to Monitor and Restrictions, page 21-4
- Bootstrap the Check Point Devices, page 21-5
- Add and Configure Check Point Devices in MARS, page 21-18
- Troubleshooting MARS and Check Point, page 21-35

Determine Devices to Monitor and Restrictions

To configure Check Point devices, you must identify the central management server and managed components, bootstrap them, and add and configure them in the MARS web interface. The Check Point product line and release, as well as the number of devices managed, determines which tasks you must perform to configure MARS to monitor your Check Point devices.

Representing a Check Point device in MARS involve two steps:

1. **Define a primary management station.** This primary management station represents the central management server that manages remote components, such as firewalls, VPN gateways, and log servers.
2. **Define one or more child enforcement modules.** Child enforcement modules are the remote components managed by the primary management station. They represent firewalls, VPN gateways, and log servers.

When managing SmartCenter and SmartCenter Pro, the primary management station is the SmartCenter server. When managing Provider-1/SiteManager-1 releases NG FP3, NG AI (R55), and NGX (R60), the primary management station is not the MDS, but each CMA defined under the MDS. In other words, you must define each CMA as a separate primary management station. The child enforcement modules are those gateways and logs servers (CLMs) managed as part of that customer or site as defined by the CMA.

Part of what you must determine is where the security event logs are stored. Two options exist:

- **Central Event Correlation.** The MLM or SmartCenter server pulls logs from all remote components.
- **Distributed Event Correlation.** In addition to the MLM or SmartCenter Server, one or more remote log servers exist where aggregation to the central management server does not occur. These severs, the CLMs, must also be represented and configure so that MARS can pull the events from them.

If the security events are stored in a distributed fashion, you must plan to define and establish SIC communication between the MARS Appliance and each Check Point log module. For SmartCenter and SmartCenter Pro, the server SIC DN is the one assigned to the primary management station. However, for Provider-1 and SiteManager-1, the server SIC DN varies based on release. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), the server SIC DN is the one associated with the CMA. For Provider-1 and SiteManager-1 NGX (R60), you can use the SIC assigned to the MDS for all CMAs and CLMs that you define.

One other restriction exists with the Provider-1 and SiteManager-1 products. For Provider-1 and SiteManager-1 NG FP3 and NG AI (R55), you must define an OPSEC application representing the MARS Appliance in each CMA (using the CMAs SmartDashboard user interface). For Provider-1 and SiteManager-1 NGX (R60), you can define one OPSEC application representing the MARS Appliance and push that definition to all CMAs and CLMs managed by the MDS.

Bootstrap the Check Point Devices

Bootstrapping the Check Point devices involves preparing those devices to send data to the MARS Appliance, as well as enabling the MARS Appliance to discover the Check Point configuration settings. In addition to preparing the Check Point devices, you must gather the information required to represent the Check Point devices in the MARS web interface.

You bootstrap the central Check Point management server, whether it be a CMA or a SmartCenter server by defining the MARS Appliance as a target log host and OPSEC Application object.

1. Using Check Point SmartDashboard or the Check Point Provider-1/SiteManager-1 MDG, add the MARS Appliance as a host.
2. Create and install an OPSEC Application object for the defined host, import the authorization key, and generate the client SIC DN. This SIC DN is the one used by OPSEC applications, including the management server, to validate the MARS Appliance. You specify this client SIC DN in the MARS web interface. When a session is established between the MARS Appliance and the Check Point management server, the appliance publishes this SIC to the management server to ensure non-repudiation of the appliance.
3. Obtain the server SIC DN of the Check Point management server. You specify this sever SIC in the MARS web interface. The MARS Appliance validates the server SIC DN against the SIC published to the appliance by the management server during session setup. This validation ensures non-repudiation of the server.
4. Create the policies to permit SIC traffic between the defined host (MARS Appliance), the Check Point management server, and any remote servers. After you identify the devices, you must verify that the network services they use for SIC-based management and reporting are permitted on the reporting device. To enable these traffic flows, you must verify or update the policies that enable the SIC traffic to flow between each reporting device and the MARS Appliance. Once you have updated these policies, you must install the policies.
5. Define the log settings to push the correct events to the defined host. You must ensure that all of the security, firewall, user authentication, and audit events are logged and configured to be published to the MARS Appliance.
6. Install the policies. Once the policies are defined, you must update the Check Point components with the policies. Policy installation include an object database push that make the Check Point modules aware of the OPSEC Application representing the MARS Appliance. Without this step, the modules will not forward any log information via LEA.

To perform this task, you need a Check Point user account with administrative privileges. This account must be able to create a new host, define OPSEC application, define and install new policies, and access the settings of each managed Check Point component.

After completing this task, you should have collected the following information:

- The Client and server SIC DNs.
- If you are defining a CMA for Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), then you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS. Only Provider-1 and SiteManager-1 NGX (R60) requires the physical IP addresses of the MDS and MLM servers.
- Any CLMs, instead of CMAs, to which security logs are being sent. If logs are being sent to CLMs, LEA is only supported using clear text.

To bootstrap the Check Point devices, perform the following procedures:

- Add the MARS Appliance as a Host in Check Point, page 21-6
- Define an OPSEC Application that Represents MARS, page 21-7

- Obtain the Server Entity SIC Name, page 21-10
- Select the Access Type for LEA and CPMI Traffic, page 21-12
- Create and Install Policies, page 21-14
- Verify Communication Path Between MARS Appliance and Check Point Devices, page 21-15

Add the MARS Appliance as a Host in Check Point

Representing the MARS Appliance in Check Point enables the following supporting tasks:

- Generate a client SIC DN for the MARS Appliance.
- Define policies to allow SIC and syslog traffic between the Check Point components and the MARS Appliance.
- Direct log traffic to the MARS Appliance.

To define the MARS Appliance as a host, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

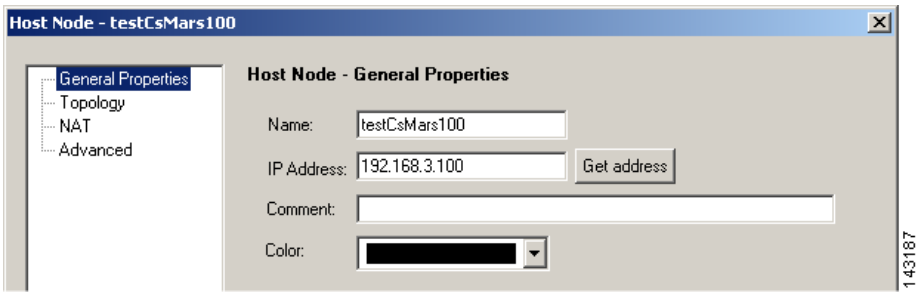
If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

Step 2 Select **Manage > Network Objects** from the main menu.

The Network Objects dialog box appears.

Step 3 Click the **New** button, and then select **Node > Host** on the menu list.

The Host Node dialog appears, with the General Properties settings selected.



Step 4 Enter the name MARS Appliance in the Name field of the General Properties page

Any Check Point policies defined to enable access or send logs to this appliance will reference the appliance by this name. Cisco best practice recommends using the actual hostname of the MARS Appliance.

Step 5 Enter the IP address of the monitoring interface in the MARS Appliance in the IP Address field.

Typically, the monitoring interface is eth0. However, if one or more intermediate gateways are applying NAT rules to the physical IP address, enter the IP address that is exposed to the Check Point central management server.

Step 6 Click **OK** to close the Host Node dialog box.

Step 7 Click **Close** to close the Network Objects dialog box.

The host representing the MARS Appliance is defined. You can now use this host when defining new policies in the Check Point user interface.

Step 8 Continue with Define an OPSEC Application that Represents MARS, page 21-7.

Define an OPSEC Application that Represents MARS

To integrate a third-party OPSEC application with Check Point components, you must define the application and associate it with the host on which the application is running. In addition to identifying this OPSEC application to the Check Point system, this procedure results in the generation of the client SIC DN for the MARS Appliance. Both the client SIC DN and the server SIC DN, obtained in Obtain the Server Entity SIC Name, page 21-10, are required to enable secure communications between the appliance and Check Point components.

This procedure also involves selecting an activation key, or shared secret, that is also required to enable the secure communications. You must record both the activation key and the client SIC DN for use when defining the Check Point devices in the MARS web interface.

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

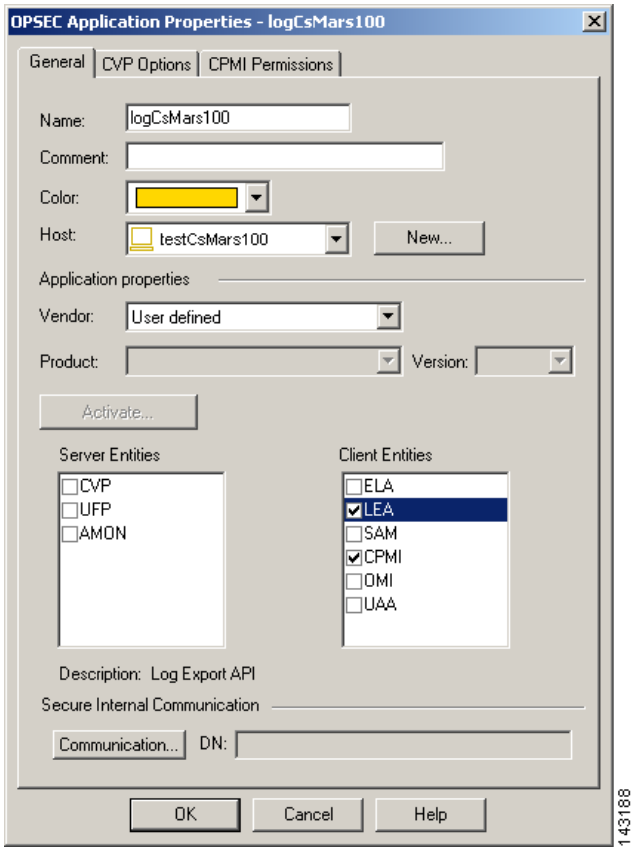
If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

Step 2 Select **Manage > Servers and OPSEC Applications** from the main menu.

The Servers and OPSEC Application dialog box appears.

Step 3 Click the **New** button, and then click **OPSEC Application** on the menu list.

The OPSEC Application Properties dialog box appears.



Step 4 Specify the name for this object in the Name field.

This value must be different from the name specified in ERROR: BROKEN STEPREF of Add the MARS Appliance as a Host in Check Point, page 21-6. Best practice recommends using the actual hostname of the host object plus some other descriptor, which combines for a unique name.

Step 5 In the Host list, select the host that you specified in ERROR: BROKEN STEPREF of Add the MARS Appliance as a Host in Check Point, page 21-6.

This OPSEC application definition is associated with the host that represents the MARS Appliance.

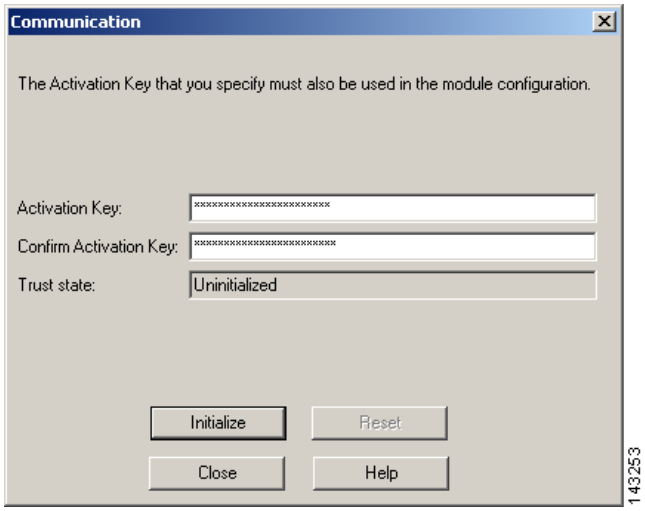
Step 6 Verify that **User defined** is selected in the Vendor field.

Step 7 Select the **LEA** and **CPMI** check boxes under Client Entities.

These values identify the OPSEC services required by the MARS Appliance.

Step 8 Click the **Communication** button under Secure Internal Communication.

The Communication dialog box appears.

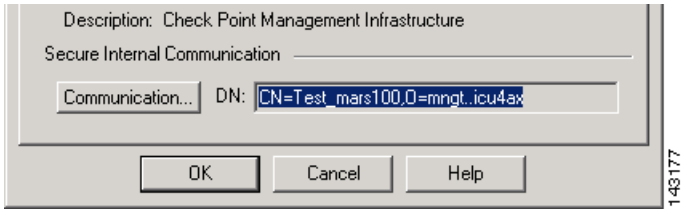


Step 9 Enter the activation key in the **Activation Key** and **Confirm Activation Key** fields of the Communication dialog box.

Note Remember this key for future use with MARS.

Step 10 Click **Initialize** to generate the client SIC DN.

The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.



Step 11 Click **Close** to close the Communication dialog box.

Step 12 Record the contents of the DN field that appears under Secure Internal Communication.

This value is used to populate the Client Entity SIC Name field of MARS in Add a Check Point Primary Management Station to MARS, page 21-19.

Tip If possible, you should cut and paste the **Secure Internal Communication DN** field value into an application, such as Notepad, for later use. Transcribing this field is error prone. Use a mouse to select the contents of read-only field, and then use **Ctrl+Insert** to copy the field to memory. You can paste the value using **Shift+Insert**. Be careful to avoid trailing spaces when you paste the value into MARS.

Step 13 Select the **CPMI Permissions** tab and verify that either **Administrator's credentials** or a permissions profile with administrative credentials is selected under Login to SmartCenter with.

Step 14 Click **OK** to close the OPSEC Application Properties dialog box.

Step 15 Click **Close** to close the Servers and OPSEC Application dialog box.

The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in Add a Check Point Primary Management Station to MARS, page 21-19.

Step 16 Select **Policy > Install Database** on the main menu.

This operation updates the remote Check Point components (child enforcement modules), such as CMAs, CLMs, log servers, and firewalls. It provides them with the authorization and credentials of the MARS Appliance, as an OPSEC component and SIC client.

Tip Using the Check Point log viewer, you can verify that the OPSEC object was pushed successfully.

Step 17 Continue with Obtain the Server Entity SIC Name, page 21-10.

Obtain the Server Entity SIC Name

The server SIC DN is one of the shared secrets used to provide non-repudiation during a secure communication between a Check Point component and the MARS Appliance. This value is used when defining a primary management station in MARS as defined in Add a Check Point Primary Management Station to MARS, page 21-19.

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX (R60), use the MDG.

Step 2 Select **Manage > Network Objects** on the main menu.

Step 3 Select **Check Points** in the Show list.

Step 4 Select the correct Check Point component in the Network objects list.

Which Check Point component you select depends on which SIC you need and what Check Point system you are using. Specifically, you want to obtain SICs for:

- Each management server to discover configuration settings via CPMI.
- Each management server to which logs are forwarded by remote components.
- Each remote log server that does not forward logs to a central management server, either the MDS or a SmartCenter.

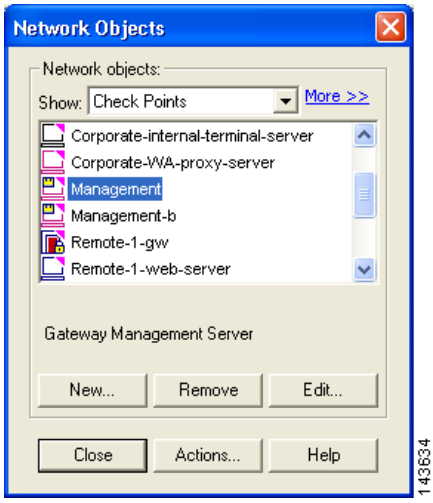
Management servers are the following devices:

- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CMA of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.
- The MDS of a Provider-1 or SiteManager-1 NGX (R60) installation.

Log servers are the following devices:

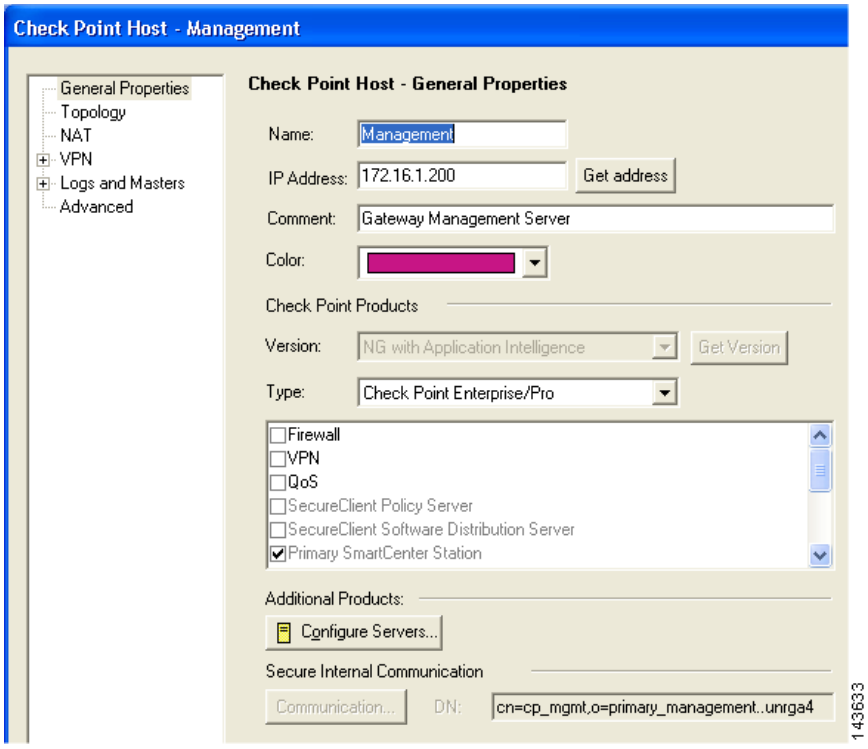
- SmartCenter server for standalone SmartCenter and SmartCenter Pro installations.
- Each CLM of a Provider-1 or SiteManager-1 NG FP3 or NG AI (R55) installation.

- The MLM of a Provider-1 or SiteManager-1 NGX (R60) installation.



Step 5 Click **Edit**.

The Check Point Host - Management dialog box appears, with the General Properties page selected.



Step 6 Record the value defined in the DN field under Secure Internal Communication.

This value is used to populate the Server Entity SIC Name field of MARS in either Add a Check Point Primary Management Station to MARS, page 21-19, Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23, or Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29.

Step 7 Click **OK** to close the Check Point Host dialog box.

Step 8 For each additional management or log server in this Check Point installation, select that device in the Network Objects list, and repeat Step 5 through Step 7.

Step 9 Click **Close** to close the Network Objects dialog box.

Step 10 Continue with Select the Access Type for LEA and CPMI Traffic, page 21-12.

Select the Access Type for LEA and CPMI Traffic

Check Point devices use special access types for configuration discovery and event log queries. For configuration discovery, the protocol is CPMI. For event log queries, the protocol is LEA. Each of these protocols has specific configurable attributes, including whether to use bulk encryption, what cipher to use, and what port to use for communications.

You must understand what the supported settings are so that you can verify the Check Point devices are configured correctly. MARS supports only three of the available Check Point authentication mode:

- **CLEAR**—Indicates that the traffic is neither authenticated nor encrypted.
- **SSLCA**—Indicates that the communications need to be authenticated and encrypted using an symmetric key cipher.
- **ASYMMSSLCA**—Indicates that the communications need to be authenticated and encrypted using an asymmetric key cipher.

These access protocols are configured as follows:

Note Typically, the default values should be used unless your Check Point deployment includes CLMs.

- ***<service>*** auth_port <*port_number*>

  This line is required in the fwopsec.conf file. The *service* value is either **LEA_SERVEAR** or **CPMI_SERVER**. Two possible values exist for *port_number*: **0**, which indicates an the server is not listening for authenticated session requests, and the port number of an authenticated and/or encrypted protocol. If the *port_number* value is 0, you must configure the server to listen for session requests in CLEAR mode on a valid port using the settings.

- ***<service>*** auth_type <*cipher*>

  The *service* value is either **LEA_SERVER** or **CPMI_SERVER**. Two possible values are supported for *cipher*: **sslca** for authentication and encryption using a symmetric key cipher, or **asym_sslca** for authentication and encryption using an asymmetric key cipher. If the **auth_port** setting is set to 0 (zero) for this service, then you do not need to specify the auth_type in the fwopsec.conf file. You can comment out this line.

- ***<service>*** port <*port_number*>

  This line is required in the fwopsec.conf file. The *service* value is either **LEA_SERVER** or **CPMI_SERVER**. The value for *port_number* must match the port number on which the desired network service listens. A *port_number* of **0** (zero) indicates that log server is not listening in CLEAR mode.

  If it is some other number, then any service can come pull the logs without authenticating. For LEA_SERVER, you cannot use port 18184, as it is used for encrypted log communications. For CPMI_SERVER, you cannot use port 18190**.** When CLEAR is enabled, authentication is disabled

for this port. Any host with access to the Check Point component at this port can pull logs. If you chose to enable CLEAR, which is less expensive in terms of overall transaction costs, you define policies that restrict access to the MARS Appliance and other know management hosts.

Note Prior to MARS 4.1 and when using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), you could not use SSLCA mode for log retrieval by the MARS Appliance. Instead, you were required to configure each CMA and CLM to accept LEA session requests using CLEAR mode. It was unnecessary to configure the LEA settings for the MLM.

The following example indicates that LEA is using ASYMSSLCA-based authentication connecting over port 18184 (default), the traffic is encrypted via SSL, and the log server is not listening for requests in cleartext.

```
LEA_SERVERauth_port18184
LEA_SERVERauth_typeasym_sslca
LEA_SERVERport0
```

The following example indicates that the log server is listening for requests in cleartext at port 18187. Such requests will be serviced and the sessions will be neither authenticated nor encrypted.

```
LEA_SERVERport18187
```

Check Point uses the following default settings:

- For LEA, SSLCA is the authentication method and communications occur over TCP 18184.
- For CPMI, SSLCA is the authentication method and communications occur over TCP 18190.

To review or change the access type settings, follow these steps:

Step 1 Log on to the Check Point server.

For Provider-1 and SiteManager-1, this server is the MDS, MLM, or CLM. Otherwise, it is the SmartCenter server.

Step 2 Open the fwopsec.conf file found in the subdirectory for each CMA and CLM.

The following example uses the find command to locate the file. Customer1 identifies the CLM.

```
[Expert@logger]# find . -name "fwopsec.conf" -print
./var/opt/CPfw1-R55/conf/fwopsec.conf
./var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf/fwopsec.conf
[Expert@logger]# cd /var/opt/CPmds-R55/customers/Cust1Log/CPfw1-R55/conf
```

Step 3 Using a text editor, such as vi or Notepad, edit the fwopsec.conf file and modify the LEA and CPMI communication settings as needed.

Step 4 Save your changes to the file.

Step 5 Repeat Step 2 through Step 4 for each CLM and CMA.

Step 6 Restart the Check Point server after the changes are made.

The CPMI and LEA servers are restarted, which reloads their configuration information, and ensures they are listening to the correct ports for session requests.

Step 7 Continue with Create and Install Policies, page 21-14.

Create and Install Policies

You must create firewall policies that permit the MARS Appliance to access the relevant ports of the Check Point central management server and any remote log servers. The default ports are as follows:

- **TCP port 18190**—Used by CPMI to discover configuration settings.
- **TCP port 18210**—Used to retrieve the certificate from the Certificate Authority on the SmartCenter, MDS, MLM, CMA, or CLM.
- **TCP port 18184**—Used to pull security event logs from the log servers, such as the MLM or CLM.

However, you must use the CPMI and LEA servers settings specified in Select the Access Type for LEA and CPMI Traffic, page 21-12. When the policies are defined, you must install them on any firewall modules that inspect traffic between the Check Point components and the MARS Appliance.

If the management server has a Check Point firewall installed, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

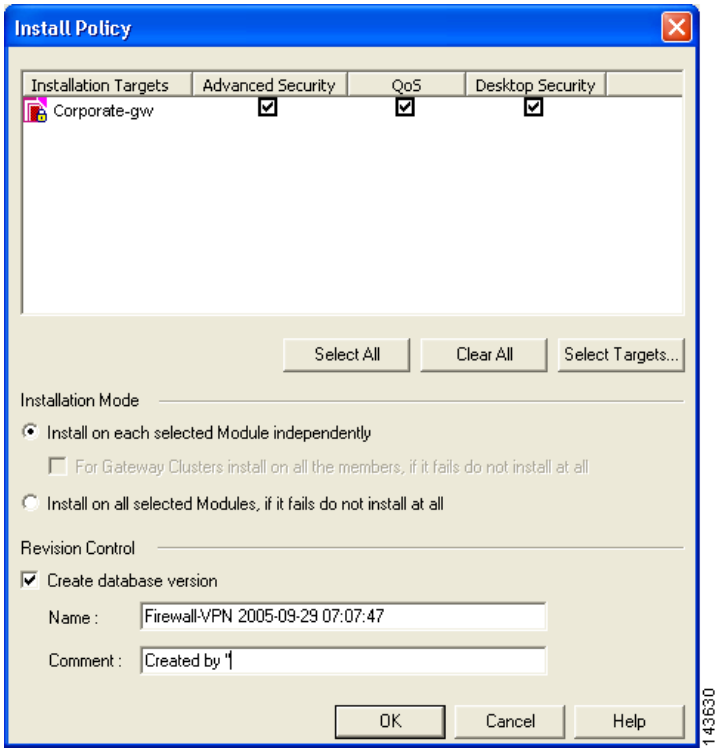
Step 2 If Check Point firewall components reside between the Check Point components (central management and log server) and the MARS Appliance monitoring those components, define the security policies that allow management and log traffic between those devices.

If you have enabled CPMI discovery, the service condition must include CMPI. To enable the log access, the service list must include FW1_lea.

Step 3 Verify that the security policies are set to log.

The Track column of each rule should display the Log action. To enable logging, right-click the **Track** field of a rule and select **Log** on the shortcut menu.

Step 4 Once you have defined the security policies that enable traffic flows between the Check Point and MARS components, select **Policy > Install** on the main menu.



Step 5 In the Install Policy dialog box, verify the **Advanced Security** check box is selected for each selected installation target.

The target devices should be those firewalls that reside between the Check Point components and the MARS Appliance.

Step 6 Click **OK** to install the policies on the selected devices.

The security policies on the target firewall devices are updated, enabling CPMI and LEA traffic flows between the Check Point components and the MARS Appliance.

Tip Using the Check Point log viewer, you can verify that the policies were installed successfully.

Verify Communication Path Between MARS Appliance and Check Point Devices

You should verify that the MARS Appliance can reach the Check Point devices, including the SmartCenter server and the remote log servers. Use the **telnet** command at CLI of the MARS Appliance to verify access to the SmartCenter server and log servers. The ports to check are defined in For more information on accessing the CLI, see Establishing a Console Connection of the *Cisco Security MARS Initial Configuration and Upgrade Guide*.

The command syntax is as follows

telnet <*ip_address*> *<port_number>*

If you are unsuccessful, verify the settings of the ports for each Check Point component and verify that no firewalls are blocking the traffic. For more information on **telent** of the *Cisco Security MARS Command Reference*.

Reset the OPSEC Application Certificate of the MARS Appliance

If you encounter an error when pulling the certificate as part of defining the Check Point devices in the MARS web interface, you must reset the certificate before you can attempt to pull it again. This procedure details how to reset the certificate, or SIC, associated with the OPSEC Application that is associated with the host that represents the MARS Appliance.

To reset the OPSEC application certificate, follow these steps:

Step 1 Log in to the correct Check Point user interface using an account with administrative privileges.

If you are using SmartCenter, use the SmartDashboard for that server. If you are using Provider-1 or SiteManager-1 NG FP3 or NG AI (R55), use the SmartDashboard of the CMA. If you are using Provider-1 or SiteManager-1 NGX, use the MDG.

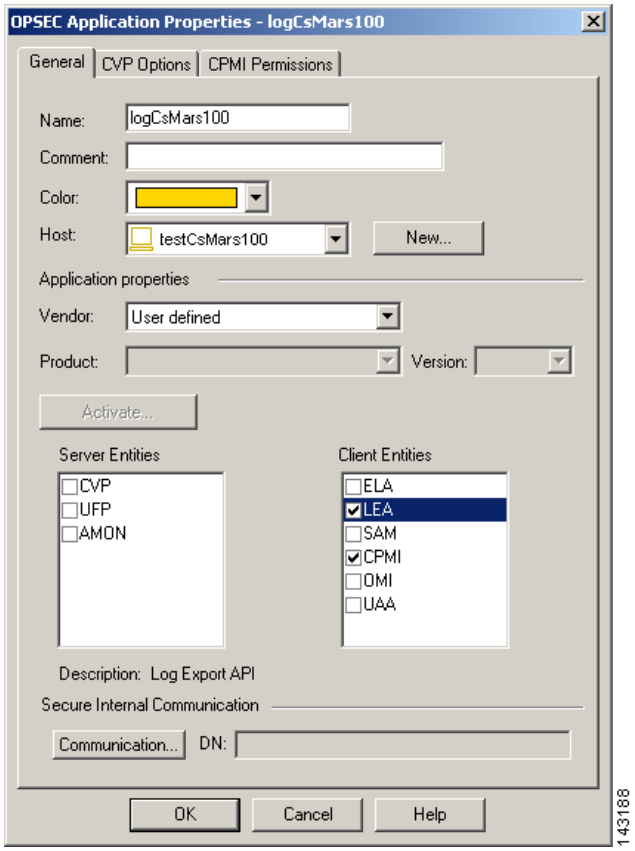
Step 2 Select **Manage > Servers and OPSEC Applications** from the main menu.

The Servers and OPSEC Application dialog box appears.

Step 3 Select **OPSEC Applications** in the Show list.

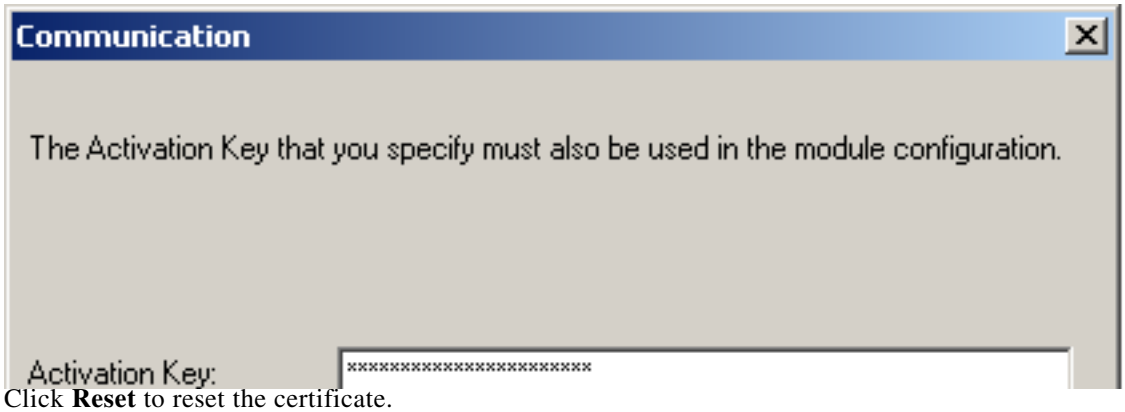
Step 4 Select the OPSEC application that represents the MARS Appliance in the Servers and OPSEC Applications list, and click **Edit**.

The OPSEC Application Properties dialog box appears.



Step 5 Click the **Communication** button under Secure Internal Communication.

The Communication dialog box appears.



Step 6 Click **Reset** to reset the certificate.

Step 7 Click **Close** to close the Communication dialog box.

The client SIC DN is generated and the Communication dialog box closes, returning to the OPSEC Application Properties dialog box. The new SIC appears in the DN field.

Step 8 Click **OK** to close the OPSEC Application Properties dialog box.

Step 9 Click **Close** to close the Servers and OPSEC Application dialog box.

The OPSEC Application that represents MARS is defined and associated to the correct host. You also have obtained the activation key and client SIC DN for later use in Add a Check Point Primary Management Station to MARS, page 21-19.

Add and Configure Check Point Devices in MARS

After you identify and bootstrap the Check Point reporting devices and install the policies that enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices. When adding a Check Point device, you add two types of devices:

- **Primary management station.** The primary management station represents the SmartCenter server or CMA that manages other Check Point components. In the web interface, the bases module is defined as a software application (Check Point Management Console application) running on a host.
- **Child enforcement module.** A child enforcement module is a Check Point component, a firewall or log server, that is managed by a primary management station. When viewing the Security and Monitoring Devices list, child enforcement modules appear as children of the hosts that are running the primary management station.

With these definitions in mind, adding and configuring the Check Point device involves the following:

1. Define a host that represents the Check Point primary management station, specifying the hostname and management and reporting IP addresses.
2. Define all of the interfaces of the host.
3. Add the correct Check Point software application to the host. This application represents the primary management station.
4. Specify the communication settings for the primary management station. These settings include identifying which access types are allowed (CPMI, LEA or both) and the authentication type and port to use for each supported access type.
5. (Optional) Define the settings for secure communications. If the access communication are not conducted in CLEAR, then you must specify the client and server SIC DNs and identify the certificate authority.
6. (Optional) Define the routes used by the firewall running on the primary management station. If a firewall is running on the primary management station, the route information is required to enable the path analysis and mitigation features of MARS.
7. Discover the child enforcement modules and the configuration settings of the primary management station. Discovery of child enforcement modules includes any log servers and firewalls managed by the primary management station. MARS discovers configuration settings, such as policies, NAT, modules, and clusters, as well as event information, such as traffic logs, SmartDefense events, and user authentication events.
8. Configure the discovered log servers. To configure these log servers, select the Self option from the Log Info page associated with each server, and specify the access type settings.
9. Define any log servers not managed by the primary management station. These servers are used by one or more of the firewalls that were discovered or by the primary management station.
10. Edit each firewall child enforcement module to select a log server.
11. (Optional) Specify an SNMP RO community string for each firewall child enforcement module for which resource utilization monitoring is desired.

12. (Optional) Define the routes used by each firewall child enforcement module. Route information is required to enable the path analysis and mitigation features of MARS.
13. Click Activate in MARS.

To add a Check Point device in MARS, you must perform the following procedures:

- Add a Check Point Primary Management Station to MARS, page 21-19
- Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23
- Edit Discovered Log Servers on a Check Point Primary Management Station, page 21-27
- Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29
- Verify Connectivity Between MARS and Check Point Devices, page 21-34

If discovery of Check Point configuration settings is not enabled for MARS, you must perform the following manual configuration procedures:

- Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23
- Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31

Before You Begin

To perform this procedure, you need the following information:

- A MARS account with Administrative privileges.
- A Check Point CMA or SmartCenter username and password that has READ access (minimum requirement).
- The client and server SIC DNs.
- If you are defining a CMA for Provider-1 or SiteManager-1, you must have the virtual IP address (VIP) for each CMA and CLM managed by the MDS.

Add a Check Point Primary Management Station to MARS

The primary management station represents one of the following:

- The SmartCenter server in a SmartCenter or SmartCenter Pro installation.
- A CMA of a Provider-1 or SiteManager-1 installation.

Note Check Point 4.1, NG FP1, and NG FP2 devices are not officially supported. They cannot be configured to retrieve configuration information using CPMI. However, they can be configured to retrieve logs using LEA. To configure one of these devices to work with the MARS, leave the Access IP field blank on the host that represents the base platform.

You must define each individual CMA of a Provider-1 or SiteManager installation, regardless of the release and version.

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

Step 2 Do one of the following:

- Select **Add SW Security apps on a new host** from the Device Type list, and continue with Step 3

- Select **Add SW security apps on existing host** from the Device Type list. Select the device to which you want to add the software application and click **Add**. Continue with Step 7.

Step 3 Specify values for the following fields:

- **Device Name**—Enter the name of the device. This name must exactly match the hostname shown in the Check Point user interface. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station in the Security and Monitoring Device list.
- **Access IP**—(Optional) This s address is used to pull from a Check Point device using CPMI, enabling MARS to discover settings from this device. This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the access IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 1-10.
- **Reporting IP**—Enter the IP address of the interface in the Check Point server from which MARS will pull traffic and audit logs. Check Point audit logs save information regarding user interaction with Check Point devices, such as log in and out of the Check Point user interface, initialize or revoke certificate, install or uninstall policy, create, modify, and delete objects, etc. No additional configuration is needed to turn on audit log on Check Point device.

  This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. 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 4 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface in the Check Point server from which configuration information will be discovered and from which security event logs will be pulled.

This address represents either a virtual IP address associated with a CMA or the physical IP address of the SmartCenter server. To learn more about the interface settings, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 1-10.

Step 5 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

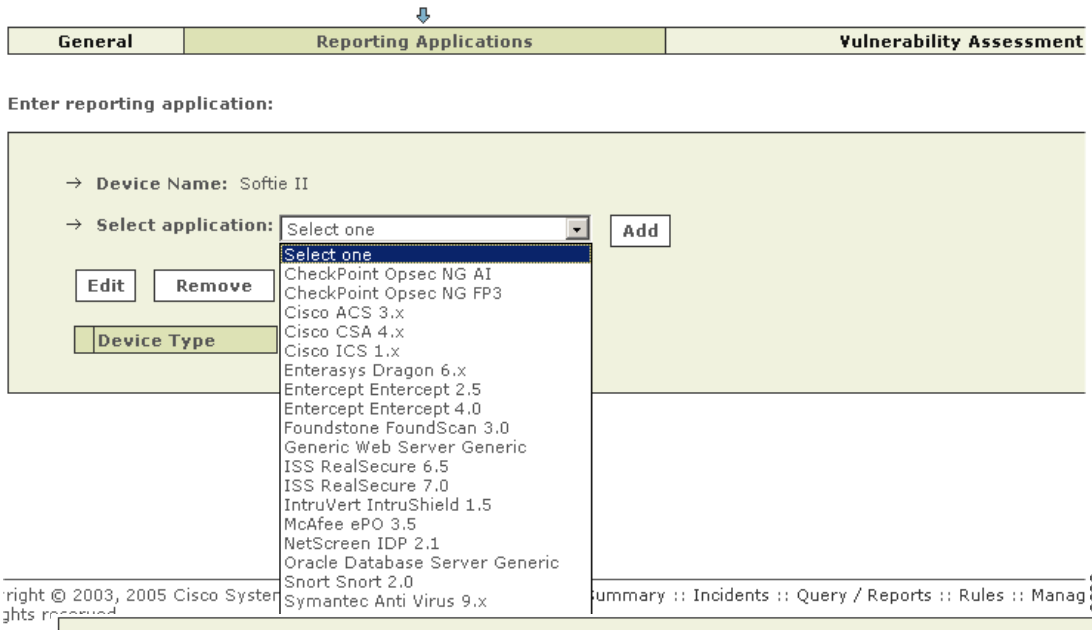
Step 6 Click **Apply** to save these settings.

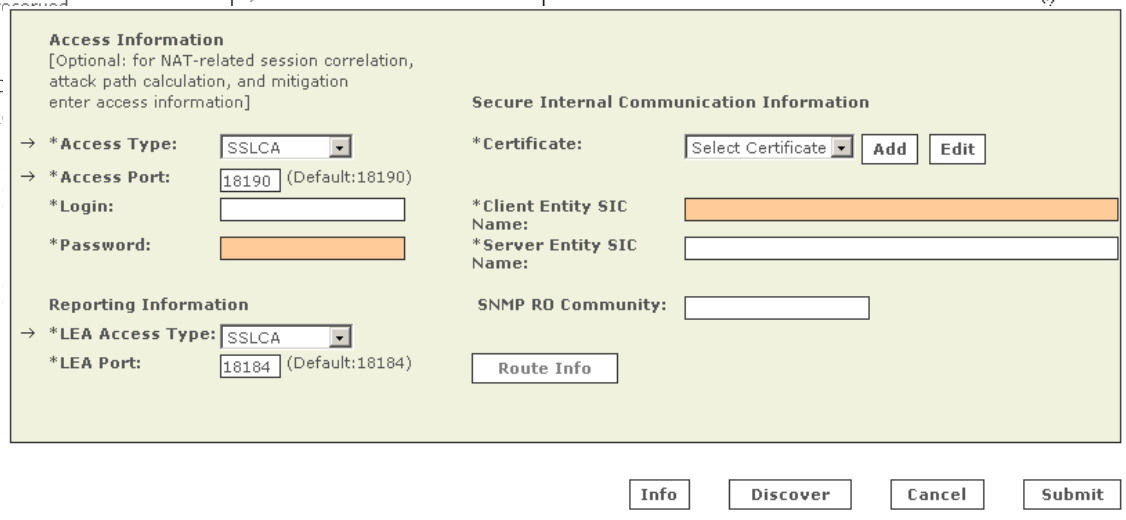
Step 7 Click **Next** to access the Reporting Applications tab.

Step 8 Select the appropriate version of Check Point Opsec from the Select Application list, and click **Add**.

The following options are available:

- **CheckPoint Opsec NG FP3**—Select this option for Check Point NG FP3 devices.
- **CheckPoint Opsec NG AI**—Select this option for Check Point NG AI (R55) devices.
- **CheckPoint Opsec NGx**—Select this option for Check Point NGX (R60) devices.





Step 9 If yc
stati

-
-

- **Login**—Identifies the Check Point administrative account to be used to discover configuration settings.
- **Password**—Identifies the password asscociated with the Login account.

Step 10 Specify values for the following fields:

- **LEA Access Type**—If a log server is running on this primary management station select **ASYMSSLC**, **CLEAR**, or **SSLCA**. You must have entered an address in the Reporting IP field on the host that represents this primary management station. This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 21-12.
- **LEA Port**—Verify that the port number corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 21-12.

Step 11 If this device uses SSLCA or ASYMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip toStep 12.):

- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 21-26.
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 21-7.
- **Server SIC Name**—Enter the SIC DN for this primary management station. This value was obtained in Obtain the Server Entity SIC Name, page 21-10. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 12 (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 on host that represents the primary management station and you must configure the Access Information settings on the primary management station. MARS uses the SNMP RO string to perform resource utilization monitoring. Currently, it is not used for configuration or log discovery.

Step 13 (Optional) To enable MARS to monitor this device for anomalous resource usage, select **Yes** from the Monitor Resource Usage list.

Before you can enable this feature, you must provide a SNMP RO Community string.

MARS monitors the device for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports. For more information, see Configuring Resource Usage Data, page 1-21.

Step 14 (Optional) To specify the route information for a firewall running on this primary management station, continue with Define Route Information for Check Point Firewall Modules, page 21-29.

Step 15 (Optional) If you defined an access IP and selected and configured an access type, click Discover to determine the device settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Note Sometimes, the discovery operation times out, in which case you should try again. At other times, a message appears that states the discovery is taking a long time and that you should proceed to performing other tasks in MARS.

Step 16 To add this device to the MARS database and continue adding firewall modules manually, 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 17 Do one of the following:

- To manually define the child enforcement modules that are managed by this primary management station, continue with Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23.
- To edit the settings of the discovered child enforcement modules, continue with Edit Discovered Firewall on a Check Point Primary Management Station, page 21-29.

Step 18 Click **Activate**.

Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station

If you have not enabled configuration discovery on the primary management station or if one or more of the managed firewalls uses a log server that is not managed by the primary management station, you can manually define firewalls or log servers. Your goal should be to represent all of the firewalls managed by this primary management station and all log servers used by those firewalls and the primary management station. While MARS does not discover configuration settings of the firewalls, it uses the defined information to discover topology, calculate attack paths, and identify preferred mitigation points in the network.

For example, if you are defining a primary management station that represents a CMA, you must define the CLM associated with that CMA. Any firewalls managed under that CMA may either act as their own log servers, publish information to the CLM, or publish information to a MLM. In the case of the later, you must define that relationship by defining the firewalls and then specifying which log servers pull their traffic and audit logs. First, however, must also define the MLM settings, as it is a log server that external to the perspective of the CMA, and it cannot be referred by a firewall until it has been defined. The CLM, however, would be considered part of the CMA (assuming the reporting IP and LEA settings are specified), so you would not define a separate child enforcement module to represent it. Instead, you would select the Management option in the Log Info dialog for firewalls that use the CLM as their log server. For more information on selecting the log server option, see Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31.

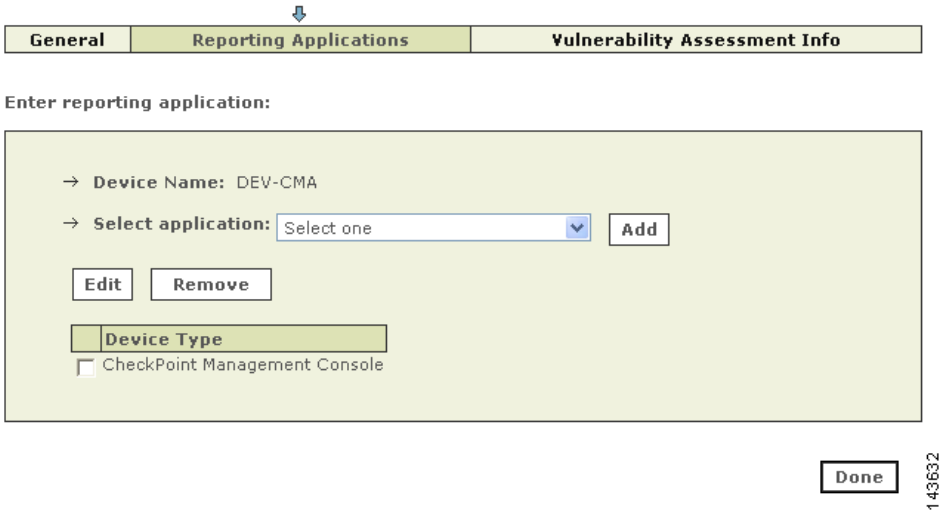
To manually define a child enforcement module that is managed by the primary management station or a log server to which either the primary management station or a child enforcement module publishes its audit and security logs, follow these steps:

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

Step 2 From the Security and Monitor Devices list, select the host that represents the primary management station and click **Edit**.

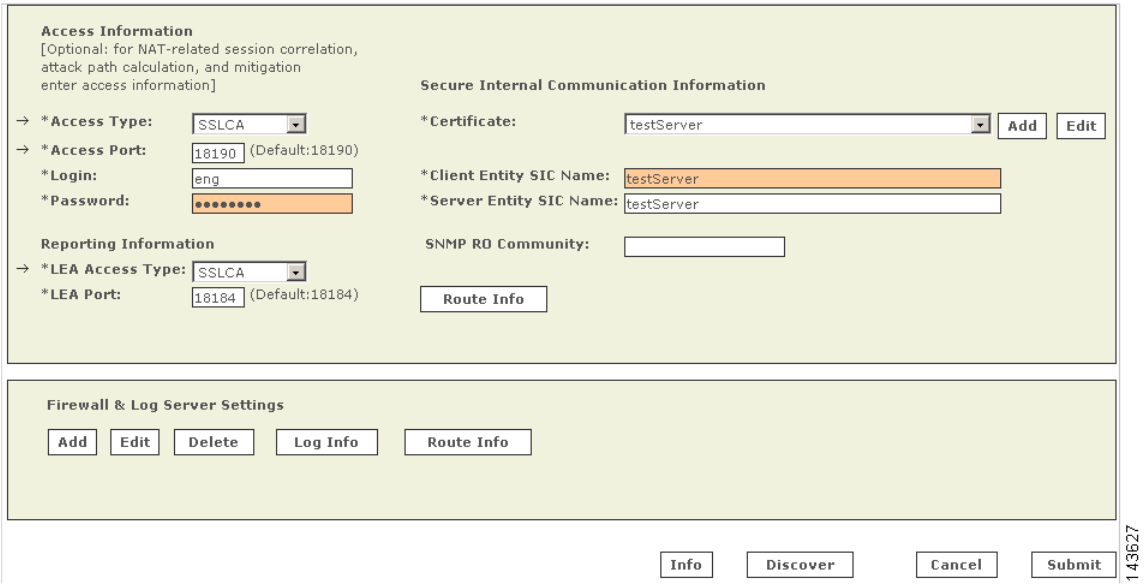
Such devices have CheckPoint Management Console as an entry in the Device Type column.

Step 3 Click **Next** to access the Reporting Applications tab.



Step 4 Select the **CheckPoint Management Console** check box in the Device Type list and click **Edit**.

The Access Information page appears.



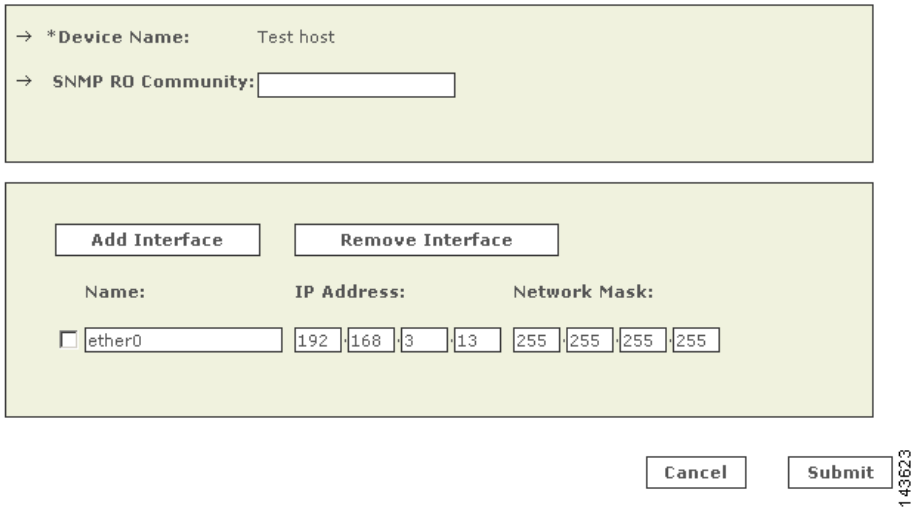
Step 5 Click **Add** under Firewall & Log Server Settings.

The list of available hosts appears.

Step 6 Do one of the following:

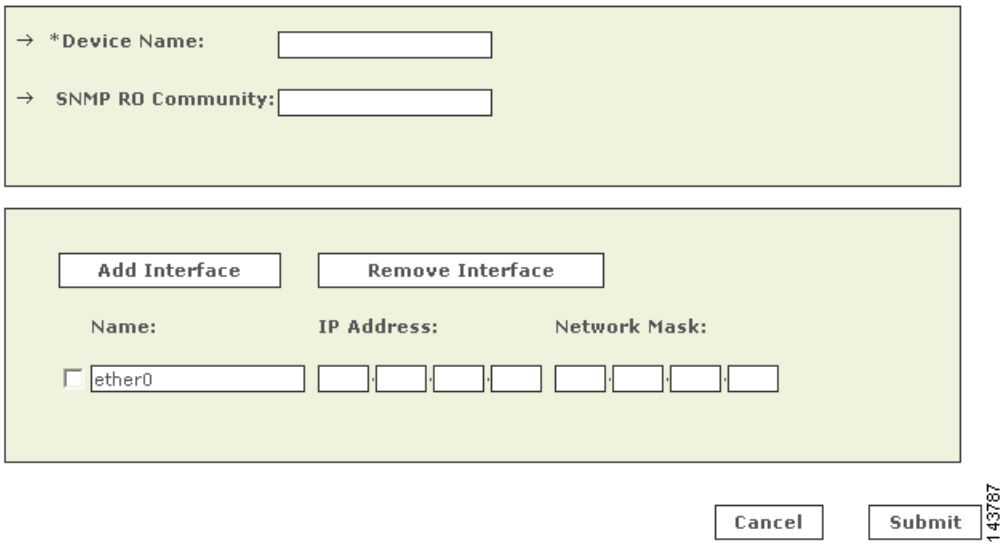
- Select the host on which the child enforcement module is running, click **Change Existing**, and continue with Step 7

  Result: A page with a read-only device name appears, prompting you to specify the SNMP RO Community string.



- Click **Add New** to define a new host, and continue with Step 7

  Result: A page appears, prompting you to specify device name and SNMP RO Community string.



Step 7 Enter the name of the child enforcement module or log server in the **Device Name** field.

MARS maps this name to the IP address specified in the interfaces. This name is used in topology maps, queries, and appears in the Children column of the base Check Point module in the Security and Monitoring Device list.

Step 8 (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module'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 on host that represents the primary management station. 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 9 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface installed in the child enforcement module or log server.

These interfaces include the ones from which the configuration information will be discovered and security event logs will be pulled. To learn more about the interface settings, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 1-10.

Step 10 Click **Submit** to add this module to the primary management station.

Step 11 (Optional) To specify the route information for a firewall child enforcement module, continue with Define Route Information for Check Point Firewall Modules, page 21-29.

Step 12 If the child enforcement module does not propagate its logs to the primary management station or if you are defining a log server that is not managed by this primary management station, you must specify where its logs are stored. Continue with Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31.

Step 13 Repeat Step 5 through Step 12 for each child enforcement module that is managed by this primary management station and each log server that is used by the primary management station or child enforcement modules.

Step 14 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 15 Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.

Step 16 Click **Activate**.

Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

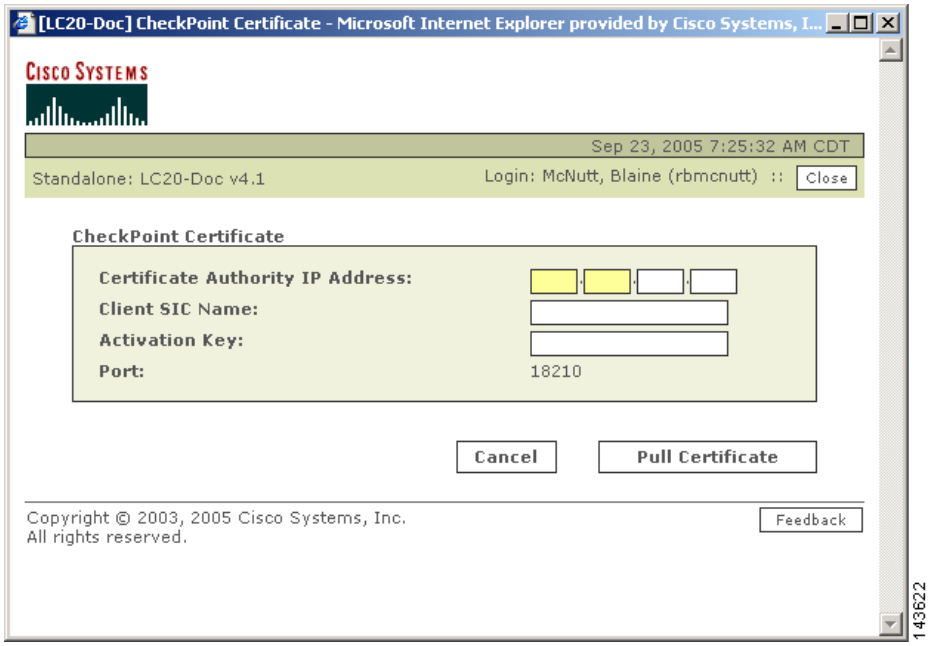
Add a Check Point Certificate Server

When defining a Check Point module that uses secured communications, you must identify the certificate sever that authenticates the SICs provided by the client and the server. Typically, a SmartCenter server or the CMA has its own certificate server, however, your configuration may use a central server. If that is the case, you must define the certificate server as part of a defining a base or child enforcement module.

Note This procedure assumes you have been refer to it, and that you are in the middle of defining a primary management station or child enforcement module.

To define a certificate server, follow these steps:

Step 1 Click **Add** to define the settings for the certificate authority.



Step 2 Specify values for the following fields:

- **Certificate Authority IP Address**—Typically, this IP address is the physical IP address of the SmartCenter server or the virtual IP address of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this IP address represents the physical IP address of the MDS that manages the CMA.
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 21-7.
- **Activation Key**—This value was also provided in Define an OPSEC Application that Represents MARS, page 21-7.

Step 3 Click **Pull Certificate**.

A message box appears stating “Discovery is done.”

A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see Reset the OPSEC Application Certificate of the MARS Appliance, page 21-16.

Step 4 Click **Close**.

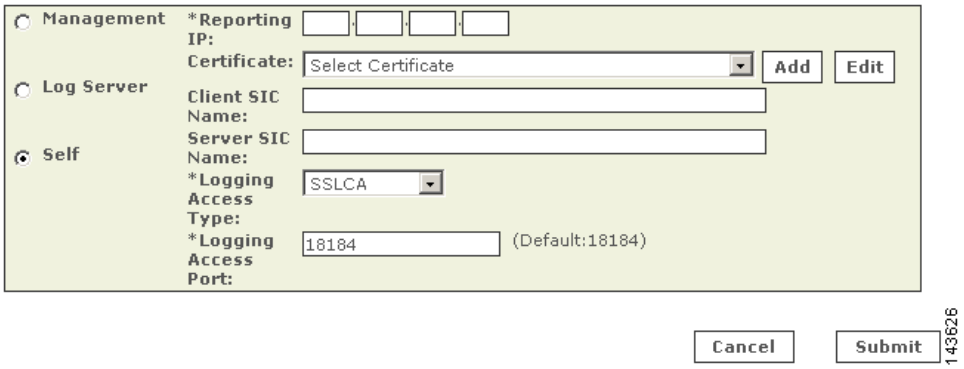
Edit Discovered Log Servers on a Check Point Primary Management Station

After performing a discovery operation, you must edit each discovered log servers. The purpose of editing this log server is to identify that it is its own log server and to provide the SIC communication settings.

To edit a discovered log server, follow these steps:

Step 1 Under Firewall & Log Server Settings, select the check box next to the desired log server, and click **Log Info**.

Step 2 Select **Self**.



Step 3 Specify values for the following fields:

- **Reporting IP**—Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 1-10.
- **Logging Access Type**—This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select ASYMSSLC, CLEAR, or SSLCA, For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 21-12.
- **Logging Port**—Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the fwopsec.conf file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 21-12.

Step 4 If this log server uses SSLCA or ASYMSSLCA as an authentication method, specify values for the following fields (Otherwise, the authentication method is CLEAR. Skip to Step 5):

- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 21-26.
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 21-7.
- **Server SIC Name**—Enter the SIC DN for the child enforcement module. This value was obtained in Obtain the Server Entity SIC Name, page 21-10. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 Click **Submit** to save your changes to this log server.

Step 6 Repeat Step 1 through Step 5 for each discovered log server.

Edit Discovered Firewall on a Check Point Primary Management Station

After performing a discovery operation, you must edit any discovered firewalls. You must specify which log server the firewall uses, define the route information, and if you want to monitor resource utilization, you must specify the SNMP RO community string.

Note When editing a Check Point Firewall, never select a Check Point Firewall from the Security and Monitoring Devices list. Instead, select the Check Point Management Console that acts as the primary management station for that firewall.

Note You must configure the discovered log servers and define any log servers not managed by the primary management station before editing the discovered firewalls. To configure the discovered log servers, see Edit Discovered Log Servers on a Check Point Primary Management Station, page 21-27. To manually define log servers, see Manually Add a Child Enforcement Module or Log Server to a Check Point Primary Management Station, page 21-23.

To edit a discovered firewall, follow these steps:

Step 1 Under Firewall & Log Server Settings, select the check box next to the desired firewall.

Step 2 Click **Edit**.

Step 3 (Optional) To enable MARS to retrieve MIB objects for this reporting device, enter the child enforcement module'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 on host that represents the primary management station. 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 4 Click **Submit**.

Step 5 To define the route settings for this firewall, continue with Define Route Information for Check Point Firewall Modules, page 21-29.

Step 6 To select the log server used by this firewall, continue with Specify Log Info Settings for a Child Enforcement Module or Log Server, page 21-31.

Step 7 Repeat Step 1 through Step 6 for each discovered firewall.

Define Route Information for Check Point Firewall Modules

To perform attack path analysis and to provide suggested mitigation configurations, MARS must understand the static routes that are defined on a firewall module. This requirement is true for firewalls running on the primary management station as well as for each firewall child enforcement module managed by the primary management station. To provide this information, you must define the routes manually in the MARS web interface. You will need a list of the routes for all interfaces in the firewall before you attempt to enter this information.

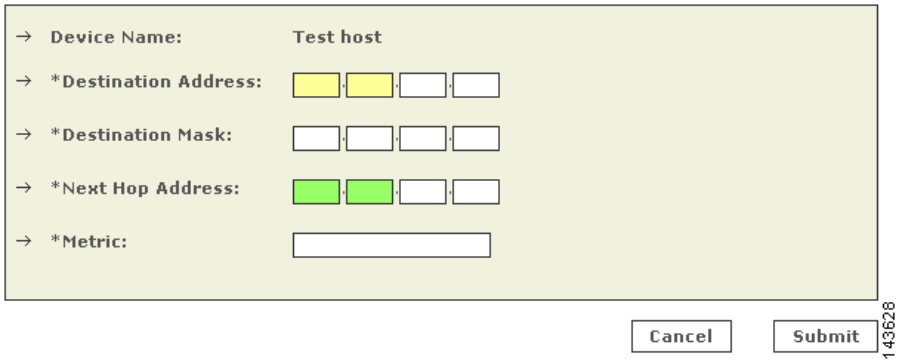
Note You do not need to specify which interface the route is associated with. MARS derives this information based on the interface settings you have specified for the host.

To define the static routes used by a firewall, follow these steps:

Step 1 Do one of the following:

- To specify the route information for the primary management station, click **Route Info** on the primary management station page.
- To specify the route information for a firewall child enforcement module, select the server under Device Type, click **Route Info**.

The Route Information dialog box appears.



Step 2 Specify values for the following fields:

- **Destination Address**—Enter the internal or external destination network address.
- **Destination Mask**—Enter the corresponding network mask value.
- **Next Hop Address**—Enter the IP address of the default gateway.
- **Metric**—Identifies the priority for using a specific route. When routing network packets, a gateway device uses the rule with the most specific network within the rule's definition. Only in cases where two routing rules have the same network is the metric used to determine which rule is applied. If they are the same, the lowest metric value takes priority. If no routing rule exists, the network packet is dropped, and if the gateway is not detected (dead), the network packet is dropped.

  A *metric* is a measurement of the cost of a route based on the number of hops (hop count) to the network on which a specific host resides. Hop count refers to the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. For the metric value, specify a number between 1 and 15.

Step 3 Click **Submit** to add the route to the list of routes

Step 4 Repeat Step 1 through Step 3 for each route defined on the firewall.

Step 5 Click **Close** to return to the Access Information page.

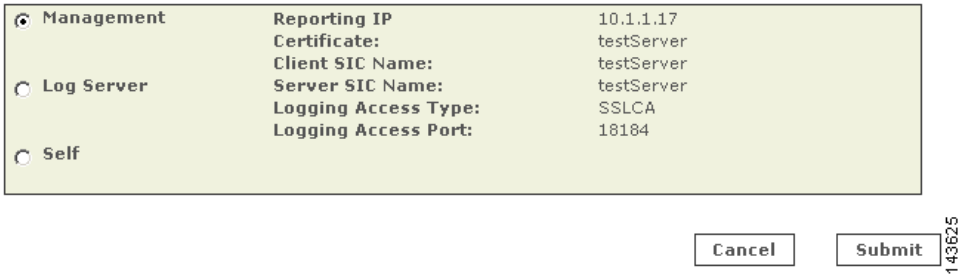
Specify Log Info Settings for a Child Enforcement Module or Log Server

There are two occasions when you must define the log settings manually:

- If you do not discover the settings of the primary management station, which does discover the log settings.
- If the child enforcement module does not propagate its logs up to the primary management station.

Three options exist for manually specifying the log settings:

- **Management**—Identifies that the child enforcement module propagates it logs up to the primary management station, the MLM or the SmartCenter server. You do not specify these settings; they are derived from the settings on the primary management station. However, the option is available if the configuration of a child enforcement module changes. If the primary management station is the log server for a child enforcement module, the log server information is populated when you perform the test connectivity operation.



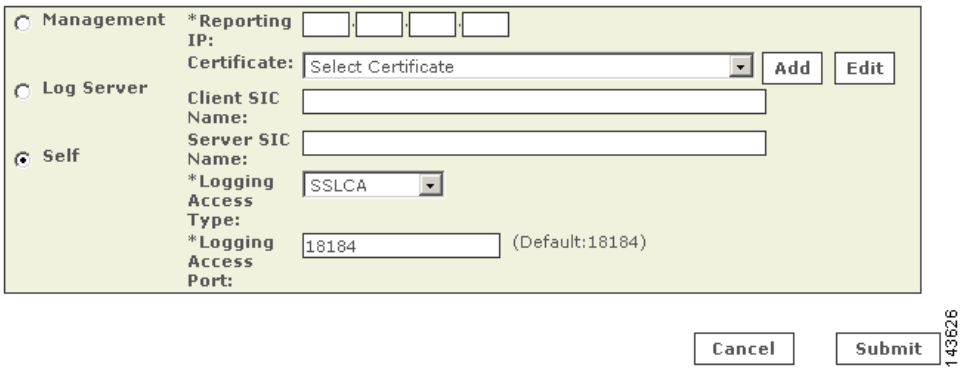
- **Log Server**—Identifies that another log server, such as a CLM, is acting as the log server for this child enforcement module. You must either select a pre-defined log server or define the settings for a new one and select it.
- **Self**—Identifies that the child enforcement module is acting as its own log server. In this case, you must specify the communication settings required to pull the logs from that module or server.

To specify the log server settings of a child enforcement module manually, follow these steps:

Step 1 (Firewall only) If a child enforcement module does not propagate its log information to the primary management station, then select that child enforcement module under Device Type, click **Log Info**, and do one of the following:

- To specify that the child enforcement module is acting as its own log server, select **Self** and continue with Step 3, omitting the Device Name field.

Figure 21-1 Log Information Published to Self



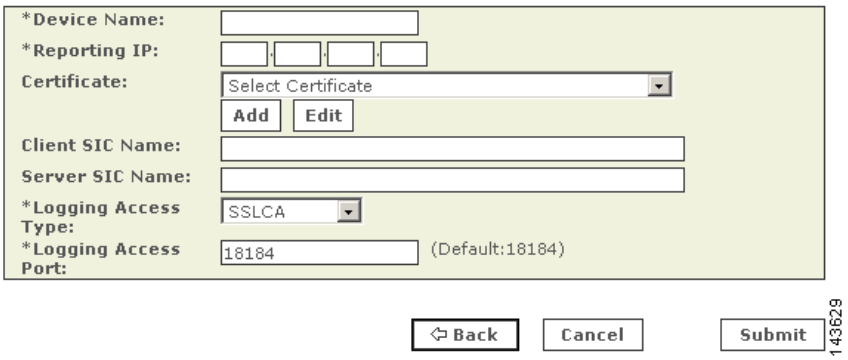
- To specify an alternate log server, select **Log Server**, and continue with Step 2.

The Log Information dialog box appears, and the desired option is selected.

Step 2 Do one of the following:

- Select a predefined log server from the Select list, click **Submit**, and continue with Step 5.

- Click **Add** to define a new log server.



Step 3 Specify values for the following fields:

- **Device Name**—Enter the name of the log server. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station 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.

- **Reporting IP**—Enter the IP address of the interface in the log server from which MARS will pull security event logs. This address represents either a virtual IP address associated with a CLM, an MLM, or another log server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 1-10.
- **Logging Access Type**—This value identifies the authentication method to use for LEA traffic, which is the protocol used to pull security logs from the log server. Select **ASYMSSLC**, **CLEAR**, or **SSLCA**, For more information on the access type, see Select the Access Type for LEA and CPMI Traffic, page 21-12.
- **Logging Port**—Verify that the port number in the corresponds to the value specified in the LEA_SERVER auth_port line of the `fwopsec.conf` file on this log server. The default authentication method for configuration discovery is SSLCA and data is passed on port 18184. For more information on this setting, see Select the Access Type for LEA and CPMI Traffic, page 21-12.

Step 4 If this log server uses SSLCA or ASYMSSLCA as an authentication method specify values for the following fields (Otherwise, CLEAR is the authentication method for Access Type and LEA Access Type, and you should skip to Step 5):

- **Certificate**—Either select the previously defined server from the list or click **Add** to define a new certificate authority and continue with Add a Check Point Certificate Server, page 21-26.
- **Client SIC Name**—Enter the SIC DN of the OPSEC application for the MARS Appliance. This value was obtained in Define an OPSEC Application that Represents MARS, page 21-7.
- **Server SIC Name**—Enter the SIC DN for the child enforcement module. This value was obtained in Obtain the Server Entity SIC Name, page 21-10. Typically, this value is the SIC DN of the SmartCenter server or of the CMA. In the case of Provider-1 and SiteManager-1 NGX (R60), this value is the SIC DN of the MDS that manages the CMA.

Step 5 To add this child enforcement module to the primary management station, click **Submit**.

Step 6 To add the primary management station 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 7 Click **Done** to close the Reporting Applications tab and return to the Security and Monitoring Devices list.

Step 8 Click **Activate**.

Once the MARS Appliance is activated, it connects to the Check Point log modules and retrieves the traffic and audit logs. MARS also begins to sessionize events generated by this device and its modules 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Verify Connectivity Between MARS and Check Point Devices

After defining the Check Point device and clicking Activate in the MARS web interface, the MARS Appliance connects to the log servers and pulls the traffic and audit logs stored on them. You can verify that these transactions are successful using the following method:

- Perform an ad hoc query for Event Types/Sessions specify to the Check Point primary management station.

Remove a Firewall or Log Server from a Check Point Primary Management Station

If the configuration of your network changes so that a firewall or log server is no longer managed by the primary management station under which it is defined, you must remove the child enforcement module.

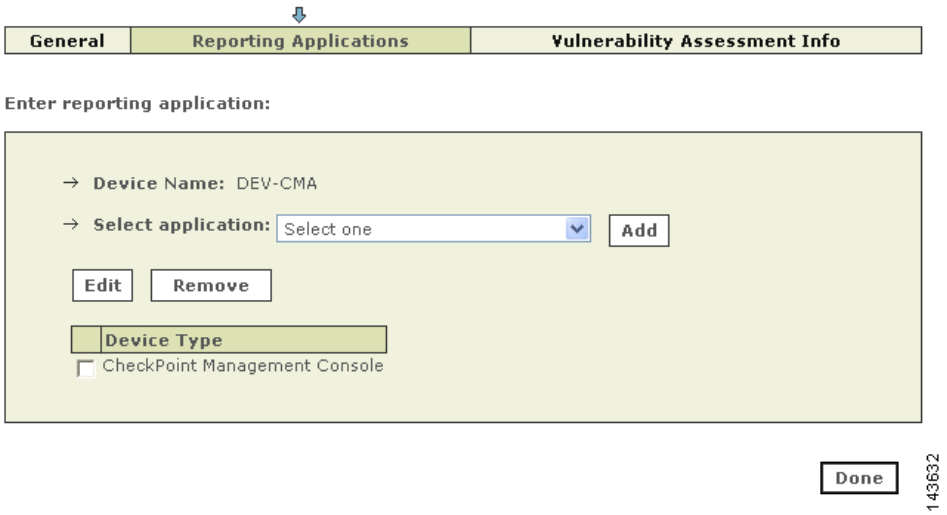
To remove a child enforcement module from the primary management station, follow these steps:

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

Step 2 From the Security and Monitor Devices list, select the host that represents the primary management station of the Check Point server and click Edit.

Such devices have CheckPoint Management Console as an entry in the Device Type column.

Step 3 Click **Next** to access the Reporting Applications tab.



Step 4 Select **CheckPoint Management Console** from the Device Type list and click **Edit**.

The Access Information page appears.

Step 5 Under Firewall & Log Server Settings, check the box next to the child enforcement module that you want to remove.

Step 6 Click **Remove**.

The Confirmation screen appears.

Step 7 Click **Submit** to remove the child enforcement module from the primary management station.

Troubleshooting MARS and Check Point

The following information can be used to troubleshoot communicate issues between the MARS Appliance and Check Point components.

- To view attack information by user, run a query where the device is a Check Point device.
- If you attempt to discover the certificate and it returns to the CheckPoint Certificate screen instead of displaying the `"Discovery done."` message box, then the discover operation failed. The likely cause is an incorrect SIC value.

Note A certificate can be pulled only once for an OPSEC Application. If for any reason the pull operation fails, you must reset the certificate using the CheckPoint SmartDashboard. For more information, see Reset the OPSEC Application Certificate of the MARS Appliance, page 21-16.

- If the device discovery operation fails, click the **View Error** button for a detailed error message.

Common reasons for failure of device discovery are as follows:

- client SIC DN name or server SIC DN name is incorrect. Use copy and paste from SmartDashboard to avoid erroneous entry.
- Invalid Certificate used.
- Invalid user name, password, or both used. Verify that the credentials provided for the Access IP match an Check Point account with administrative privileges.
- Unsupported version of Check Point. (Discovery works only with NG FP3 and above. Internally we have tested up to Version R60)
- Invalid authentication method used. The default method is SSLCA. Check the fwopsec.conf file to determine which method is used. CS-MARS currently support only three authentication methods for CPMI communication: SSLCA, ASYM_SSLCA and CLEAR. For more information on specifying these settings, see Select the Access Type for LEA and CPMI Traffic, page 21-12.
- Invalid access port. Default port for secured CPMI-based communication is TCP 18180. Check the `fwopsec.conf` to verify the configured port.
- The MARS Appliance does not have access to port 18190, or an alternate specified in fwopsec.conf for CPMI. At the CLI of the MARS Appliance, use the **telnet** command to test the access port. For more information on **telnet**, see Verify Communication Path Between MARS Appliance and Check Point Devices, page 21-15.
- The policy database was not installed after creating OPSEC Application in the SmartDashboard.
- Firewall policies were not created and installed that permitted the MARS Appliance to connect to the Check Point primary management station. For information, see Create and Install Policies, page 21-14.

For additional Check Point discovery-related debug information, use the **pnlog** command at the CLI of the MARS Appliance. You can use the *cpdebug* attribute to specify appropriate debug level. Level 9 presents all debug messages. You can view the debug messages using the **pnlog showlog cpdebug** command at the CLI. For more information on **pnlog**, see see **pnlog** of the *Cisco Security MARS Command Reference, 6.X*.

CHAPTER 22

NetScreen ScreenOS Devices

MARS can monitor NetScreen ScreenOS devices running versions 4.0, 5.0, 5.4, and 6.0. To prepare a NetScreen device to be monitored, you must:

1. Provide MARS with SNMP, SSH or Telnet administrative access to NetScreen device.
2. Define the SNMP RO community strings to be shared between the NetScreen device and MARS.
3. Select the syslog messages to published to MARS.
4. Add the Netscreen Device to the MARS web interface.

To accomplish these requirements, you must perform two procedures:

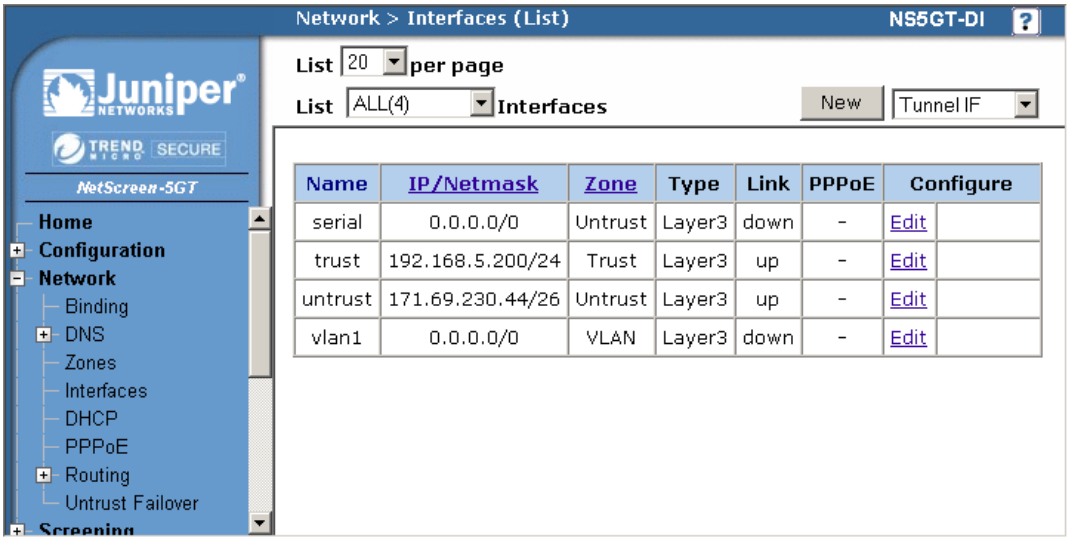
- Bootstrap the NetScreen Device, page 22-1
- Add the NetScreen Device to MARS, page 22-5

Bootstrap the NetScreen Device

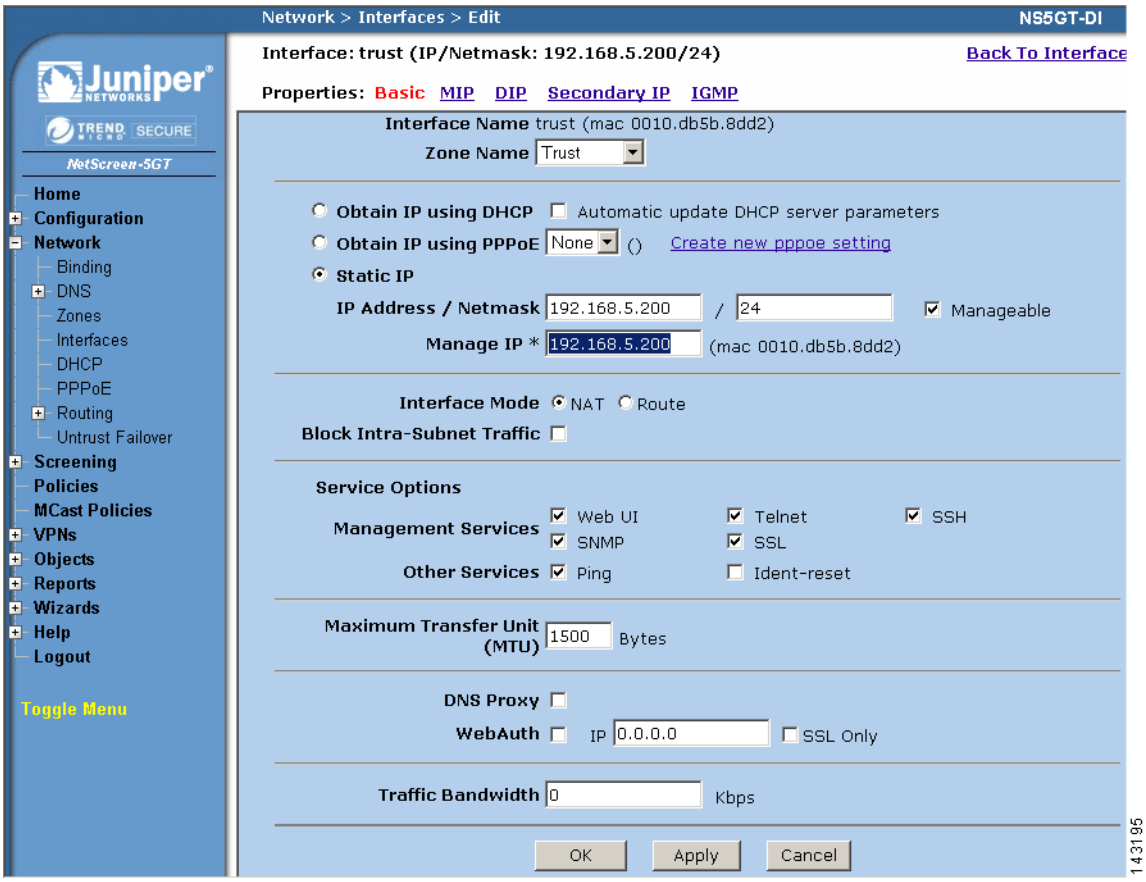
To prepare the NetScreen device to be monitored by MARS, follow these steps:

Step 1 Login to the NetScreen with appropriate username and password.

Step 2 In the main screen, on the left hand column click **Network > Interfaces**.



Step 3 Click **Edit** next to the appropriate interface to configure for MARS to have access to SNMP and Telnet/SSH.



Step 4 Under Service Options, select one of the following values:

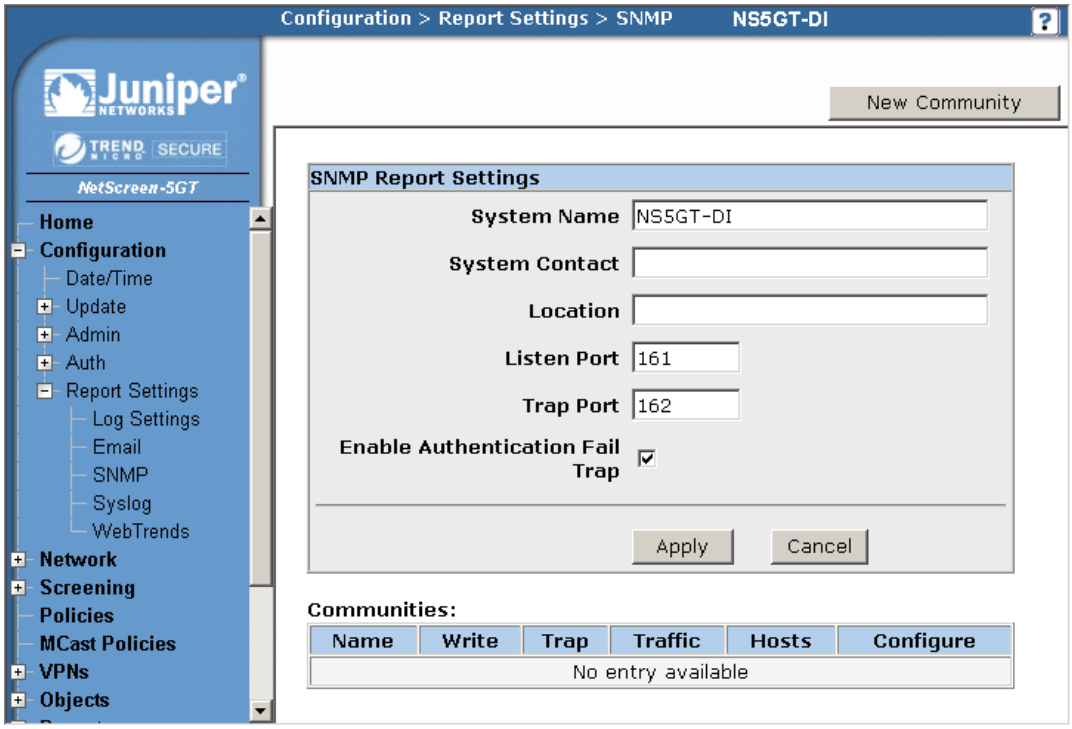
- SNMP

- Telnet
- SCS (4.0 only)
- SSH (5.0 and later)

MARS can only use one of the access methods to perform configuration discovery. This value will also be selected in the Access Type value of Add the NetScreen Device to MARS, page 22-5.

Step 5 Click **Apply** then click **OK**.

Step 6 Configure the SNMP information by selecting **Configure > Report Settings > SNMP**.



Step 7 Add the MARS IP address in the Host List by clicking **Edit**.

Step 8 Enter the MARS IP address and verify that the Community Name value matches the community string entered in the MARS web interface when adding this device.

Step 9 (Optional) If the community string does not match, click **New Community** to define one that matches the on defined in MARS.

Step 10 Configure the Syslog information by selecting **Configure > Report Settings > Syslog**.

Step 11 Verify that the **Enable Syslog Messages** and **Include Traffic Log** boxes are checked.

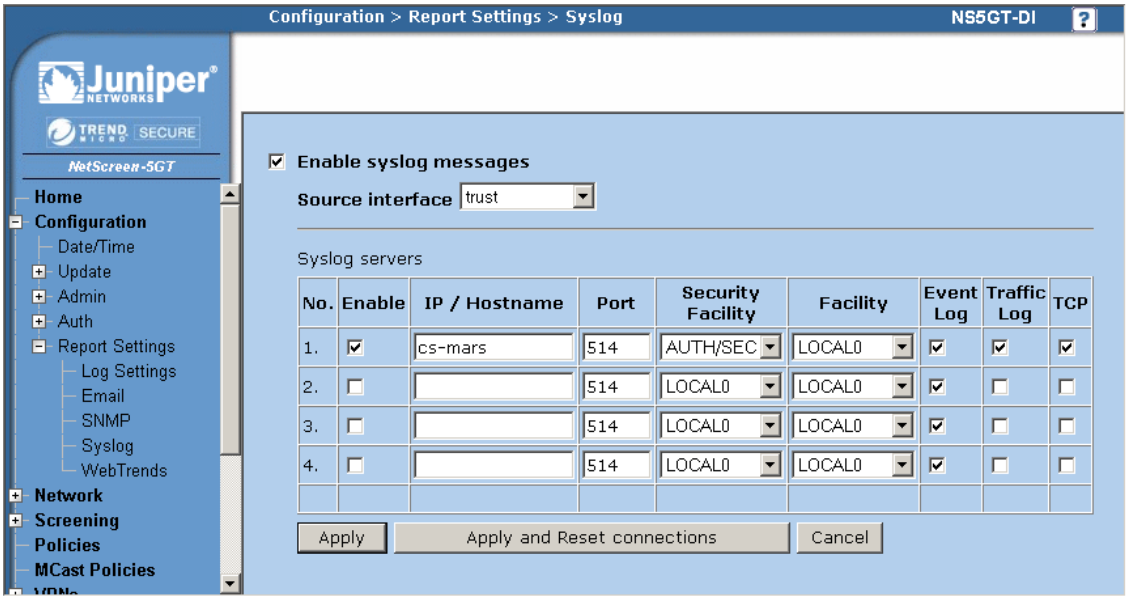
Step 12 Enter the IP address of the MARS Appliance that will listen for events from this device

Step 13 Verify that the default syslog port number of 514 is selected.

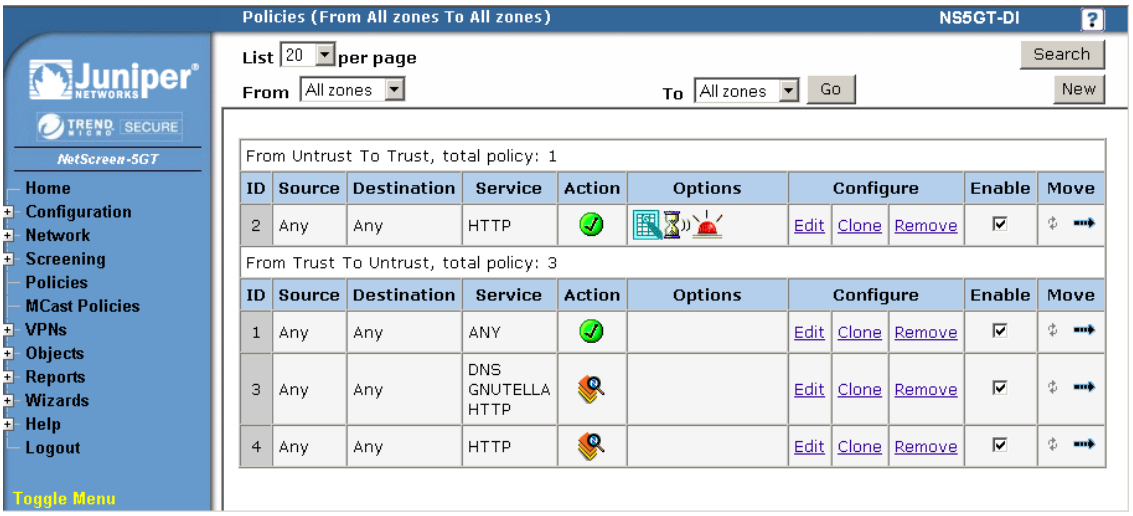
Step 14 Select the **AUTH/SEC** for Security Facility and **LOCAL0** for Facility.

Step 15 For NetScreen 5.0, select the **Event Log** in addition to **Traffic Log**.

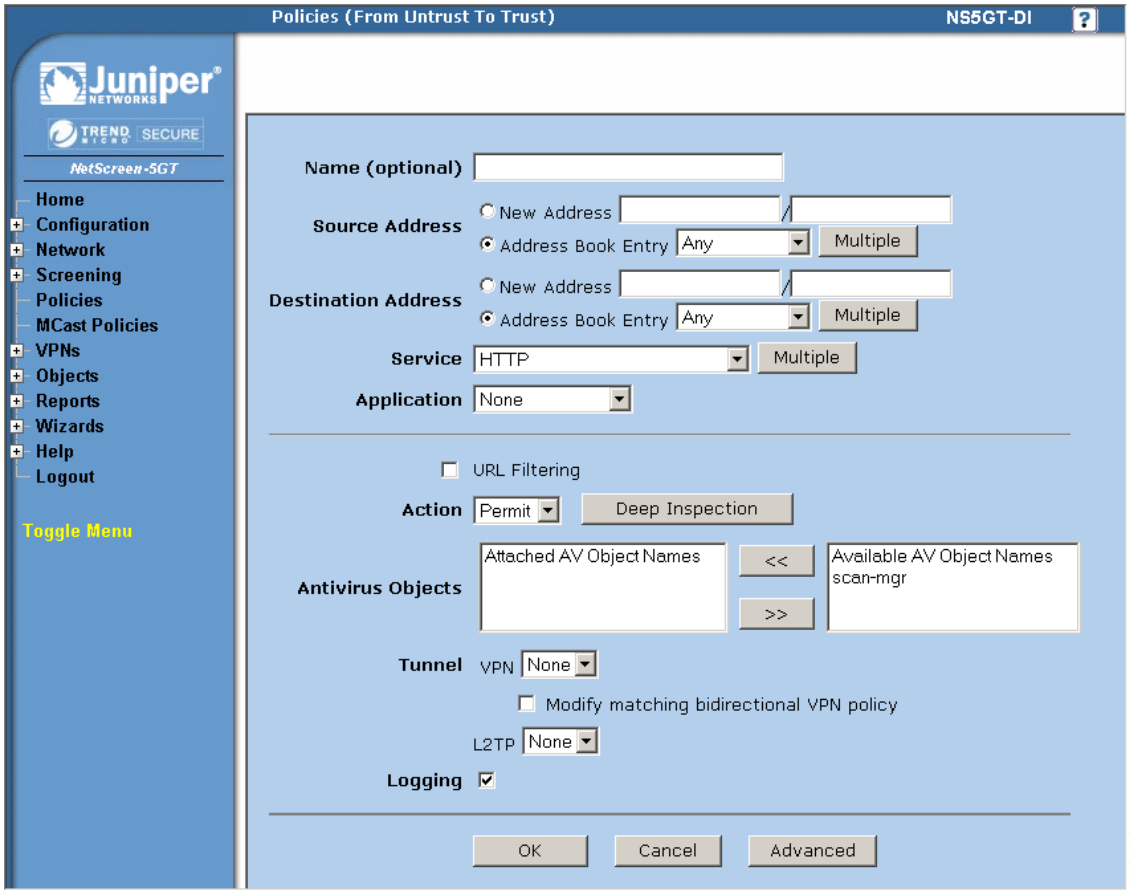
Step 16 Click **Apply**.



Step 17 Configure logging for each policy that user wants to send the events to the MARS Appliance. Select **Policies** on the left hand area.



Step 18 Click **Edit** then **Advance** and verify that **Logging** box is checked. Repeat for all policies which events need to be sent to MARS.



Step 19 Verify that all the Syslog event severity levels that need to be sent to MARS are configured. Verify which Syslog severity levels that are enabled by selecting **Configuration > Report Settings > Log Settings**.

Add the NetScreen Device to MARS

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

Step 2 Select one of the following versions from the Device Type list.

- **NetScreen ScreenOS 4.0**
- **NetScreen ScreenOS 5.0**
- **NetScreen ScreenOS 5.4**
- **NetScreen ScreenOS 6.0**

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 or 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 **TELNET**, **SSH**, or **FTP** from the Access Type list, and continue with the procedure that matches your selection:

- 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

For more information on determining 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 (Optional) If you defined an access IP and selected and configured an access type, click **Discover** to determine the device settings.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, the "Discovery is done." dialog box appears when the discovery operation completes. Otherwise, an error message appears. After the initial pull, the MARS Appliance pulls based on the schedule that you define. For more information, see Scheduling Topology Updates, page 1-18.

Step 9 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 10 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

PART 7

Network Access Control

CHAPTER 23

Cisco NAC Appliance

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager (CAM) web console and enforced through the Clean Access Server (CAS) and the Clean Access Agent (CAA). Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation before clients access the network.

CAM manages one or more CASs. Cisco Security MARS receives event data from CAM. CAM can send both syslog messages and SNMP traps. SNMP traps provide system health status, whereas the syslog message provide details about quarantined or infected hosts, connection attempts, and connection status.

This chapter contains the following topics:

- Bootstrap the Cisco NAC Appliance, page 23-1
- Define a Cisco NAC Appliance in MARS Manually, page 23-2

Bootstrap the Cisco NAC Appliance

Using the Clean Access Manager (CAM) web console, perform the following tasks so that the NAC appliance publishes the required events to Cisco Security MARS.

Syslog Support

To enable syslog processing support, define the MARS appliance as a syslog server. For detailed steps, see Configuring Syslog Logging in *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

SNMP Support

For SNMP support, perform the following tasks:

1. Enable SNMP alerts for the NAC appliance.
2. Define the MARS appliance as a trapsink.

For detailed steps, see SNMP in *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

Define a Cisco NAC Appliance in MARS Manually

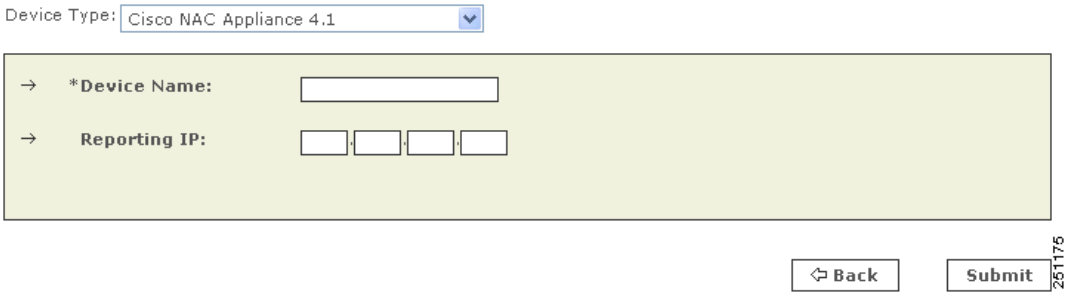
To define a Cisco NAC appliance manually, you must define the appliance in the MARS web interface. When the appliance is defined and the changes are activated, MARS normalizes the syslog message receive by the appliance against known event types.

To define a NAC appliance in MARS, follow these steps:

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

Step 2 Select **Cisco NAC Appliance 4.1** for the Device Type list.

A the Device Type page appears.



Step 3 Type the name of this appliance in the **Device Name** field.

Step 4 Type the reporting IP of the appliance in the **Reporting IP** field.

Step 5 To save your changes, click **Submit**.

The device name appears under the Security and Monitoring Information list. 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 6 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to recognize, map, and sessionize events generated by this appliance 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

PART 8

Virtual Private Network Gateways

CHAPTER 24

Cisco VPN 3000 Concentrator

VPN devices provide MARS with information about remote hosts, login in requests and denials, and access times. With this data, MARS can provide end-to-end attack path analysis and identify the VPN device through which attacks are launched.

MARS can receive and process events from the Cisco VPN 3000 Concentrator, versions 4.0.1 and 4.7. To enable communications, you must perform two tasks.

This chapter contains the following topics:

- Bootstrap the VPN 3000 Concentrator, page 24-1
- Add the VPN 3000 Concentrator to MARS, page 24-2

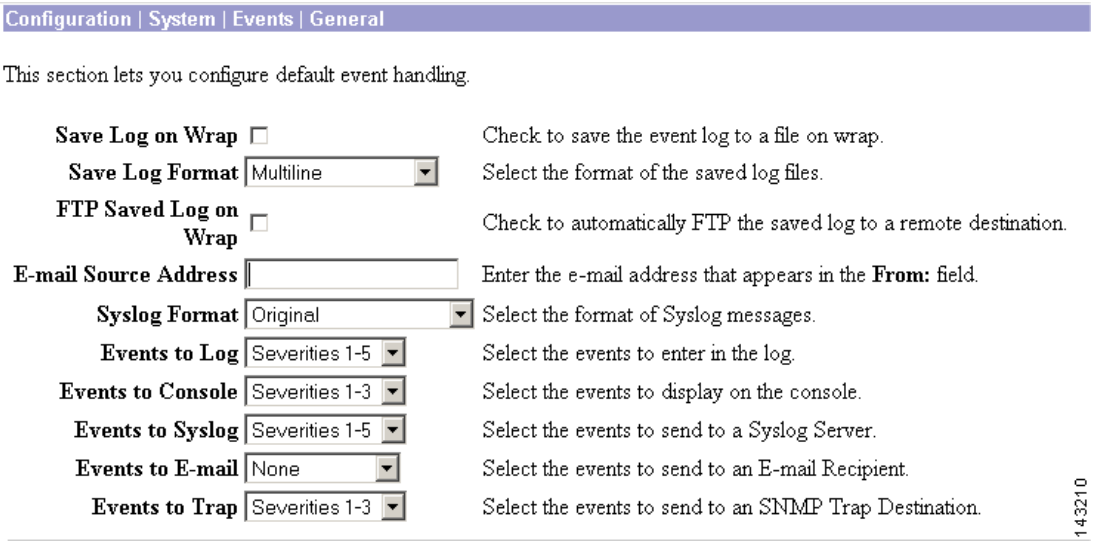
Bootstrap the VPN 3000 Concentrator

To configure a Cisco VPN 3000 Concentrator to generate and publish events to the MARS Appliance, you must verify that the correct events are generated in the correct format, and you must direct the Cisco VPN 3000 Concentrator to publish syslog events to the MARS Appliance.

To configure Cisco VPN 3000 Concentrator to send syslog events to MARS, follow these steps:

Step 1 Open your browser and log in to the Cisco VPN 3000 Concentrator Series Manager.

Step 2 From the tree on the left, select **Configuration > System > Events > General**.

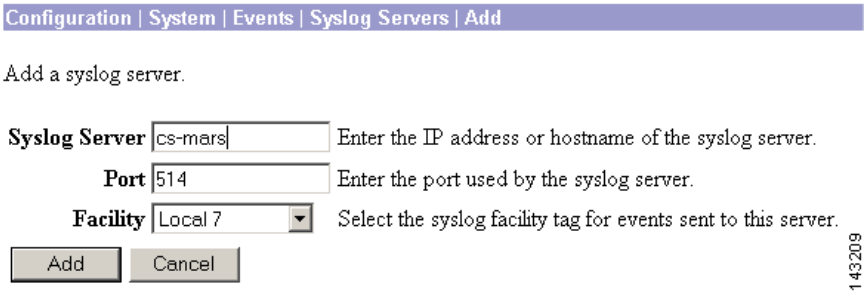


Step 3 Verify that the Syslog Format is Original.

Step 4 Select **Severities 1-5** in the Events to Syslog field.

Step 5 From the tree on the left, select **Configuration > System > Events > Syslog Servers**.

Step 6 Click **Add** to define a target syslog server.



Step 7 In the Syslog Server field, enter the IP address or hostname of the MARS Appliance.

Step 8 Click **Add** to save the syslog server settings.

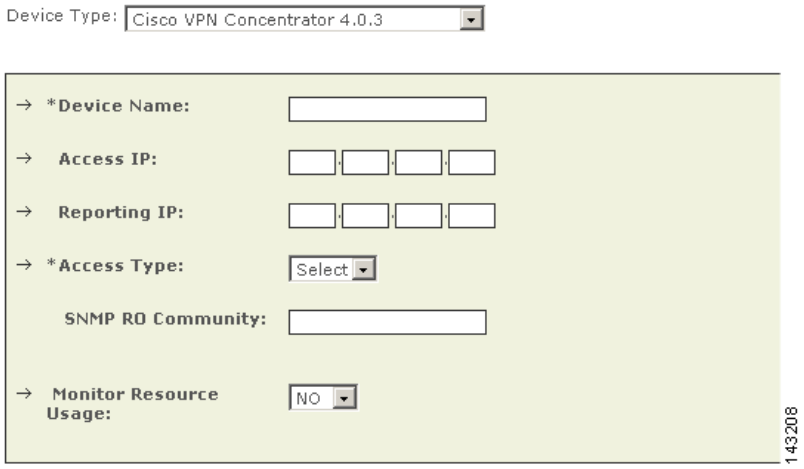
Step 9 Click **Save** in the top-right corner to save all changes.

Add the VPN 3000 Concentrator to MARS

To add the VPN 3000 Concentrator to MARS, follow these steps:

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

Step 2 Select either **Cisco VPN Concentrator 4.0.1** or **Cisco VPN Concentrator 4.7** from the Device Type list.



Step 3 Enter the name of the VPN Concentrator in the Device Name field.

Step 4 Enter the IP address used to administer the VPN Concentrator in the Access IP field.

Step 5 Enter the IP address from which the syslog messages are sent to MARS in the Reporting IP field.

Step 6 Select **SNMP** from the Access Type list.

Step 7 (Optional) To enable MARS to retrieve MIB objects for this Concentrator, enter the device's read-only community string in the **SNMP RO Community** field.

MARS uses the SNMP RO string to read MIBs related to the reporting device's CPU usage and other device anomaly data.

Step 8 Click **Discover**.

Step 9 Click **Submit**.

PART 9

WLAN Controller

CHAPTER 25

Cisco Wireless LAN Controller

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

The following system rules support Cisco Wireless Controller devices:

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

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

- System Rule: Rogue WLAN AP Detected

The following system reports support Cisco Wireless Controller devices:

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

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

The following bugs apply to this feature set:

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

  If a user deletes a device from the MARS web interface (Admin > Security and Monitoring Devices page) and clicks Activate, MARS will report any future events (syslog, SNMP traps, etc.) received from that device as Unknown Reporting Device. To prevent these events from appearing, configure the device in question to stop sending events to MARS.
- **CSCsk71706**—WLAN: IP not in MARS DB should be define at IP Management

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

This chapter contains the following topics:

- WLAN Configuration Overview, page 25-2

WLAN Configuration Overview

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

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

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

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

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

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

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

   —or—

   Define the WLAN Controllers using a seed file. For information on using seed files, see Adding Multiple Reporting and Mitigation Devices Using a Seed File, page 1-34.
3. Discover or manually define the access points managed by the WLAN controller.

Bootstrap the WLAN Controller

To prepare the WLAN controller, you must:

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

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

Step 1 In the WLAN Controller user interface, select **Management > SNMP > General**, and enable SNMP v1.

Step 2 Select **Management > SNMP > Trap Receivers**.

Step 3 Click **New** and define the MARS appliance as a trap receiver by specifying the following values

- **Name**—Enter the name of the MARS appliance.
- **IP Address**—Enter the IP address of the appliance.
- **Status**—Set to enable.

Step 4 To define the SNMP communities value, select **Management > SNMP > Communities**.

Note This value is required when you define the WLAN controller in the MARS web interface.

Step 5 To selectively enable/disable traps, select **Management > SNMP > Trap Controls**. Verify the traps are being generated for the receiver that represents the MARS appliance.

Add a Cisco Wireless LAN Controller to MARS

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

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

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

Step 2 Select **Cisco WLAN Controller 4.x** from the Device Type list.

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

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

Step 3 Specify values for the following fields:

- **Device Name**—Specify the name of this controller.
- **Access IP**—Required to enable MARS to discover settings from the controller device, including the list of managed access points, enter the administrative IP address in the Access IP field.

  This IP address is the one assigned to the management interface on the controller.
- **Reporting IP**—Enter the IP address of the interface that publishes SNMP notifications in the Reporting IP field
- **Access Type**—Select SNMP.
- **SNMP RO Community**—Required for discovery to enable MARS to retrieve values of the MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.

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

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

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

Step 5 Do one of the following:

- To discover the controller settings and all access points associated with the controller, click **Discover**
- To manually define access points, continue with Manually Define Access Points, page 25-4.

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

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

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

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

Manually Define Access Points

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

To manually define access points, follow these steps:

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

Step 2 From the list of devices, select the host running Cisco WLAN Controller 4.x, and click **Edit**

Step 3 (Optional) Click **Add Access Point** and specify the following values for at least one access point:

- **Device Name**—Identifies the name of this access point as it will appear under the Access Point Name list on the WLAN controller device page.
- **MAC Address**—Identifies the MAC address of the access point.

Step 4 To create the access point and save your changes, click **Submit**.

Step 5 To save your changes to the controller, click **Submit**.

Step 6 To enable MARS to start parsing events from this device, click **Activate**.

PART 10

AAA

CHAPTER 26

Configuring AAA Devices

Revised: Jan 4, 2008

Authentication, authorization, and accounting (AAA) devices provide accountability throughout your network, ensuring that valid users are authorized to use the network services they request and providing detailed event logs regarding failures and successes in such requests.

The AAA server is a key component in the Network Access Control (NAC)initiative (see Configuring Network Admission Control Features and Enable NAC-specific Messages, page 17-4). Cisco Secure Access Control Server (ACS), which is the AAA server for NAC, returns access control decisions to the network access device on the basis of the antivirus credentials of the hosts that are requesting network services.

MARS supports the Cisco Secure ACS software and the Cisco Secure ACS Solution Engine, version 3.3 and later. In the case of Cisco Secure ACS software, support is provided by an agent that resides on the Cisco Secure ACS server. For the Cisco Secure ACS Solution Engine, this agent must reside on a remote logging host. This agent provides MARS with three event logsin syslog format. The logs are as follows:

- Passed authentication log (requires Cisco Secure ACS, 3.3 or later)
- Failed attempts log
- RADIUS accounting log

To support NAC and the 802.1x features, Cisco Secure ACS uses the RADIUS authentication protocol and the cisco-av-pair attributes. For more information on configuring Cisco Secure ACS as a posture validation server for NAC, see the following URLs:

- "Network Admission Control" chapter in *User Guide for Cisco Secure ACS for Windows Server, Version 3.3*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/user/guide/nac.html

- "Posture Validation" chapter in *User Guide for Cisco Secure ACS for Windows, Version 4.0*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/nac.html

- "Using Profile Templates" section in the "Network Access Profiles" chapter in *User Guide for Cisco Secure ACS for Windows, Version 4.0*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/sp.html#wp1075429

For more information on the cisco-av-pair attributes, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/ac.html

This chapter explains how to prepare the Cisco Secure ACS server or the Cisco Secure ACS Solution Engine to allow MARS to collect the event logs. It also describes how to configure MARS to receive and process these logs correctly. Using the web interface, you must define a host to represent the Cisco Secure ACS server (or the remote logging agent collecting logs for the Cisco Secure ACS Solution Engine) and then add the software application to that host.

Supporting Cisco Secure ACS Server

To configure a Cisco Secure ACS server to act as a reporting device, you must perform three tasks:

1. Configure Cisco Secure ACS server to generate the correct log files and details and define the AAA clients.
2. Install the PN Log Agent on the Cisco Secure ACS server and configure it to forward the correct log files.
3. Add the Cisco Secure ACS server to the MARS web interface

You can also configure Cisco Secure ACS to provide command authorization for the MARS Appliance. In this role, Cisco Secure ACS verifies that the MARS Appliance is authorized to execute specific commands on reporting devices and mitigation devices.

Supporting Cisco Secure ACS Solution Engine 4.x

MARS supports the Cisco Secure ACS Solution Engine via a remote logging host. Cisco Secure ACS Remote Agent for Windows is a Windows-based application that supports Cisco Secure ACS Solution Engine for remote logging.

Even though the Cisco Secure ACS Solution Engine supports up to five appliance via a remote logging host, MARS currently supports only one Cisco Secure ACS Solution Engines per remote logging host. Otherwise, MARS cannot identify the IP address of the originating Cisco Secure ACS Solution Engine.

To enable this support, follow these steps:

1. Configure the Cisco Secure ACS Solution Engine to publish logs to the MARS appliance. To perform this task, see Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3
2. Add the Cisco Secure ACS Solution Engine to MARS as a Cisco ACS 4.x reporting device. To perform this task see Add and Configure a Cisco Secure ACS Solutions Engine in MARS, page 26-15, and substitute the ACS server references with the remote logging host.

Supporting Cisco Secure ACS Solution Engine 3.x

MARS supports the Cisco Secure ACS Solution Engine via a remote logging host. Cisco Secure ACS Remote Agent for Windows is a Windows-based application that supports Cisco Secure ACS Solution Engine for remote logging.

Even though the Cisco Secure ACS Solution Engine supports up to five appliance via a remote logging host, MARS currently supports only one Cisco Secure ACS Solution Engines per remote logging host. Otherwise, MARS cannot identify the IP address of the originating Cisco Secure ACS Solution Engine.

To enable this support, follow these steps:

1. Configure the Cisco Secure ACS Solution Engine to publish logs to the remote logging host. See Bootstrap Cisco Secure ACS, page 26-3.
2. Install and configure the Cisco Secure ACS Remote Agent for Windows on the target remote logging host. This host must be running a supported version of Microsoft Windows.

   For instructions on installing and configuring the remote agent, see Installation and Configuration Guide for Cisco Secure ACS Remote Agents.
3. Install the pnLog Agent on the remote logging host.

   For information on installing and configuring the pnLog Agent, see Install and Configure the PN Log Agent, page 26-8.
4. Add the remote logging host to MARS as a Cisco ACS 3.x reporting device. To perform this task see Add and Configure an Cisco Secure ACS Server in MARS, page 26-13, and substitute the ACS server references with the remote logging host.

Bootstrap Cisco Secure ACS

Bootstrapping the Cisco Secure ACS includes the following tasks:

- Configuring the ACS device to generate the desired logs.
  - Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3
  - Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4
- Define AAA Clients, page 26-6
- (Optional) Configure TACACS+ Command Authorization for Cisco Routers and Switches, page 26-8

Configure Cisco Secure ACS 4.x to Generate Logs

MARS support the Cisco Secure ACS sever and the ACS Solutions Engine (SE). This procedure details how to configure the 4.x version of either of these devices so as to generate the syslog messages required parsed by MARS. It also explains how to configure ACS to publish those syslogs to the MARS appliance.

To configure Cisco Secure ACS 4.x to generate the syslogs required by MARS and to publish to MARS, follow these steps:

Step 1 Refer to the "Syslog Logging Configuration Scenario" in the *Configuration Guide for Cisco Secure ACS* for details.

Step 2 Enable the following syslog events:

- **CisACS_01_PassedAuth**—Cisco ACS passed authentications.
- **CisACS_02_FailedAuth**—Cisco ACS failed attempts.
- **CisACS_03_RADIUSAcc**—Cisco ACS RADIUS accounting.
- **CisACS_04_TACACSAcc**—Cisco ACS TACACS+ accounting.
- **CisACS_05_TACACSAdmin**—Cisco ACS TACACS+ administration.
- **CisACS_06_VoIPAcc**—Cisco ACS VoIP accounting.

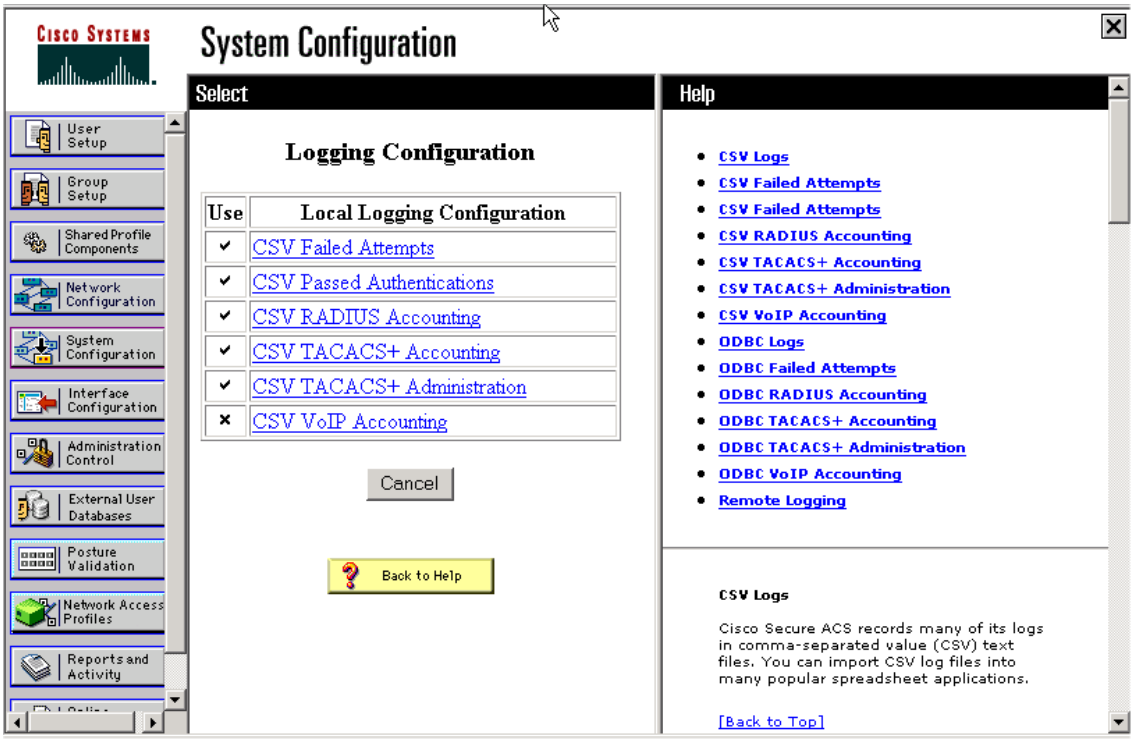
- **CisACS_11_BackRestore**—ACS backup and restore log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_12_Replication**—ACS database replication log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_13_AdminAudit**—ACS administration audit log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_14_PassChanges**—ACS user password changes log messages.
- **CisACS_15_ServiceMon**—ACS service monitoring log messages.
- **CisACS_16_ApplAdmin**—ACS appliance administration audit log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.

Configure Cisco Secure ACS 3.x to Generate Logs

To configure Cisco Secure ACS to generate the audit logs required by MARS, follow these steps:

Step 1 Log in to the Cisco Secure ACS server or Solution Engine.

Step 2 Select **System Configuration > Logging**.

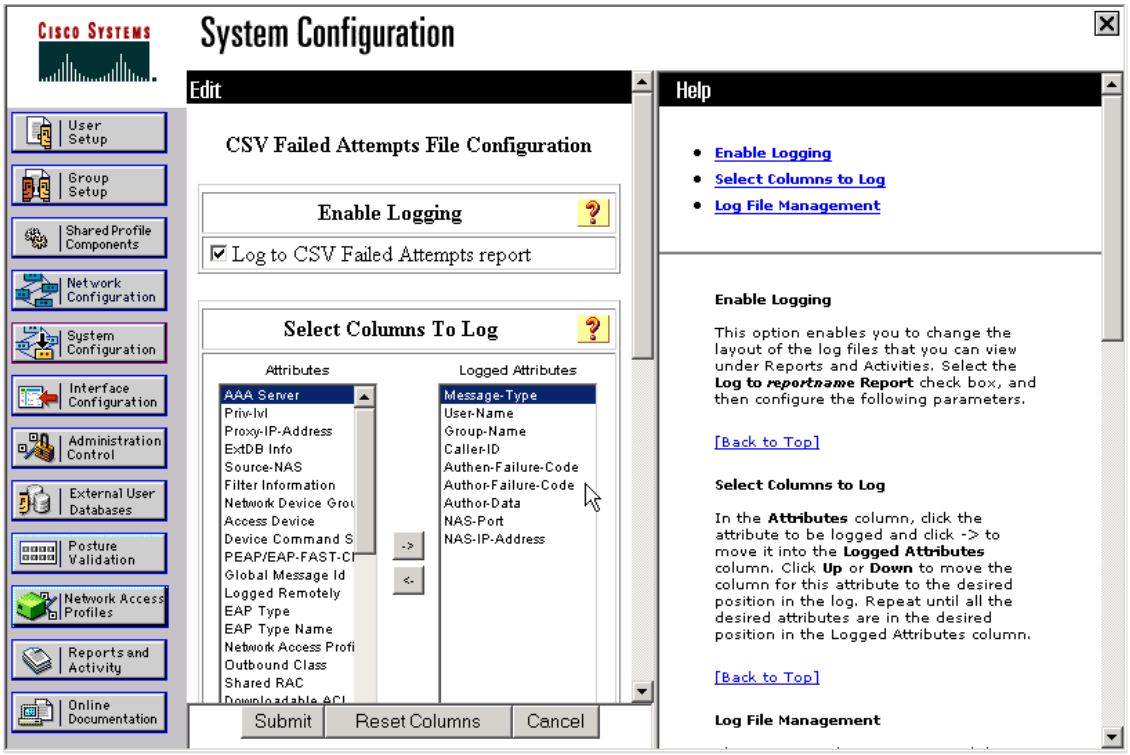


Step 3 Verify that CVS Failed Attempts, CVS Passed Authentications and CVS RADIUS Accounting Logging are enabled.

Step 4 Click **CSV Failed Attempts**, and verify that the following attributes appear in the Logged Attributes list:

- User-Name

- Caller-ID
- NAS-Port
- NAS-IP-Address
- AAA-Server
- Authen-Failure-Code
- Message-Type



Step 5 Click **Submit**.

Step 6 Click **CVS Passed Authentications**, and verify that the following attributes appear in the Logged Attributes list:

- AAA Server'
- User-Name
- Caller-ID
- NAS-Port
- NAS-IP-Address
- System-Posture-Token
- EAP Type Name

Step 7 Click **Submit**.

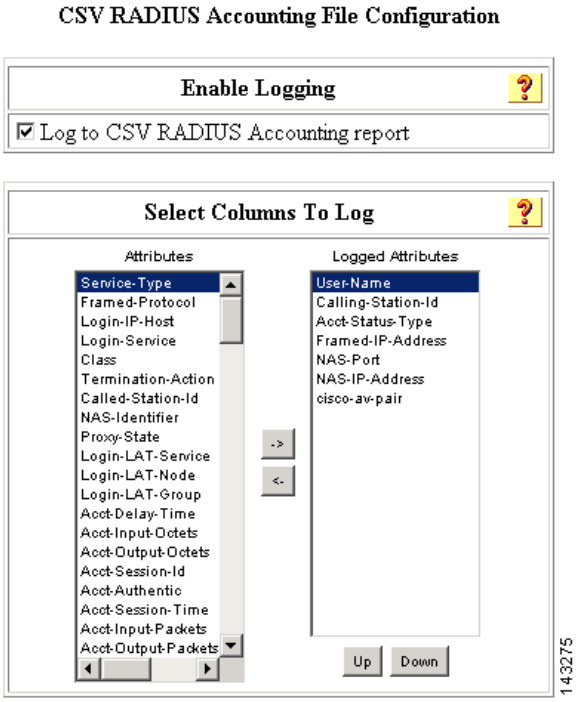
Step 8 Click **CVS RADIUS Accounting**, and verify that the following attributes appear in the Logged Attributes list:

- User-Name

- Calling-Station-Id
- Acct-Status-Type
- NAS-Port
- NAS-IP-Address
- AAA Server
- Framed-IP-Address

Step 9 To support the 802.1x features of NAC, select the following RADIUS accounting attributes:

- Framed-IP address
- cisco-av-pair



Step 10 Click **Submit**.

For additional details on the RADIUS attributes supported by Cisco Secure ACS, see to the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/ad.html

Define AAA Clients

To support the 802.1x features of NAC, you must also define the Cisco switches as AAA clients within Cisco Secure ACS. When defining a AAA client, verify the following settings:

- Enable the authentication method that best supports the 802.1x functionality that you want to enable. This option is selected in the Using Authentication box.

- Enable logging of watchdog packets, interim updates. Select the Log Update/Watchdog Packets from this AAA Client check box. This option ensures that interim updates are sent from the Cisco Secure ACS to MARS.

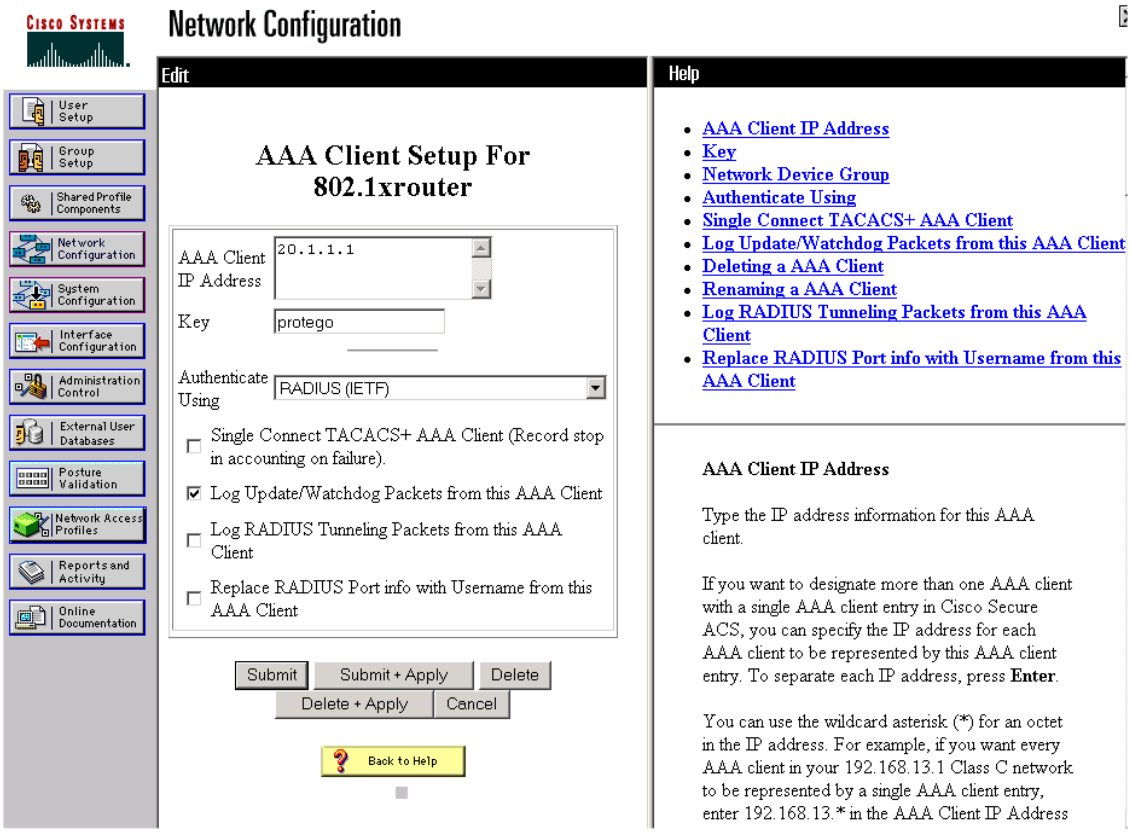
To enable 802.1x logging support, the following configuration must also be completed.

- Ensure DHCP snooping is enabled on each network access device that you plan to define as an 802.1x client in MARS

Note The attack path can not be calculated for a NAC 802.1x security incident when the events triggering the incident are reported to the MARS Appliance by Cisco Secure ACS. However, the MARS Appliance knows the switch port to block so you can mitigate without the attack path.

Figure 26-1 displays example settings for such a client.

Figure 26-1 Configure a AAA Client to Support 802.1x



For more information on defining AAA clients, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/n.html#wp342084

Configure TACACS+ Command Authorization for Cisco Routers and Switches

You can use the TACACS+ feature of Cisco Secure ACS to authorize the command sets that MARS is allowed to execute on a reporting device. The use of this feature is not required by MARS. However, if you are using this feature on your routers and switches, you must ensure that MARS is allowed to execute specific commands. Required commands are grouped under two operations: configuration retrieval and mitigation.

The following commands support configuration retrieval:

- all **show** commands
- **changeto system**
- **changeto context <*context_name* >**
- **enable**
- **page**
- **no page**
- **terminal length 0**
- **terminal pager lines 0**
- **write terminal**

The following commands support mitigation:

- **conf terminal**
- **interface <*interface_name* >**
- **shutdown**
- **set port disable <*port_name* >**

For more information on configuring command authorization sets in Cisco Secure ACS, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/c.html#wp697557

Install and Configure the PN Log Agent

MARS includes the PN Log Agent to monitor Cisco Secure ACS active log files (failed attempts, passed authentications, and RADIUS accounting). This agent pushes these log files via syslog to MARS. You can download the PN Log Agent from the software download center at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

Note If you are upgrading to a new version of the PN Log Agent, see Upgrade PN Log Agent to a Newer Version, page 26-11.

As part of its operation, the PNLog Agent service writes error and informational message to the Application Log, which can be viewed using the Event Viewer. To learn more about these messages, see Application Log Messages for the PN Log Agent, page 26-11.

To install and configure the PNLog Agent, follow these steps:

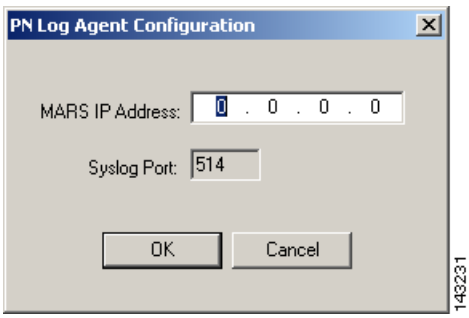
Step 1 Download the PN Log Agent and install it on the server running Cisco Secure ACS or on the remote logging host to which the Cisco Secure ACS Solution Engine is publishing its logs.

Note If installing on a remote logging host, you must have configured the Cisco Secure ACS Remote Agent for Windows on the target remote logging host. For instructions on installing and configuring the remote agent, see Installation and Configuration Guide for Cisco Secure ACS Remote Agents.

Step 2 Select **Start > All Programs > Protego Networks > PNLogAgent > Pn Log Agent**

Step 3 Click **Edit > PN-MARS Config**.

The PN Log Agent Configuration dialog box appears.

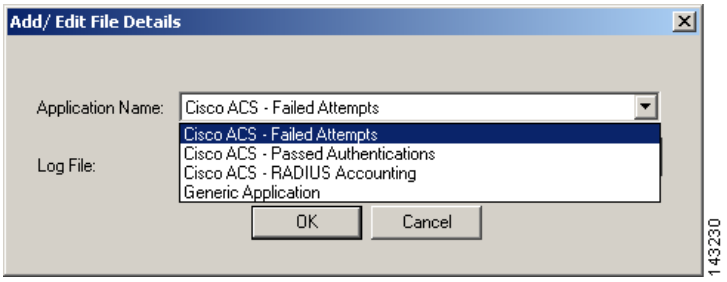


Step 4 In the MARS IP Address field, enter the address of the MARS Appliance, and click **OK**.

Step 5 Select **Edit > Log File Config > Add**.

Step 6 From the Edit pull down menu select **Add**.

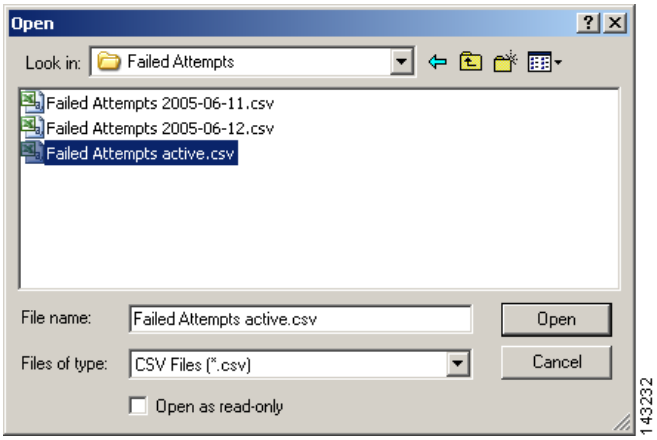
The Add/Edit File Details dialog box appears.



Step 7 From the Application Name list, select the **Cisco ACS-Failed Attempts**.

Step 8 Click on the **...** button to select the appropriate log where all Cisco Secure ACS logs are stored. In this example after selecting **Failed Attempts** application, be sure to select the matching log file, **Failed Attempts** active log.

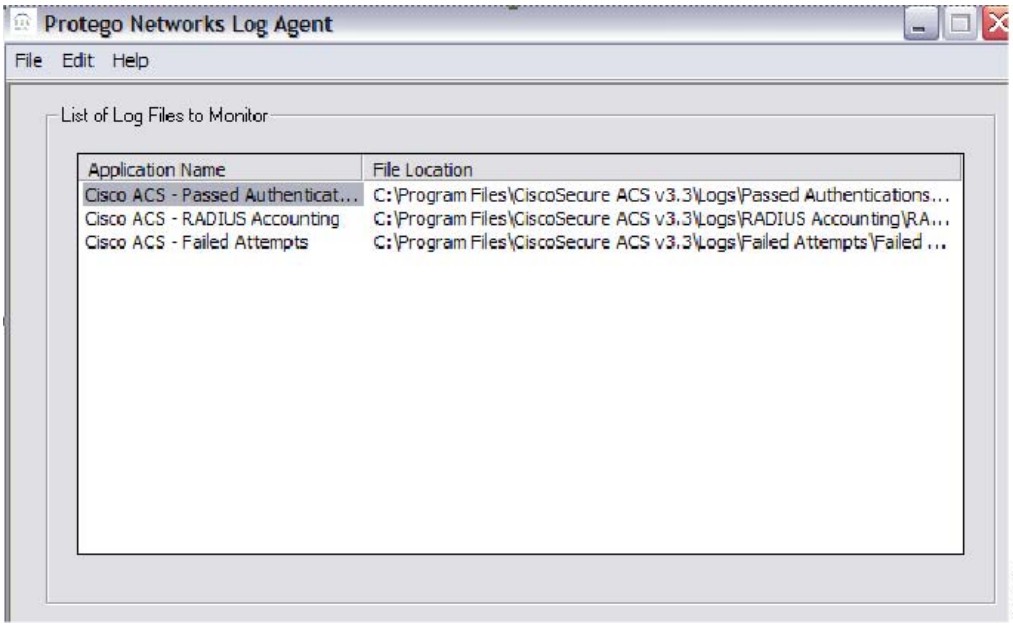
The Open dialog box appears.



Step 9 Add all 3 applications and their active log files:

- Failed Attempts active
- Passed Authentications active
- RADIUS Accounting active

The configured files appear in the List of Log Files to Monitor list.



Step 10 Select **File > Activate**.

Upgrade PN Log Agent to a Newer Version

You can determine which version of the PN Log Agent is running on your server by selecting Help > About in the PN Log Agent Configuration dialog box. This program is updated independently of the MARS Appliance software updates. Therefore, the version number does not correspond to any release of the MARS Appliance software.

Note Beginning with the 4.1.3 release of the pnLog agent, the agent requires a minimum of Cisco Security Monitoring, Analysis, and Response System, release 4.1.3 running on the appliances to which it is reporting in order to operate correctly.

To upgrade to the new PN Log Agent from an existing installation, you must perform the following steps:

Step 1 On the Cisco Secure ACS or syslog server where PN Log Agent is running, uninstall the old agent.

a. To uninstall the old agent, click **Start > Control Panel > Add/Remove Programs** .

b. Select **PnLogAgent** in the list of currently installed programs, and click **Remove** .

c. Select **Yes** to confirm the removal.

Step 2 Reboot the server.

Step 3 Install the new agent. You can download this tool from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

Step 4 Re-configure the new agent, specifying the list of files and IP address of the MARS Appliance, etc.

For information on configuring the pnLog Agent, see Install and Configure the PN Log Agent, page 26-8.

Application Log Messages for the PN Log Agent

The PN Log Agent service writes events to the Application Log of Event Viewer on the Cisco Secure ACS server. The agent, identified in the log messages as PNLogAgentService, writes status messages, such as successful service start and stop. It also writes error messages for incomplete configuration and error conditions, such as when the service is out of memory.

Table 26-1 categories the types of messages that can occur and explains their affects on the PNLog Agent service.

Table 26-1 Possible Application Log Messages for PN Log Agent

Type/Message	Effect on Service/Cause of Error
Fatal Errors	
Failed to start thread to monitor file.	Windows errors or configuration errors that will stop the service
The service failed to monitor the configured file. Please check service privileges.	
The service failed to obtain path from log file name and shall exit the thread now!	
The service failed to get the CS-MARS device IP Address. Please use the PnLogAgent to configure it.	
The service has detected an invalid IP address. Please use the PnLogAgent to configure the correct IP Address for CS-MARS.	
Error	
Network detected to be down while attempting to send syslog message	Network connectivity errors that will cause the service to not send syslog messages, but will keep the service running
Destination network unreachable while attempting to send syslog message	
Network dropped connection on reset condition while attempting to send syslog message	
Connection reset by peer while attempting to send syslog message	
Connection refused by target while attempting to send syslog message	
No route exists to host. Please check the network connectivity	
Attempt to send syslog returned error code: <error_code>	
The log file doesn't have all required attributes. Attribute missing: <missing_attribute>	Error in configuration
The number of attributes in the file header don't match the number of attributes in the value. Hence this log entry shall not be sent to CS-MARS.	
The service detected that the configured file is missing some mandatory header attributes. A list of mandatory attributes is available in the CS-MARS user documentation.	
The service failed to read the file pnWinEvent.dat and will now wait for an update to the configuration.	
Failure in reading from pnWiinEvent.dat. Service will wait for an update	

Table 26-1 Possible Application Log Messages for PN Log Agent (Continued)

Warning	
The attribute <attribute_name> has a value that exceeds the CS-MARS limit for an individual attribute value and shall be split.	Warning in case some attribute data in the file exceeds MARS raw message length... MARS will store the data after splitting it into multiple events
Informational	
PnLogAgentService started	Informational messages describing expected operations for the service.
PnLogAgentService Exiting	
The service read the configuration and will attempt to process files.	
As the service has no logs configured, it shall wait for an update	
Exiting thread processing file as service stop received!	

Add and Configure an Cisco Secure ACS Server in MARS

To add the host and Cisco Secure ACS software application to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

You can also select **Add SW Security apps on an existing host** if you have already defined the host within MARS, perhaps as part of the Management > IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

Step 3 In the Device Name field, enter the hostname of the server or the remote logging host.

Step 4 In the Reporting IP field, enter the IP address of the interface in Cisco Secure ACS server or the remote logging host from which the syslog messages will originate.

Step 5 In the Operating System field, select **Windows**.

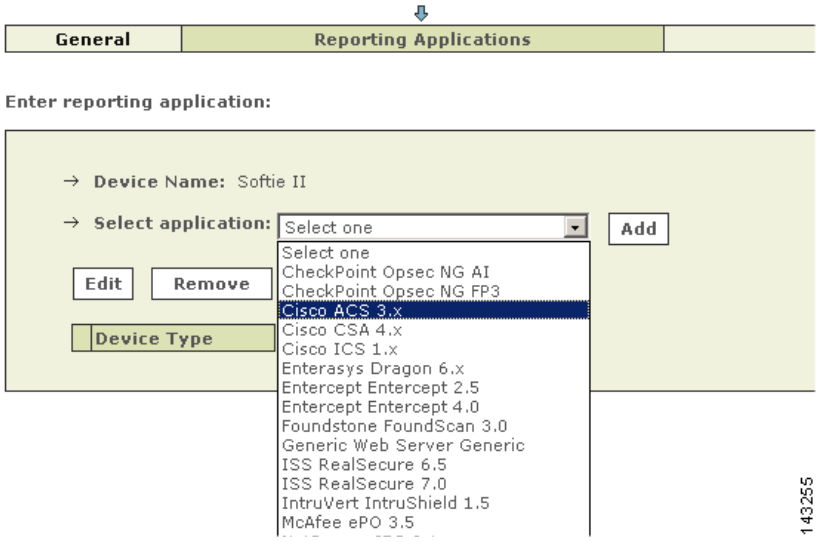
Cisco Secure ACS SW runs only on a Windows host. Windows 2000 and Windows 2003 are the supported platforms for Cisco Secure ACS.

Step 6 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in Cisco Secure ACS server or remote logging host from which the syslog messages will originate.

This address is the same value as the Reporting IP address.

Step 7 Click **Apply**.

Step 8 Click **Next** to move the Reporting Applications tab.



Step 9 In the Select Application box, select **Cisco ACS 3.x** or **Cisco ACS 4.x**, and then click **Add**.

The Cisco ACS Windows Requirements page appears.

- (3.x) This page explains that you must have installed an agent on the server as described in Install and Configure the PN Log Agent, page 26-8.
- (4.x) This page explains that you must either have enabled the ACS device to publish syslogs to MARS as described in Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3. The PNLog agent *cannot* be used to support the 4.x devices.

Step 10 Click **Submit** to add this application to the host.

`Cisco ACS 3.x` appears in the Device Type list.

Step 11 Click the **Vulnerability Assessment Info** link to define the host information that MARS uses to determine false positive attacks against this host. Continue with Define Vulnerability Assessment Information, page 36-12.

Step 12 Click **Done** to save the changes.

The new host appears in the Security and Monitoring Information list.

Step 13 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Add and Configure a Cisco Secure ACS Solutions Engine in MARS

MARS supports the native syslog format for the Cisco Secure ACS Solutions Engine (SE), version 4.x and later. This topic explains how to configure MARS so that it can parse the syslogs it receives from the Cisco Secure ACS SE device.

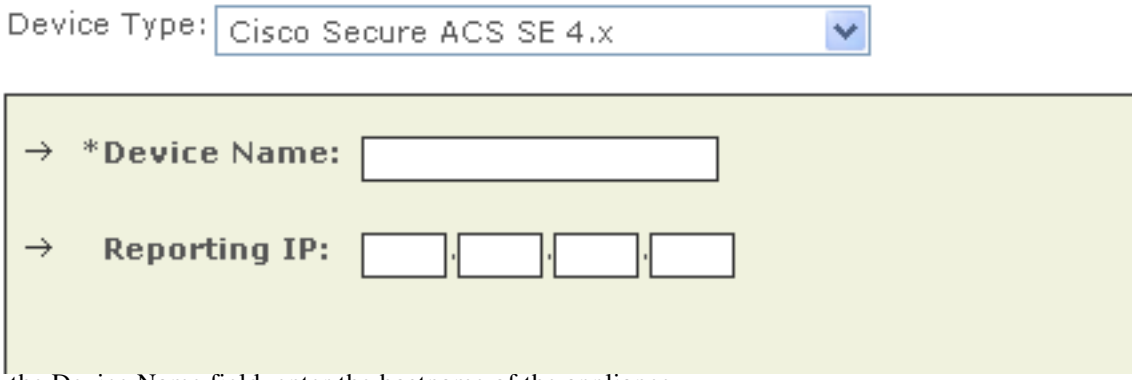
Before You Begin

You must either have enabled the ACS SE device to publish syslogs to MARS as described in Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3. The PNLog agent *cannot* be used to support the 4.x devices.

To add the host and Cisco Secure ACS SE appliance to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Cisco Secure ACS SE 4.x**.



Step 3 In the Device Name field, enter the hostname of the appliance.

Step 4 In the Reporting IP field, enter the IP address of the interface in Cisco Secure ACS appliance from which the syslog messages will originate.

Step 5 Click **Submit** to add this application to the host.

`Cisco ACS SE 4.x` appears in the Security and Monitoring Information list.

Step 6 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Troubleshooting Cisco Secure ACS Integration

To verify that MARS is receiving event data from a Cisco Secure ACS, use one of the following options:

- When you configure PN Log Agent, verify that the logs show up in the list of configured files and that you were able to click Activate without errors. If errors occur, verify that you have configured the options as defined in Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4.
- Use TCPDUMP at the MARS CLI to verify that MARS is receiving syslog traffic on port 514 from the PN Log Agent running on the Cisco Secure ACS or remote logging host.
- Use the web interface to submit an inline query to determine whether events are being received from the Cisco Secure ACS. The query definition should include the 'All matching events' option as the Result Format value and Real Time as the Filter By Time value.
- When upgrading to Cisco Secure ACS 4.1, the location of the log files changes. To address this issue, you must reconfigure the PN Log Agent to point to the new folders.

Error Messages

The service detected that the configured file is missing some mandatory header attributes.

Issue: It is possible receive an error in the Application Log accessed using the Event Viewer that states the following:

```
Event Type: Error
Event Source: pnLogAgentService
Event Category: None
Event ID: 1
Date:  9/7/2006
Time:  12:00:53 AM
User:  N/A
Computer: ACS1
Description:
LogEventService: The service detected that the configured file is missing some mandatory header attributes. A
list of mandatory attributes is available in the CS-MARS user documentation.
```

This error is not accompanied with any advice about how to resolve the error and PN Log Agent indicates no errors during configuration. The cause of this error messages is that when the log file changes at midnight, the file header is not written out until an event is generated. Thus, when the PN Log Agent service detects that the logs are missing headers, it generates the error.

Resolution: You can safely ignore such errors that re-occur daily around the same time (around midnight) as long as the MARS Appliance still receives events from the he Cisco Secure ACS or remote logging host. If you are otherwise receiving this message, it indicates that you have not properly configured the Cisco Secure ACS to generate events required by the PN Log Agent. Verify that you have configured the options as defined in Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4.

PART 11

Intrusion Detection and Prevention (Host based)

CHAPTER 27

Cisco Security Agent 4.x and 5.x Device

Revised: November 14, 2008

To enable Cisco Security Agent (CSA) as a reporting device in MARS, you must identify the CSA Management Console (CSA MC) as the reporting device. The CSA MC receives alerts from the CSA agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the CSA agent that originally triggered the event, rather than the CSA MC that forwarded it. Therefore, MARS requires host definitions for each of the CSA agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the CSA MC.

As of MARS, release 4.1.1, the MARS Appliance discovers CSA agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the CSA agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the CSA MC as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the CSA MC; however, you are not required to define each agent. The default topology presentation for discovered CSA agents is within a cloud.

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

Prior to 4.1.1., you were required to manually add each agent or by using an exported hosts file, as defined in Export CSA Agent Information to File, page 27-2.

Note Prior to the 4.1.1 release, CSA was identified by the device type name *Cisco CSA 4.0* . As part of an upgrade, any Cisco CSA 4.0 devices were renamed as *Cisco CSA 4.x*. This new name includes support for Cisco CSA 4.0 and 4.5.

This chapter contains the following topics:

- Configure CSA Management Center to Generate Required Data, page 27-2
- Add and Configure a CSA MC Device in MARS, page 27-3
- Troubleshooting CSA Agent Installs, page 27-6

Configure CSA Management Center to Generate Required Data

To bootstrap CSA, you must configure the CSA MC to forward SNMP notifications to the MARS Appliance. In addition, you can export the list of CSA agents in a format that MARS can import. However, this export operation is not necessary, as MARS discovers the agents as they generate notifications.

This section contains the following topics:

- Configure CSA MC to Forward SNMP Notifications to MARS, page 27-2
- Export CSA Agent Information to File, page 27-2

Configure CSA MC to Forward SNMP Notifications to MARS

The only required configuration is to ensure that CSA MC forwards the SNMP notifications that it receives from agents to MARS. From these notifications, MARS is able to discover the agent and its relevant settings. It is also from these events that MARS learns about the host-level activities transpiring on your network.

To forward all notifications to the MARS Appliance, follow these steps:

Step 1 Log in to the CiscoWorks Server desktop.

Step 2 From the navigation tree, select **VPN/Security Management Solution > Management Center > Security Agents**.

Step 3 In the Management Center screen, click the **Alerts** link.

Step 4 Click **New**.

Step 5 In the Name and Description fields, enter a name and description for the SNMP notification.

Step 6 Scroll down and select the **SNMP** check box.

Step 7 In the Community name field, enter the SNMP notification's community name.

Step 8 In the Manager IP address field, enter the MARS's IP address.

Step 9 Click **Save** and exit the program.

Export CSA Agent Information to File

With the release of MARS 4.1.1, you are no longer required to define each Cisco CSA agent, as they are discovered as a device sends an SNMP notification to the CSA Management Console (CSA MC).

Note The following instructions apply to Cisco CSA 4.x when Microsoft Internet Explorer is used to access the CSA MC web interface.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

To export the all hosts report as a tab-delimited file, follow these steps:

Step 1 Log in to the CSA MC by accessing the console using the fully qualified domain name in the URL.

When accessing the CSA MC, you must use a fully qualified domain name in the URL. If you use the CiscoWorks Desktop to launch CSA MC, the ActiveX reports do not display.

Step 2 Click **Reports > Host Details**.

Step 3 Click **New**.

Step 4 In Groups, choose **<All Hosts>**, in Viewer Type, choose **ActiveX (IE only)**.

Step 5 Click **View report**.

A window appears that contains the host details.

Step 6 Click **Export**, and select export to an **Excel 5.0 Document** type.

Step 7 In the **Name** box, identifies the name for the file that you are exporting, for example, csahosts.xls.

Step 8 Open the exported file in Excel, and click **File > Save As...**

Step 9 In the Save as type box, click **Text (Tab delimited) (*.txt)**.

Step 10 In the File name box, enter the name for this file, for example, csahosts.txt, and click **Save**.

Step 11 Upload the generated file to an FTP server where the MARS Appliance can access it.

You will return to this file when adding the CSA device n the MARS web interface, as defined in Add and Configure a CSA MC Device in MARS, page 27-3.

Add and Configure a CSA MC Device in MARS

Before you can identify the agents, you must add the CSA MC to MARS. All CSA agents forward notifications to the CSA MC, and the CSA MC forwards SNMP notifications to MARS. Once you define the CSA MC and activate the device. MARS can discover the agents that are managed by that CSA MC. However, you can also chose to manually add the agents.

To add a CSA MC to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click on **Reporting Applications** tab.

Step 6 From the Select Application list, select one of the following values:

- **Cisco CSA 4.x.**
- **Cisco CSA 5.x**

Note As of the 4.3.1 and 5.3.1 releases of MARS, CSA 5.x is supported.just as 4.x is supported (including agent discovery.

Step 7 Click **Add**.

The Management Console page appears.

Step 8 Do one of the following:

- To save your changes and allow the CSA agents to be discovered automatically, click **Submit**, and then click **Done**.
- To add agents using an exported hosts report, continue with Add CSA Agents From File, page 27-5.
- To add a single agent manually, continue with Add a CSA Agent Manually, page 27-4.

Add a CSA Agent Manually

You can manually add a CSA Agent as a child of the CSA MC. This feature allows you to represent all of your agents, even if they have not generated any notifications.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

To add CSA agents manually, follow these steps:

Step 1 Click **Admin > Security and Monitoring Devices**.

Step 2 From the list of devices, select the host running Cisco CSA Management Center, and click **Edit**.

Step 3 Click the **Reporting Applications** tab, select **Cisco CSA Management Center** in the Device Type list, and click **Edit**.

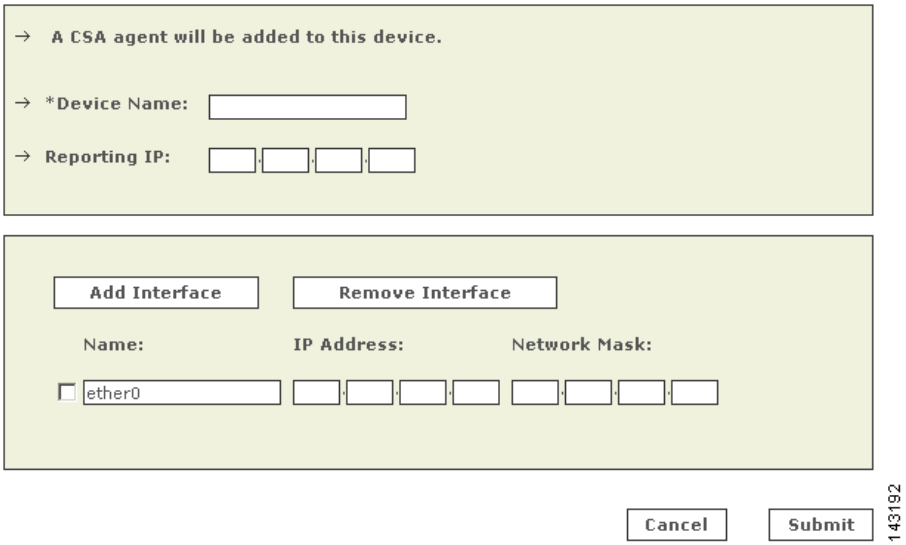
Step 4 Click the **Add Agent**.

Step 5 Do one of the following:

- Select the existing device, click **Edit Existing**, and continue with Step 8.

  A page displays with the values pre-populated for hostname, reporting IP address, and at least one interface.

- Click **Add New**, and continue with Step 6.



Step 6 In the Device Name field, enter the hostname on which this CSA agent resides.

This value should reflect the DNS entry for this device.

Step 7 In the Reporting IP field, enter the IP address that the agent uses to send logs to the CSA MC.

Step 8 Define each interface that is configured for this host by specifying the interface name, IP address, and network mask. To add a new interface, click **Add Interface**.

The interface settings are used for attack path calculation. It is very important that you identify any dual-homed hosts by defining each interface.

Step 9 Click **Submit**, and then click **Done**.

Step 10 To activate this device, click **Activate**.

Add CSA Agents From File

You can add the complete list of hosts on which CSA Agents are installed by exporting the all hosts report from CSA MC and importing that file into MARS. The only advantage to adding agents using an export file is that the first notification received that originates from the agent is not attributed to the CSA MC.

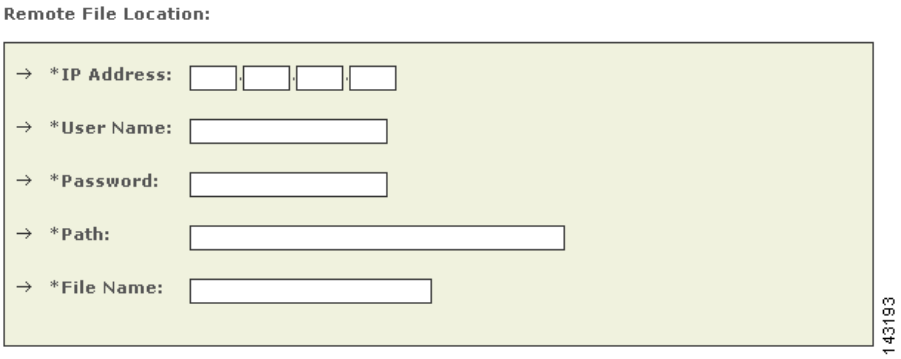
To add CSA agents from a file, follow these steps:

Step 1 Click **Admin > Security and Monitoring Devices**.

Step 2 From the list of devices, select the host running Cisco CSA Management Center, and click **Edit**.

Step 3 Click the **Reporting Applications** tab, select **Cisco CSA Management Center** in the Device Type list, and click **Edit**.

Step 4 Click **Load From File**.



Caution The file should be formatted as a tab delimited file. You cannot use a CSV file. To generate a tab delimited file of the CSA agents managed by the CSA MC, see Export CSA Agent Information to File, page 27-2.

Step 5 In the IP Address field, enter the address of the FTP server where you stored the exported hosts file, as described in Export CSA Agent Information to File, page 27-2.

Step 6 In the User Name field, enter the name of the account used to authenticate to the FTP server.

Step 7 In the Password field, enter the password that corresponds to the account specified in Step 6.

Step 8 In the Path field, enter the path to the folder where the file is stored. If this file is stored in the root folder, you must specify a backslash (\) in this field. The format of this value is ***\<path_here>*** .

Step 9 In the File Name field, enter the name of the tab delimited file.

Step 10 Click **Submit**.

The following message displays and the hosts are added as agents of the CSA MC:

```
Success:
Status: OK
```

Step 11 Click **Done**.

Troubleshooting CSA Agent Installs

When importing CSA agents from a file, the following messages can occur.

Table 27-1 Error and Status Messages when Importing CSA Agents from File

Message	Description/Issue
Status: NumberFormatException occurred parsing the file at line X	Occurs when you have a CSV file rather than a tab delimited file. The line number varies.

Table 27-1 Error and Status Messages when Importing CSA Agents from File (Continued)

Error Occurred: Status: DbDevice occurred parsing the file at line -1	Occurs when duplicate files are imported, even if you have deleted all of the agents and the CSA MC.
Success: Status: OK	Indicates a successful import of CSA agents using the tab-delimited file.
Error Occurred: Status: FileNotFoundException	Indicates that the file does not exist at the specified path. If the path is at the root of your FTP server, verify that you have included \ as the path value.
Error Occurred: Status: NoRouteToHostException	Indicates that the identified FTP server is not reachable from the MARS Appliance. You may need to define additional routes or enable traffic flows to ensure the connection is allowed.

CHAPTER 28

Entercept Entercept 2.5 and 4.0

To configure Entercept in MARS, you must perform the following tasks:

1. Generate CSV file that identifies each of the Entercept hosts by logging into the host running the Entercept console and copying the data out of the database table.
2. Configure the Entercept console to send SNMP traps to the MARS Appliance
3. Identify the events that should be generated as SNMP traps.
4. Define a host that represents the management console (Entercept console) in MARS web interface.
5. From that host in the MARS web interface, import the CSV seed file to identify the Entercept agents running on other hosts.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

This chapter contains the following topics:

- Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5), page 28-1
- Define the MARS Appliance as an SNMP Trap Target, page 28-2
- Specific the Events to Generate SNMP Traps for MARS, page 28-2
- Add and Configure an Entercept Console and its Agents in MARS, page 28-3

Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5)

Note Entercept agent information is saved in a database file on the Entercept console.

When you configure the MARS box to add Entercept agents, you can extract them from the database file on the Entercept console, instead of typing the mapping for each agent.

Create a CSV file for Entercept Agents in Version 2.5

Step 1 Go to the directory ***Program Files\Cisco IDS\Console\Database*** and copy the file ***CoreShield.mdb*** to another directory, e.g.: ***C:\temp***.

Step 2 Open the copied ***CoreShield.mdb*** with Microsoft Access, and go to the "Agents" table.

Step 3 Export the table to a file named: ***Agents.txt*** and choose the exported file format to be CSV.

Step 4 Copy ***Agents.txt*** to a specific directory that is ready for the MARS box to load.

```
   A sample agents.txt file could be:
1,3,"entercept1",6,1,1,1,438,1,"127.0.0.1",0,,1051055867,2086

where the fields are: AgentID, AgentTypeID, ComputerName, ComputerType,
NewFlag, StatusID, OperatingModeID, VersionID, VersionModeID, IP,
License, Note, NoConnection, and UpTime.
```

Define the MARS Appliance as an SNMP Trap Target

Step 1 Log in to the Entercept Console.

Step 2 Click **Configuration**.

Step 3 Click the **Address Book** tab.

Step 4 In the All Contacts tree, click **SNMP Trap**.

Step 5 Click the **Plus (+)** button.

Step 6 In the New SNMP Trap page, specify the following values:

- **Alias**—Enter an name for the MARS Appliance.
- **Privilege Level**—Set to Global.
- **Status**—Set to Enabled.
- **Name**—Enter the MARS Appliance's name if the DNS server can resolve the name. Otherwise, use its IP address.
- **Community**—Enter a community string name,
- **Port**—Enter the SNMP port number used by the MARS Applaince.
- **Protocol**—Select SNMP.

Specific the Events to Generate SNMP Traps for MARS

Step 1 Click the **Notifications** tab.

Step 2 Click the **Plus (+)** button.

Step 3 On the General tab, in the name field, enter a name for the notification.

Step 4 Click the **Agent Groups** tab and select the **All Agents** radio button.

Step 5 Click the **Security Events** tab and select the **Events by Severity Levels** radio button. Select the events that you want (High, Medium, Low, and Information).

Step 6 Click the **System Events** tab and select the **Events by Severity Levels** radio button. Select the events that you want (Error, Warning, and Information).

Step 7 Click the **Address Book** tab and click a destination in the Available Destinations field. Click the **Down arrow** to move it into the Selected Destinations field.

Step 8 Click **OK** and exit the program.

Add and Configure an Entercept Console and its Agents in MARS

Adding an Entercept device has two distinct steps. First, you add configuration information for the for the Entercept Console host. Second, you add the agents managed by that console.

This section contains the following topics:

- Add the Entercept Console Host to MARS, page 28-3
- Add Entercept Agents Manually, page 28-4
- Add Entercept Agents Using a Seed File, page 28-4

Add the Entercept Console Host to MARS

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click on **Reporting Applications** tab.

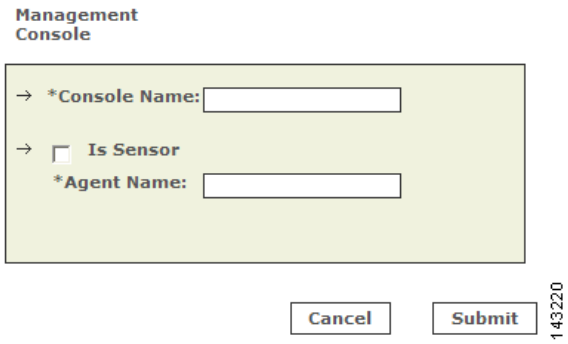
Step 6 From the Select Application list, select Entercept 2.5 or 4.0

Step 7 Click **Add**.

Step 8 Enter the Console Name.

Step 9 Check the **Is Sensor** check box, which identifies the deivce as a sensor.

Step 10 Enter the sensor's **Agent Name**, which is the agent name for the console if it is an agent.



Step 11 Click **Submit**.

You can now add the agents.

Add Entercept Agents Manually

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

Step 1 Click **Add Agent**.

Step 2 Select the device that already has agent running or **Add New**.

Step 3 If you selected Add New, then specificy the following values:

- **Device Name**
- **Agent Name**
- **Reporting IP**
- For the first interface, enter an IP address and mask.
- For multiple interfaces, click **Add Interface**, and add the new interfaces' IP address and mask.

Step 4 Click **Submit** .

Add Entercept Agents Using a Seed File

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

Step 1 Click **Load From CSV**.

Step 2 Enter the FTP server information and location of the CSV (comma separated values) file.

- If you need to generate the Entercept Agent CSV file, see Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5), page 28-1.

Step 3 Click **Submit**.

PART 12

Virus Protection

CHAPTER 29

Symantec AntiVirus Configuration

To enable a Symantec AntiVirus agent as a reporting device in MARS, you must identify the Symantec System Center console as the reporting device. The Symantec System Center console receives alerts from the AV agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the AV agent that originally triggered the event, rather than the Symantec System Center console that forwarded it. Therefore, MARS requires host definitions for each of the AV agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the Symantec System Center console.

The MARS Appliance discovers AV agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the AV agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the Symantec System Center console as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the Symantec System Center console; however, you are not required to define each agent. The default topology presentation for discovered AV agents is within a cloud.

Note The first SNMP notification from an unknown AV agent appears to originate from the Symantec System Center console. MARS parses this notification and defines a child agent of the Symantec System Center console using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the AV agent.

Prior to 4.2.1, you were required to manually add each agent or by using an exported agent list, as defined in Export the AntiVirus Agent List, page 29-7. Beginning in release 4.2.1, the MARS Appliance discovers AV agents as they generate alerts.

Configuring the Symantec AntiVirus integration requires performing two tasks:

- Configure the AV Server to Publish Events to MARS Appliance, page 29-2
- Add the Device to MARS, page 29-8

In addition, you can perform the following task to expedite populating the Agent list in MARS:

- Export the AntiVirus Agent List, page 29-7

Configure the AV Server to Publish Events to MARS Appliance

To configure the AV server to publish events to MARS, follow these steps:

Step 1 Log in to the Windows server running Symantec AV.

Step 2 To identify the Local Controller as a valid SNMP trap destination, click **Administrative Tools > Services > SNMP Service > Traps > Trap destinations**.

Step 3 Enter the IP address of the Local Controller in the Trap Destination page, and click **OK** to close all open windows.

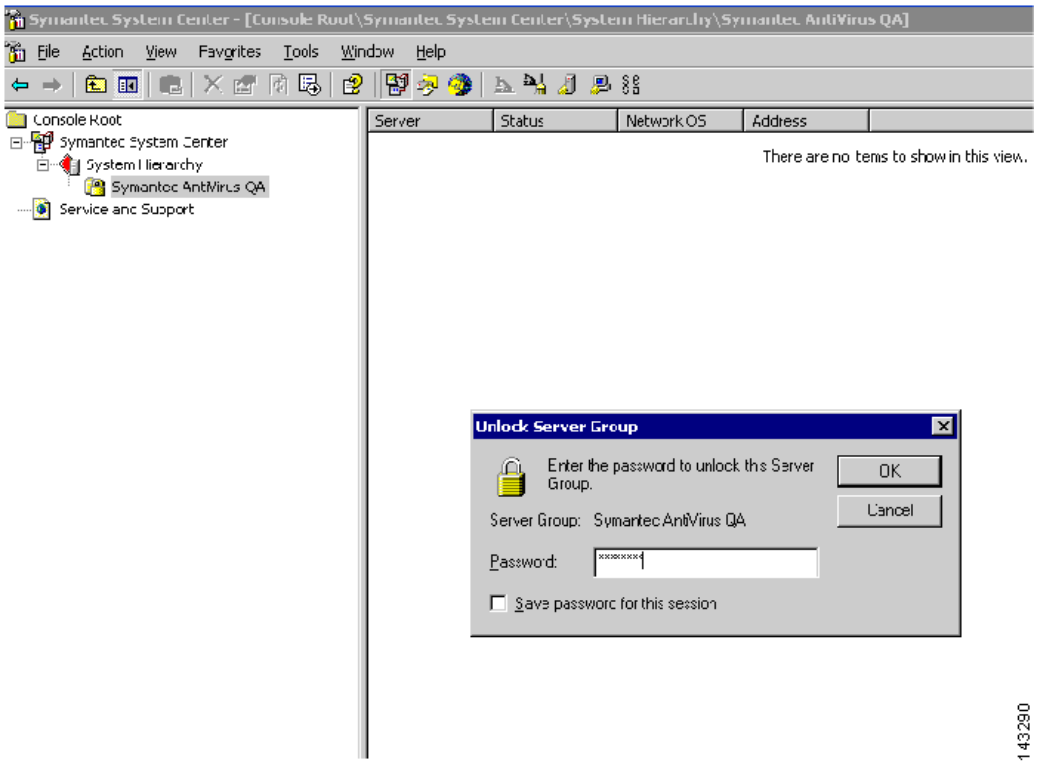
Step 4 Select **Start > All Programs > Symantec System Center Console**.

Step 5 In the Symantec System Center window, click **System Hierarchy**.

Step 6 Under System Hierarchy, right-click the appropriate server group name and unlock the server group by supplying the configured password.

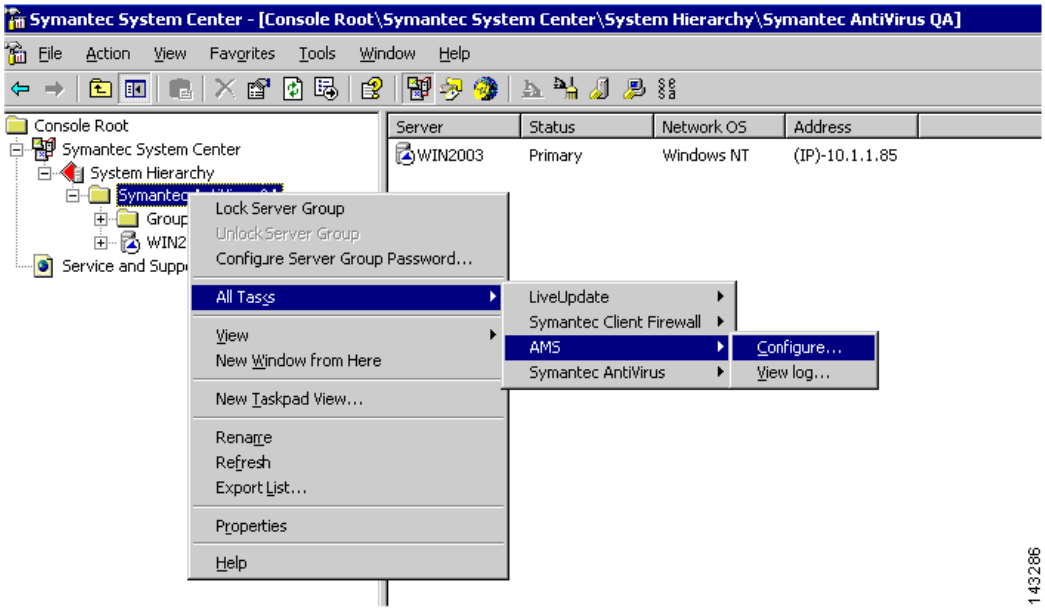
Unlocking the server enables you to configure it.

Figure 29-1 Symantec Unlock Server



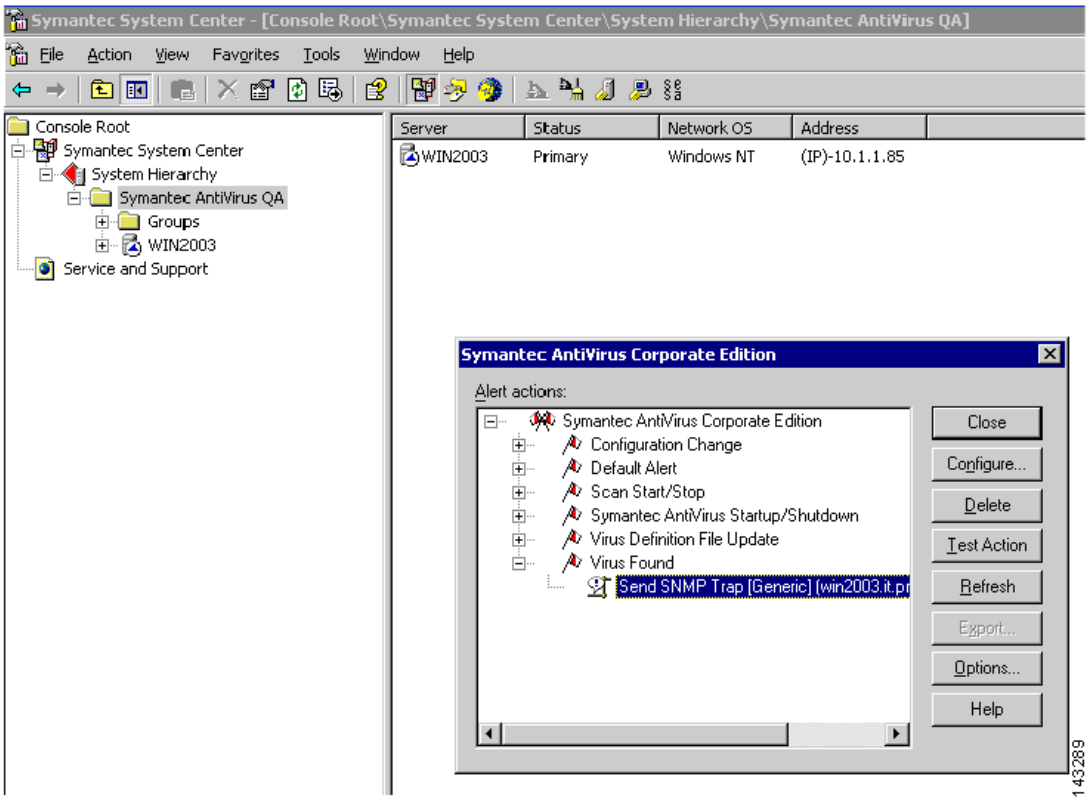
Step 7 Configure Symantec server (AMS-Alert Management System) to send SNMP traps to MARS. Right click the unlocked server group name, then select **All Tasks > AMS > Configure**.

Figure 29-2 Symantec AV AMS



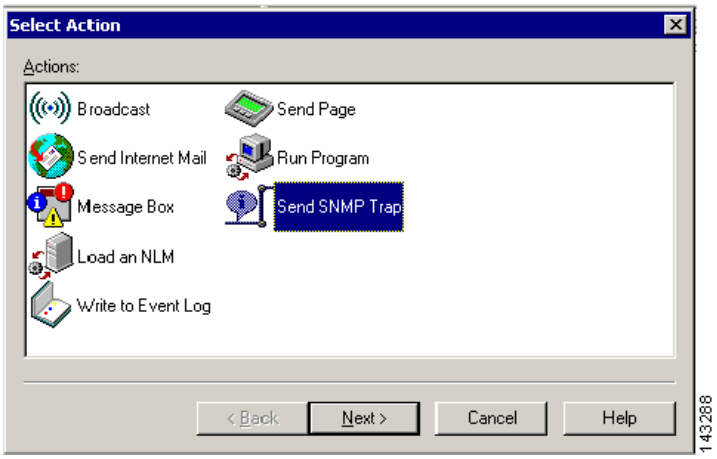
Step 8 Select **Send SNMP Trap** under each Alert Action, then click **Configure**.

Figure 29-3 Symantec AV Trap



Step 9 Click **Send SNMP trap**, and then click **Next**.

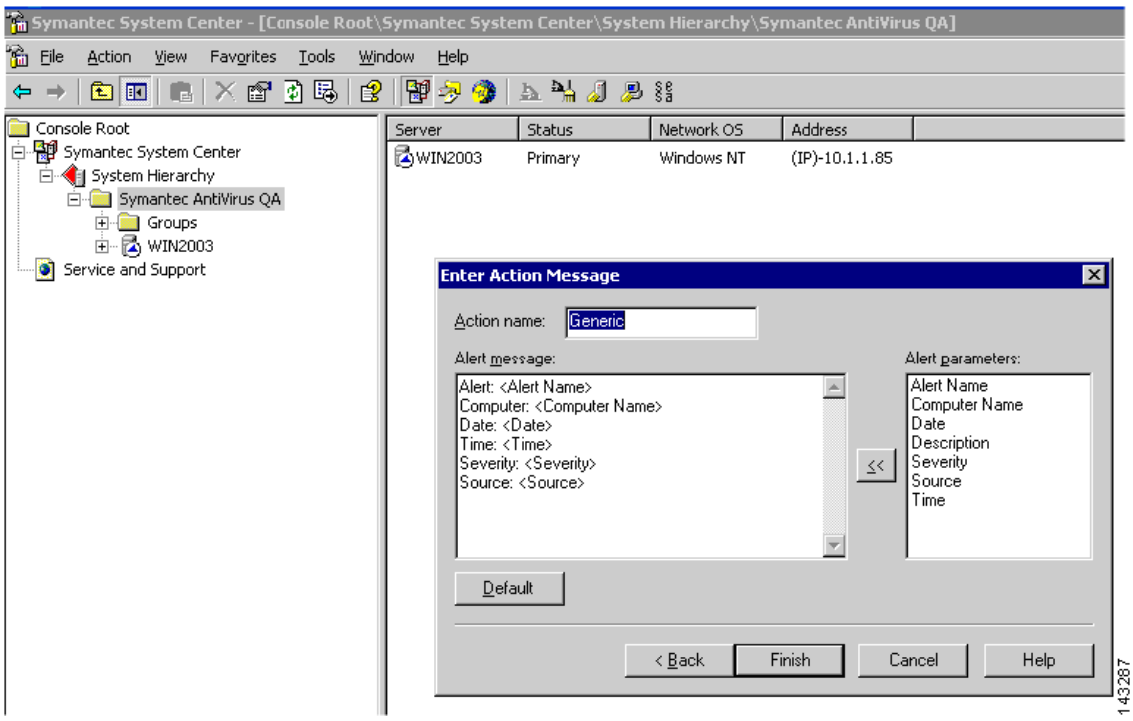
Figure 29-4 Symantec AV Send SNMP Trap



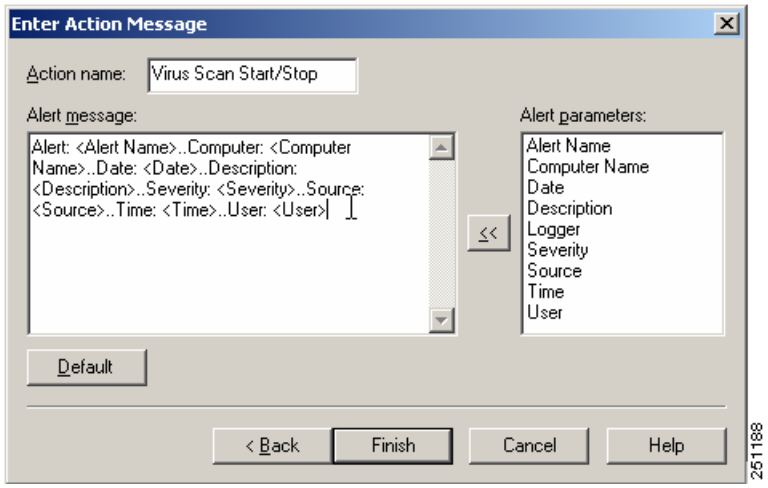
Step 10 Select the Local Controller to send the SNMP trap to as defined in Step 3, and then click **Next** to view the Action Message window.

Step 11 Add alert parameters to the Alert message list according to the following information:

Figure 29-5 Symantec AV Action Msg



The following mandatary fields are required for MARS to parse AV traps. If these fields are among those possible, you must define these fields in order before defining any of the optional fields.



Note For MARS Appliance models 25, 55, 110, 210, and GC2, do not include a CR/LF (Enter key) in the action message.

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Action: <*Actual Action* >
- Description: <*Description* >

Note This ordering is required is because some optional fields can be so long as to prevent Mars from correctly parsing the mandatory fields if they do not appear first in the list of attributes.

The following optional fields can be defined after all mandatory fields are defined:

- User: <*User* >
- Virus Name: < *Virus Name* >
- File Path: <*File Path* >
- Severity: <*Severity* >
- Source: <*Source* >

The following list identifies the trap type and the full list of possible fields:

Alert: Virus Found

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Action: <*Actual Action* >

- Severity: <*Severity* >
- Source: <*Source* >
- File Path: <*File Path* >
- Logger: <*Logger* >
- Requested Action: < *Requested Action* >
- User: <*User* >
- Virus Name: <*Virus Name* >

Alert: Virus Definition File Update

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Description: <*Description* >
- Severity: <*Severity* >
- Source: <*Source* >

Alert: Symantec AntiVirus Startup/Shutdown

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Description: <*Description* >
- Severity: <*Severity* >
- Source: <*Source* >

Alert: Scan Start/Stop

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Severity: <*Severity* >
- Source: <*Source* >
- Source: <*Source* >
- Logger: <*Logger* >
- User: <*User* >

Alert: Scan Start/Stop

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >

- Description: <*Description* >
- Severity: <*Severity* >
- Source: <*Source* >
- Logger: <*Logger* >

Alert: Default Alert

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Severity: <*Severity* >
- Source: <*Source* >
- Failed Alert: <*Failed Alert* >

Alert: Configuration Change

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Severity: <*Severity* >
- Source: <*Source* >
- Failed Alert: <*Failed Alert* >

Alert: Configuration Change

- Alert: <*Alert Name* >
- Computer: <*Computer Name* >
- Date: <*Date* >
- Time: <*Time* >
- Description: <*Description* >
- Severity: <*Severity* >
- Source: <*Source* >

Step 12 Repeat Step 8 through Step 11 for each alert event.

Export the AntiVirus Agent List

While MARS discover the list of anitvirus agents that report to the Symantec System Center console automatically, you can export the list of Symantec AntiVirus Clients and Agents as a CSV file (*.csv), which enables you to use the CSV file to manually load the agents into MARS. For more information on adding agents from the file, Add Agents from a CSV File, page 29-9. This approach is much faster than if you had to identify the agents manually.

To generate the CSV file, follow these steps:

Step 1 Select = **View > Default Console View** to ensure the generated CVS file will be based on the Console Default View.

Step 2 Right-click the name of the server that you want to export, choose **Export List**, and save it as Text (Comma Delimited) (*.csv) file.

Step 3 Copy the file to an FTP server that the MARS Appliance can access.

You will use this file when you add the AntiVirus agents within the web interface.

Add the Device to MARS

Before you can identify the agents, you must add the Symantec System Center console to MARS. All AntiVirus agents forward notifications to the Symantec System Center console, and the Symantec System Center console forwards SNMP notifications to MARS. Once you define the Symantec System Center console and activate the device. MARS can discover the agents that are managed by that Symantec System Center console. However, you can also chose to manually add the agents.

Tip For Symantec AntiVirus, the Symantec agent hostname (AV client computer name) appears in the "Reported User" column of the event data. Therefore, you can define a query, report or rule related to this agent based on the "Reported User" value.

To add the host and application configuration information, follow these steps:

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

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

Step 3 To add a new host, enter the device name and IP addresses.

Step 4 Cclick **Apply**.

Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select one of the following values:

- **Symantec AntiVirus 9.x**
- **Symantec AntiVirus 10.x**

Step 7 Click **Add**, then add the agents.

Step 8 Done one of the following:

- To save your changes and allow the AntiVirus agents to be discovered automatically, click **Submit** , and then click **Done**.
- To add agents using an exported seed file, continue with Add Agents from a CSV File, page 29-9.
- To add a single agent manually, continue with Add Agent Manually, page 29-9.

Add Agent Manually

MARS can automatically discover agents or you can manually add them one at a time or in bulk using a CSV file (see Add Agents from a CSV File, page 29-9.) This topic explains how to manually add a single agent. The value of defining an agent is that is accelerates the discover process; however, it is not required.

To add an agent manually, follow these steps:

Step 1 Click **Add Agent**.

Step 2 Select the existing device or click **Add New**.

Step 3 Enter the following information for new device.

- **Device Name**—The DNS entry for this device.
- **Reporting IP**—The IP address that the agent uses to send logs to the console.

Step 4 Under the Interfaces list, specify the IP address and netmask values asscoaited with each interface installed in the host on which the agent is running.

MARS uses interface information to calculate attack paths.

Step 5 Click **Submit**.

Add Agents from a CSV File

You can generate a CSV file that contains the list of agents managed by the Symantec AV server as defined in Export the AntiVirus Agent List, page 29-7. Once the file is generated, you can use the file to import the list of agents into the MARS web interface as child modules of the Symantec AV server.

Note Other population options exist: MARS can automatically discover agents (default) or you can manually add them one at a time (see Add Agent Manually, page 29-9.)

To import the list of AV agents into MARS. follow these steps:

Step 1 Click **Load From CSV**.

Step 2 Enter the FTP server information and location of the CSV (comma-separated values) file.

Step 3 Click **Submit**.

CHAPTER 30

McAfee ePolicy Orchestrator Devices

The McAfee ePolicy Orchestrator (ePO) is a central management application for many McAfee product. Antivirus (AV) devices provide detection and prevention against known viruses and anomalies, as do host-based IPS solutions. MARS is able to receive event data about the following devices that can be managed by ePO:

- McAfee VirusScan 8.0(I)/8.5(I)
- McAfee HIPS 6.0 (via ePO 3.6.x)
- McAfee HIPS 7.0 (via ePO 4.0)

Configuring MARS to receive and process the data generated by a McAfee ePolicy Orchestrator server requires you to perform two procedures.

- Configure the ePO server to forward SNMP traps to MARS
- Define the ePO server in the MARS web interface
- (Optional) Export a list of ePO agents from the ePO server and import that list as agents of the ePO server you defined in MARS. This step is not required as the list of managed agents is dynamically discovered by MARS as the ePO server forwards events generated by the agents.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

This chapter contains the following topics:

- Configure ePolicy Orchestrator 4.0 to Generate Required Data, page 30-1
- Configure ePolicy Orchestrator 3.5 and 3.6 to Generate Required Data, page 30-6
- Add and Configure ePolicy Orchestrator Server in MARS, page 30-10

Configure ePolicy Orchestrator 4.0 to Generate Required Data

To prepare the ePolicy Orchestrator server to forward SNMP events to MARS, follow these steps:

Step 1 Select **Start > Program Files > Network Associates > ePolicy Orchestrator 4.x Console**.

Step 2 In the tree, select **McAfee Security > ePolicy Orchestrator**, and click the **Log on to server** link under Global Task List.

Step 3 In the Log On to Server dialog box, enter the user name and password required to access the ePolicy Orchestrator server, and click **Log on**.

Step 4 Click **Automation**, and then click the **SNMP Servers** subtab.

Step 5 Click **New SNMP Server**.

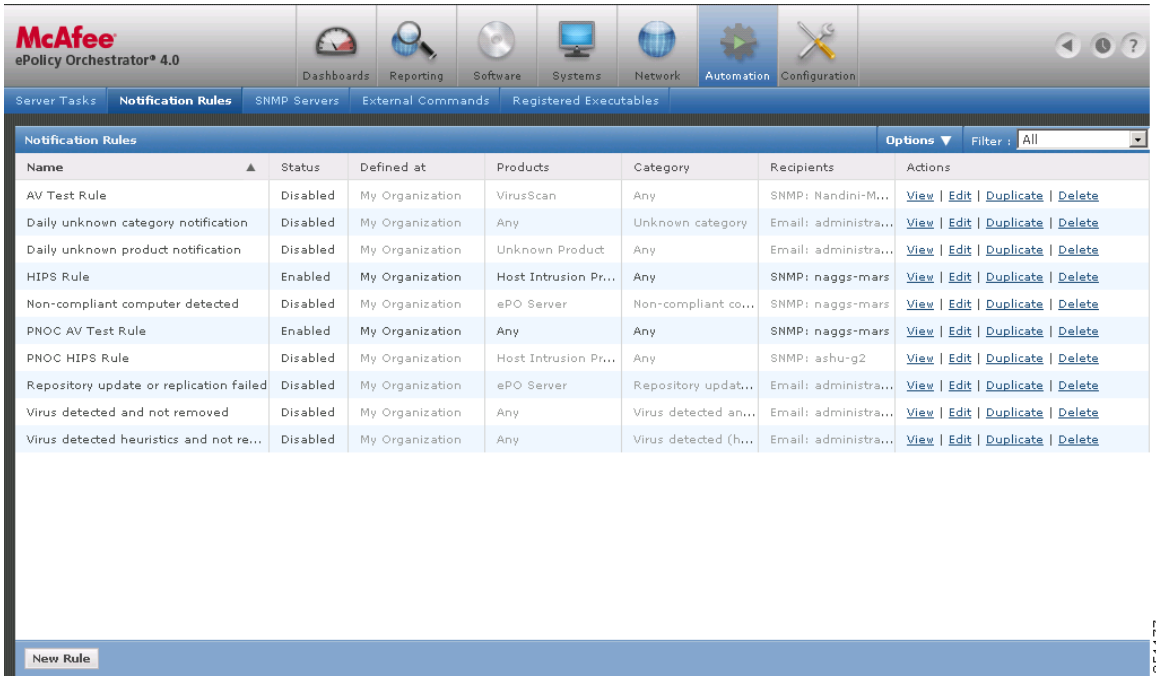
Step 6 Specify the following values, and click **OK**:

- **Name**—Enter the hostname of the Local Controller.
- **Server address**—Enter the IP address of the eth0 interface, the monitoring interface for the MARS Appliance.

The SNMP server is added to represent the MARS Appliance.

Step 7 Click the **Notification Rules** subtab.

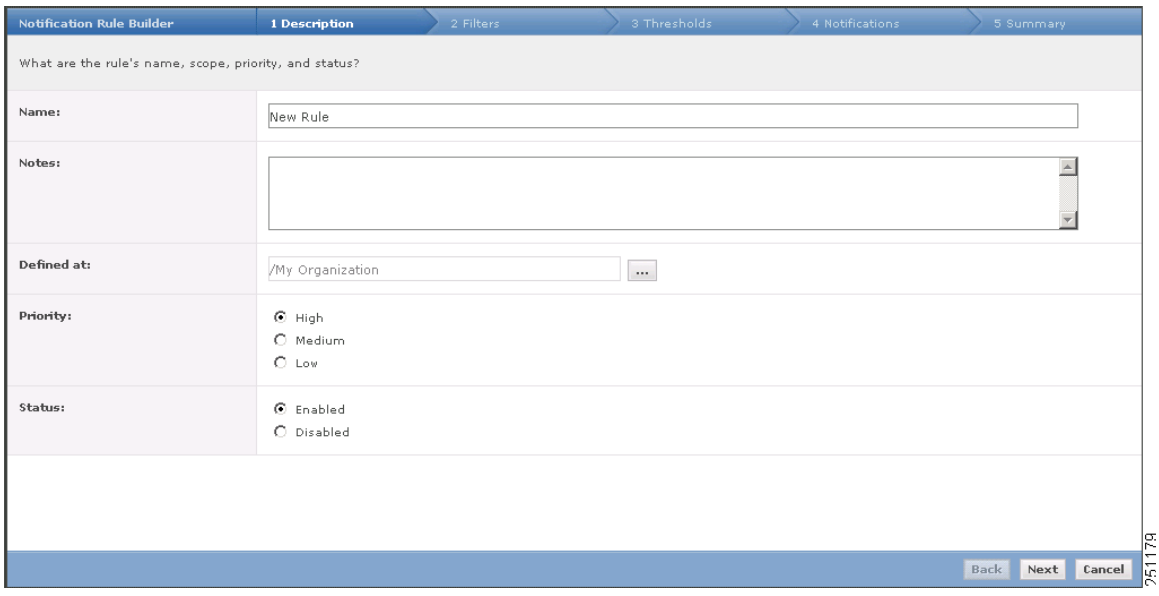
The list of active notification rules appears.



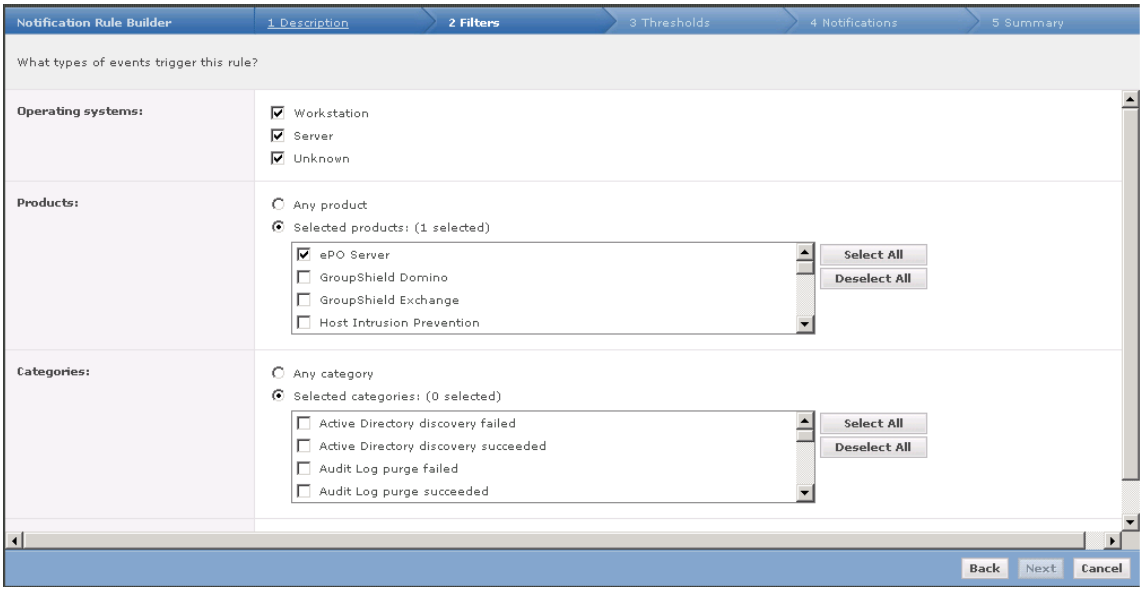
Step 8 Edit each enabled rule in the list so that all notifications are sent to the SNMP server that represents the MARS Appliance. To edit a rule, follow these steps:

a. Click the rule.

The Describe Rule wizard page appears.

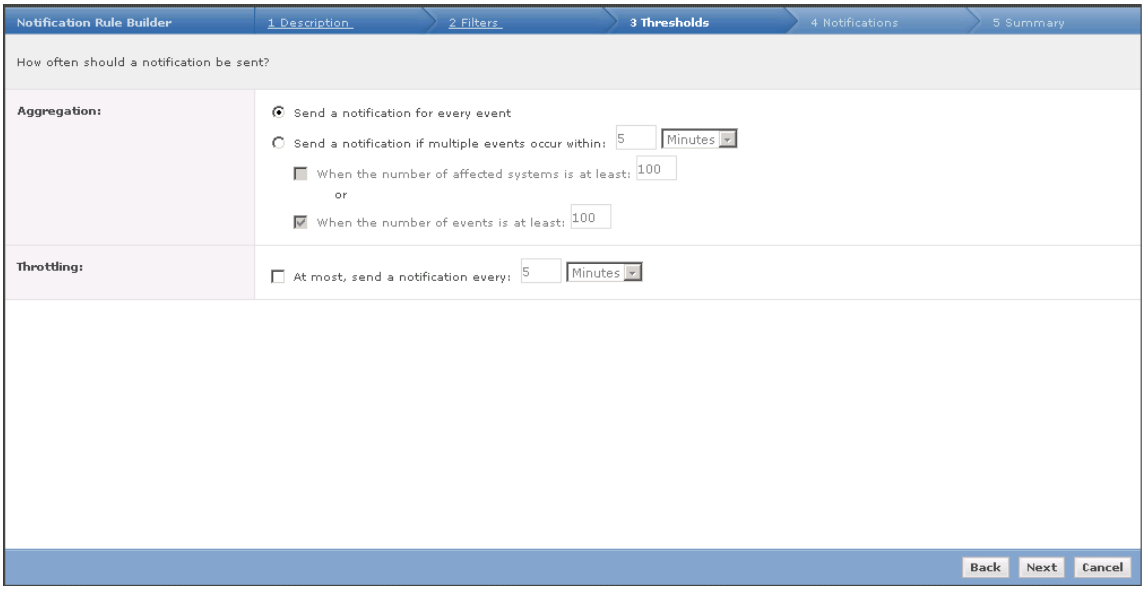


b. Click **Next** to proceed to Set Filters page.



c. Under Add or Edit Notification Rule, click the **3. Set Thresholds** link.

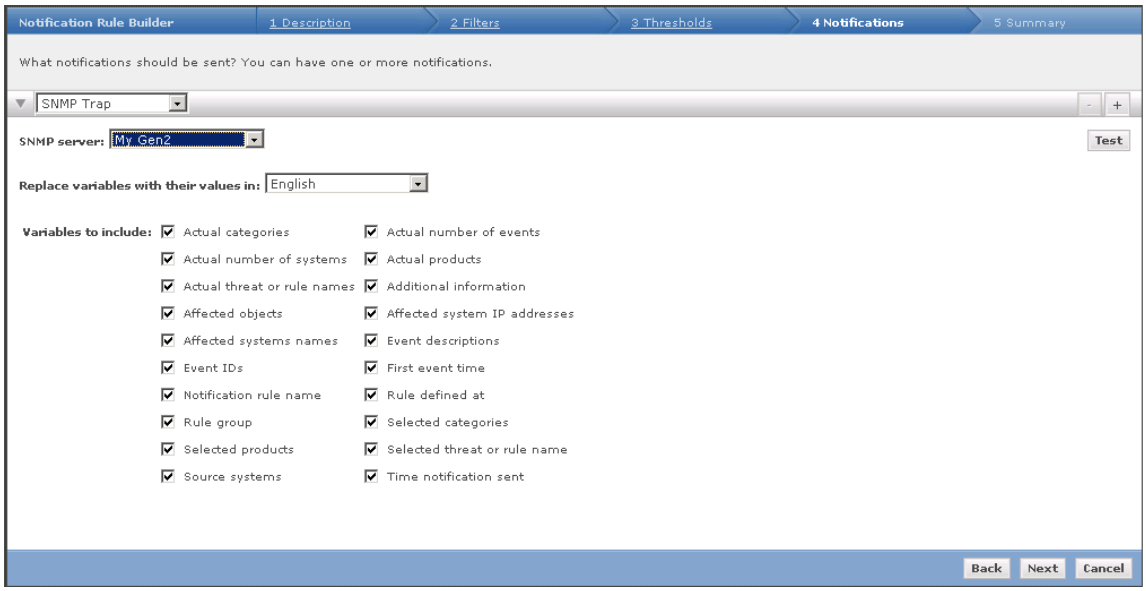
Figure 30-1 Set Threshold Values



d. Verify the Aggregation and Throttling values are set as shown in Figure 30-1Figure 30-3

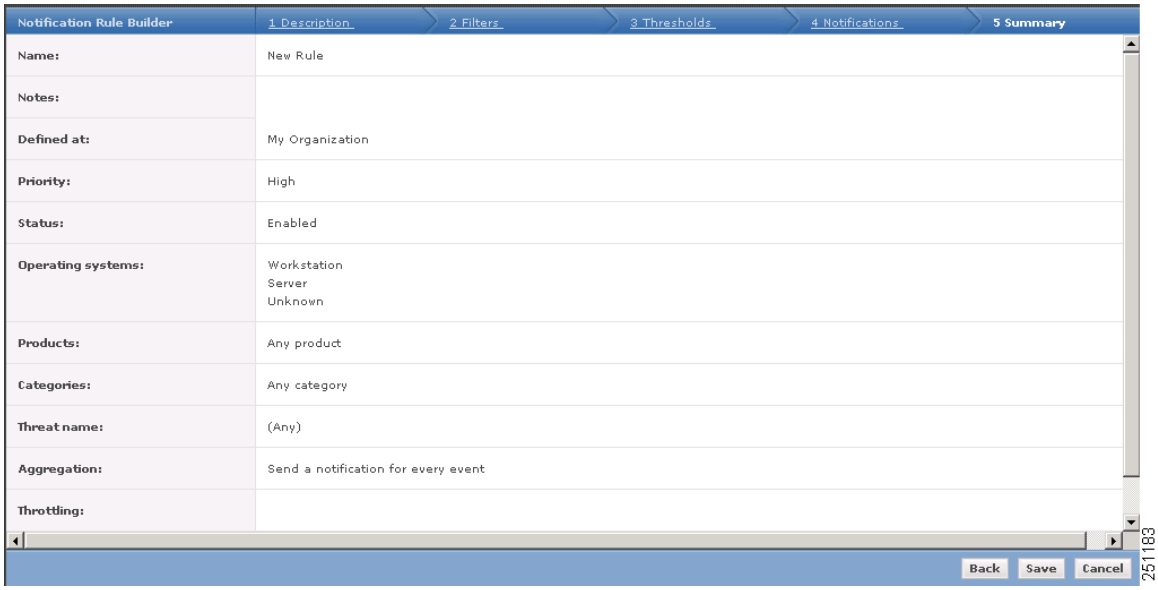
e. Click **Next** to proceed to the Create Notifications page.

Figure 30-2 Notification Rule Builder: Notifications Step



f. In the SNMP server list, select the SNMP server that represents the MARS Appliance.

g. Verify that all the variables are selected as shown in Figure 30-2, and click **Next**.



h. Click **Save** to add the SNMP trap to the list of notifications for the selected rule.

i. Click **Finish** to save the changes to the selected rule.

j. Repeat a. through i. for each rule.

Configure ePolicy Orchestrator 3.5 and 3.6 to Generate Required Data

To prepare the ePolicy Orchestrator server to forward SNMP events to MARS, follow these steps:

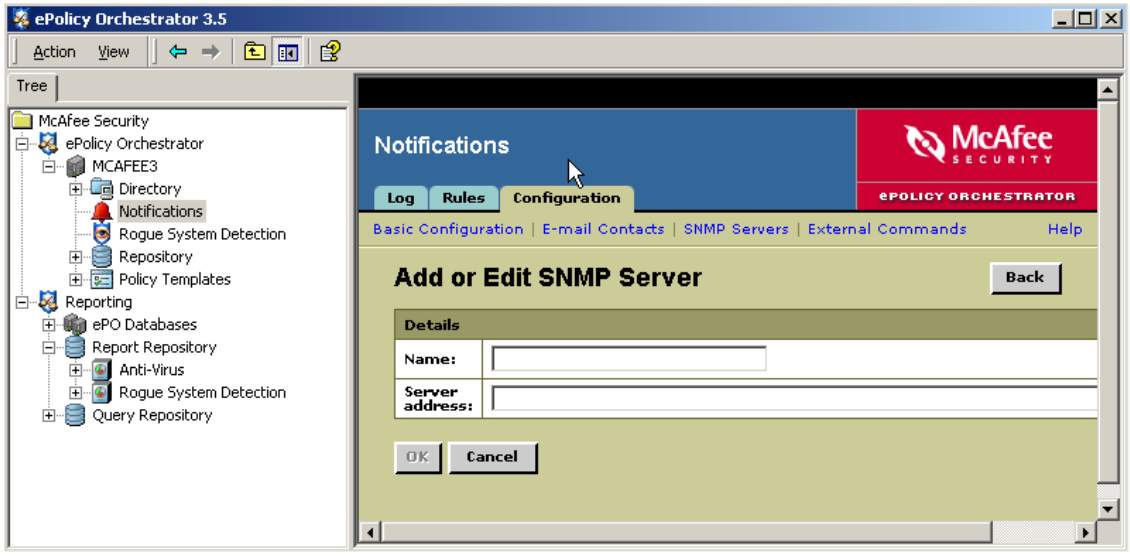
Step 1 Select **Start > Program Files > Network Associates > ePolicy Orchestrator 3.x Console**.

Step 2 In the tree, select **McAfee Security > ePolicy Orchestrator**, and click the **Log on to server** link under Global Task List.

Step 3 In the Log On to Server dialog box, enter the username and password required to access the ePolicy Orchestrator server, and click **OK**.

Step 4 In the tree, select **McAfee Security > ePolicy Orchestrator > <Server_Name> > Notifications** and click the **Configuration** tab and click the **SNMP Servers** link.

Step 5 Click **Add**.



Step 6 In the Name field, enter the hostname of the MARS Appliance.

Step 7 In the Server address field, enter the IP address of the eth0 interface, the monitoring interface for the MARS Appliance, and click **OK**.

The SNMP server is added to represent the MARS Appliance.

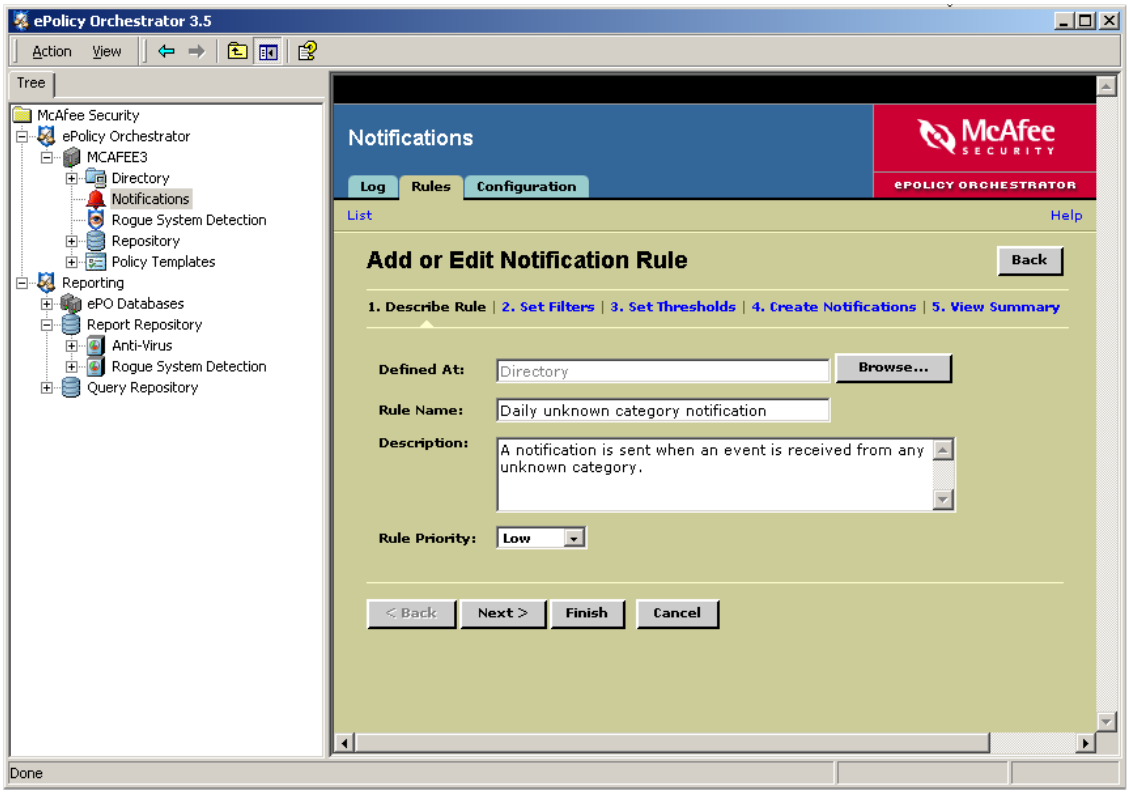
Step 8 Click the **Rules** tab.

You can access the Rules tab by selecting **McAfee Security > ePolicy Orchestrator > <*Server_Name*>** > Notifications > and then clicking the **Rules** tab.

Step 9 Edit each rule in the list so that all notifications are sent to the SNMP server that represents the MARS Appliance. To edit a rule, follow these steps:

a. Click the rule.

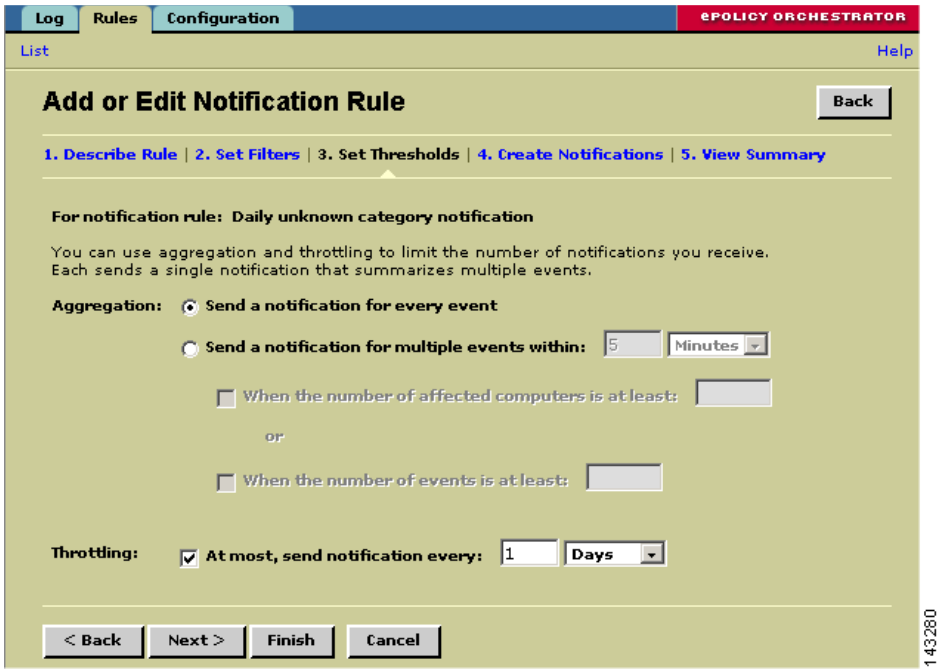
The Describe Rule wizard page appears.



b. Click **Next** to proceed to Set Filters page.

c. Under Add or Edit Notification Rule, click the **3. Set Thresholds** link.

Figure 30-3 Set Threshold Values

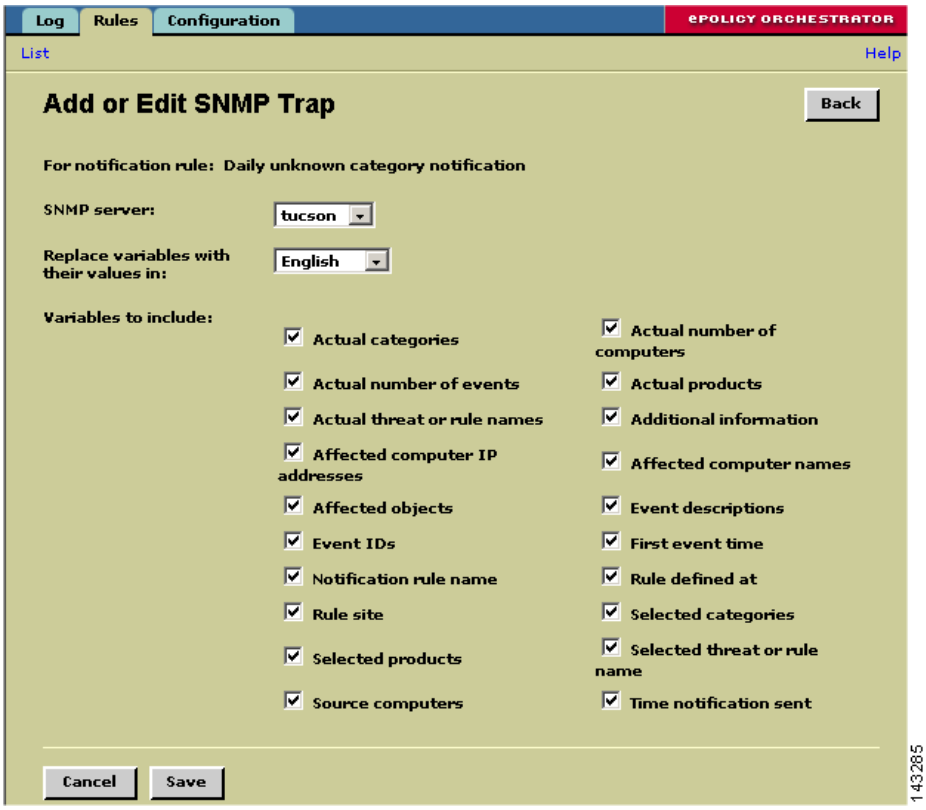


d. Verify the Aggregation and Throttling values are set as shown in Figure 30-1Figure 30-3

e. Click **Next** to proceed to the Create Notifications page.

f. Click **Add SNMP Trap**.

Figure 30-4 SNMP Trap Settings



g. In the SNMP server list, select the SNMP server that represents the MARS Appliance.

h. Verify that all the variables are selected as shown in Figure 30-4.

i. Click **Save** to add the SNMP trap to the list of notifications for the selected rule.

j. Click **Finish** to save the changes to the selected rule.

k. Repeat a. through j. for each rule.

Add and Configure ePolicy Orchestrator Server in MARS

Before MARS can begin processing SNMP traps from ePolicy Orchestrator, you must define the ePolicy Orchestrator server as software running on a host. When ePolicy Orchestrator is defined as a reporting device, MARS can process any inspection rules that you have defined using ePolicy Orchestrator event types.

After you add the ePolicy Orchestrator server to MARS, the appliance can discover the agents that are managed by the ePolicy Orchestrator server as events are generated by those agents. You do not need to manually define the agents associated with this server.

To add an ePolicy Orchestrator server to MARS, follow these steps:

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

Step 3 In the Device Name field, enter the hostname of the server.

Step 4 In the Reporting IP field, enter the IP address of the interface in the ePolicy Orchestrator server from which SNMP traps will originate.

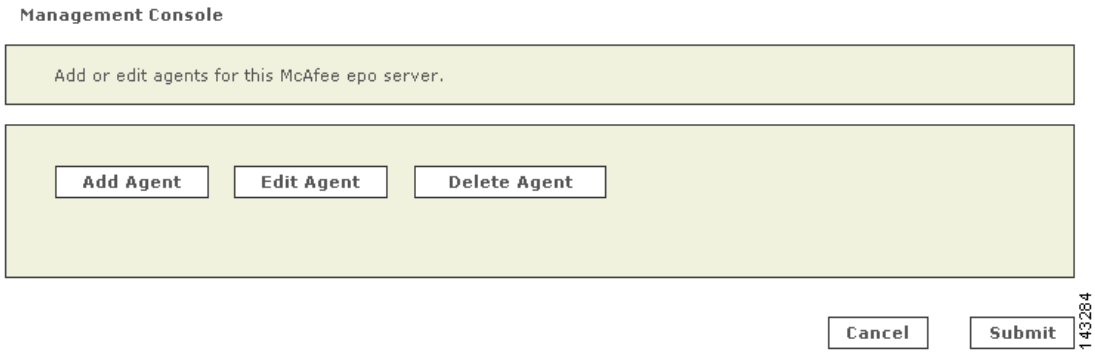
Step 5 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in the ePolicy Orchestrator server from which syslog messages will originate.

This address is the same value as the Reporting IP address.

Step 6 Click **Apply**.

Step 7 Click **Next** to move to the Reporting Applications tab.

Step 8 In the Select Application field, select **McAfee ePO 3.5**, **McAfee ePO 3.6.x**, or **McAfee ePO 4.0**, and then click **Add**



Step 9 Click **Done** to save the changes.

Step 10 Click **Submit**.

Step 11 To activate the device, click **Activate**.

Dynamic discovery of agents is supported. MARS discovers the agents by identifying the originating device in the SNMP traps. Therefore, the agents are discovered as SNMP traps originating from those devices are forwarded by the ePO server.

You are not limited to dynamic discovery for populating agents. For details on manually importing agents into MARS, see Add ePO Agents From File, page 30-11.

Add ePO Agents From File

You can add the complete list of hosts on which ePO Agents are installed by exporting the all hosts report from ePolicy Orchestrator server and importing that file into MARS. The only advantage to adding agents using an export file is that the first notification received that originates from the agent is not attributed to the ePO server.

Note For 3.6.x and 4.0 releases, you can import reporting agents using a CSV file exported from ePO. In 4.0, you can export from the ePO user interface. In 3.6.x, you can export from the database. Refer to the documentation that came with your product for instructions on exporting a CSV file from ePO.

Caution Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

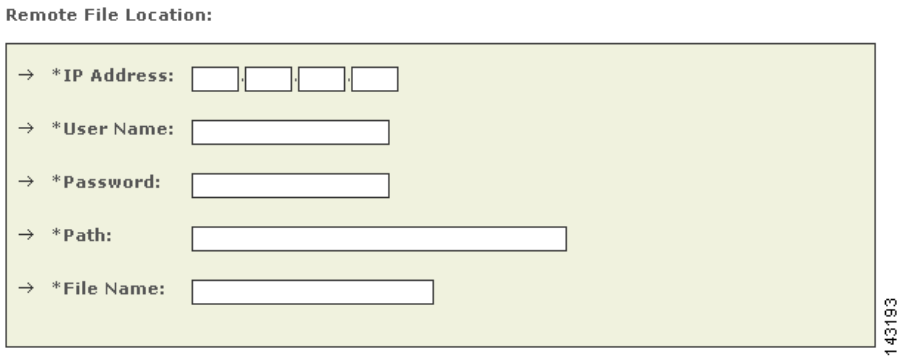
To add ePO agents from a file, follow these steps:

Step 1 Click **Admin > Security and Monitoring Devices**.

Step 2 From the list of devices, select the host running ePolicy Orchestrator server, and click **Edit**.

Step 3 Click the **Reporting Applications** tab, select **McAfee ePO 3.6.x** or **McAfee ePO 4.0** in the Device Type list, and click **Edit**.

Step 4 Click **Load From File**.



Caution The file should be formatted as a tab delimited file. You cannot use a CSV file. To generate a tab delimited file of the ePO agents managed by the ePolicy Orchestrator server, see the documentation that came with your ePolicy Orchestrator product.

Step 5 In the IP Address field, enter the address of the FTP server where you stored the exported hosts file.

Step 6 In the User Name field, enter the name of the account used to authenticate to the FTP server.

Step 7 In the Password field, enter the password that corresponds to the account specified in Step 6.

Step 8 In the Path field, enter the path to the folder where the file is stored. If this file is stored in the root folder, you must specify a backslash (\) in this field. The format of this value is **\<*path_here*>** .

Step 9 In the File Name field, enter the name of the tab delimited file.

Step 10 Click **Submit**.

The following message displays and the hosts are added as agents of the ePolicy Orchestrator server:

```
Success:
Status: OK
```

Step 11 Click **Done**.

CHAPTER 31

Cisco Incident Control Server

The Cisco Incident Control Server (Cisco ICS) enables extended protection across Cisco IOS routers, switches, and IPS devices. In coordination with Trend Micro's incident control solutions, Cisco ICS prevents the spread of day-zero outbreaks in three ways:

- First, Cisco ICS issues temporary ACLs to those Cisco mitigation devices that can block such traffic, typically using a protocol and port pair block. This temporary block is referred to as an Outbreak Prevention ACL (OPACL).
- Second, as soon as a signature is available, Cisco ICS updates all Cisco IPS and IDS devices running on your network with the signature required to detect and prevent the specific threat. This signature is referred to as an Outbreak Prevention Signature (OPSig).
- Third, Cisco ICS can manage supporting products (sold seperately), such as Tend Micros's Damage Cleanup Services (DCS), which cleans infected hosts by removing trojans and other malware.

To complete the Cisco ICS communication settings, you must perform two tasks: configure Cisco ICS to send syslog messages to the MARS Appliance, and add the Cisco ICS management server to the MARS web interface as a reporting device.

This chapter contains the following topics:

- Configure Cisco ICS to Send Syslogs to MARS, page 31-1
- Add the Cisco ICS Device to MARS, page 31-2
- Define Rules and Reports for Cisco ICS Events, page 31-3

Configure Cisco ICS to Send Syslogs to MARS

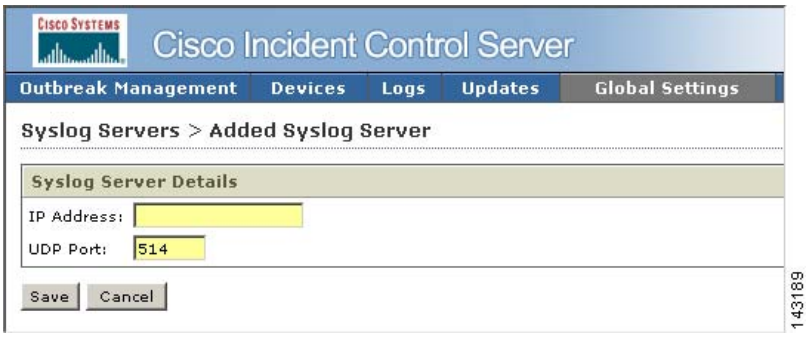
Cisco ICS publishes syslog messages to MARS. To configure Cisco ICS, you simply define a syslog server with the IP address of the MARS Appliance. You do not need to enable any special logs, and you cannot tune the messages that are sent to MARS. The Cisco ICS events for which syslog messages are geneerated have been selected to provide the most benefit to your Security Threat Mitigation (STM) system.

To prepare Cisco ICS to publish events to MARS, follow these steps:

Step 1 Log in to the Cisco ICS Management Console.

Step 2 Click **Global Settings > Syslog Servers**.

Step 3 Click **Add**.



Step 4 In the IP Address field, enter the address of the MARS Appliance to which the Cisco ICS will publish syslog messages.

Step 5 Click **Save**.

Cisco ICS now publishes syslog message to MARS. For MARS to be aware of this device, you must add the Cisco ICS device as a software application running on a host and you must click Activate in the web interface.

Add the Cisco ICS Device to MARS

Before MARS can being processing the syslog messages as Cisco ICS messages, you must define the Cisco ICS management server as an software application running on a host. After Cisco ICS is defined as a reporting device, MARS can process any inspection rules that you have defined using Cisco ICS event types.

To add a Cisco ICS server to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

You can also select **Add SW Security apps on an existing host** if you have already defined the host within MARS, perhaps as part of the Management > IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

Step 3 In the Device Name field, enter the hostname of the server.

Step 4 In the Reporting IP field, enter the IP address of the interface in Cisco ICS server from which the syslog messages will originate.

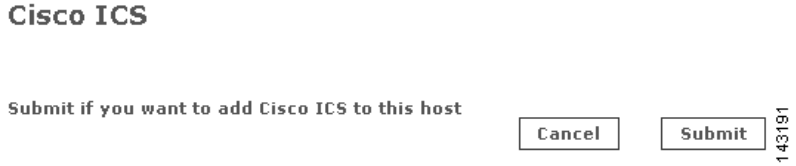
Step 5 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in Cisco ICS server from which the syslog messages will originate.

This address is the same value as the Reporting IP address.

Step 6 Cclick **Apply**.

Step 7 Click **Next** to move the Reporting Applications tab.

Step 8 In the Select Application field, select **Cisco ICS 1.x** , then click **Add**.



Step 9 Click **Select** to add the Cisco ICS application to this host.

Step 10 Click **Done** to save the changes.

Step 11 To activate the device, click **Activate**.

Define Rules and Reports for Cisco ICS Events

From Cisco ICS, MARS receives syslog messages that allow it to identify outbreaks, successful OPACL and OPSig deployments, and failed attempts to deploy. MARS stays abreast of when the OPACLs and OPSigs fire on Cisco IPS devices. MARS also monitors the Cisco ICS server for system issues, such as database failures.

These events assist MARS in providing an accurate, holistic assessment of your network. OPACL and OPSig matching events provide five-tuple correlation, which MARS uses to perform attack path analysis and verify the containment of threats. You can uses the events to define inspection rules that help you perform manual mitigation on devices that cannot use OPACLs and OPSigs.

For example, an inspection rule could be written to match the OPACL event. Your mitigation team can respond by investigating the OPACL that was pushed to the reporting device, from which they can determine the five tuple (source address and port, destination address and port and network service). Using that information, they could push equivalent ACLs to devices not managed by Cisco ICS.

When defining inspection rules or reports, you can access the list of Cisco ICS-specific events by entering *Cisco ICS* in theDescription / CVE: field and clicking Search on the Management > Event Management page of the web interface.

There are four predefined system inspection rules for Cisco ICS:

- New Malware Discovered
- New Malware Prevention Deployed
- New Malware Prevention Deployment Failed
- New Malware Traffic Match

In addition, there are five predefined reports:

- Activity: New Malware Discovered - All Events
- Activity: New Malware Prevention Deployment Failure - All Events
- Activity: New Malware Prevention Deployment Success - All Events
- Activity: New Malware Traffic Match - All Events
- Activity: New Malware Traffic Match - Top Sources

PART 13

Content Management

CHAPTER 32

Cisco CSC SSM

The Cisco CSC SSM (Content Security and Control Security Services Module) integrates with Trend Micro InterScan to provide an all-in-one antivirus and spyware management solution for a network. It provides the following protections:

- Detects and takes action against viruses, worms, Trojans, and other threats in network traffic using the SMTP, POP3, HTTP, and FTP protocols
- Blocks compressed or very large files that exceed specified parameters
- Scans for and removes spyware, adware, and other types of grayware

CSC-SSM is a module that resides in a Cisco ASA appliance. Based on user-defined policies, the ASA forwards the specified traffic to the CSC SSM for inspection. The CSC SSM performs actions according to its policies and generates syslog messages about those actions. Cisco Secure MARS parses those messages, which can alert the system to potential and active network threats.

Note MARS neither parses the configuration settings for the CSC SSM nor monitors the module for performance anomalies. Any anomalies in operation will be reported by the host ASA appliance. Also, while the host ASA appliance does appear in the topology path analysis diagram, the CSC SSM module does not.

This chapter contains the following topics:

- Defining a CSC SSM in MARS, page 32-1

Defining a CSC SSM in MARS

You can define a CSC SSM module in MARS by adding it manually. Because MARS does not parse (or discover) the configuration settings for the CSC SSM, you do not need to bootstrap the module to allow MARS administrative access to the module. However, you do need to define MARS as a syslog target of the module.

1. Bootstrap the CSC SSM module to send syslog message to the MARS appliances.

   See "Configuring System Log Message Settings" to define the MARS appliances as a target syslog server on the CSC SSM.

2. Define the CSC SSM module under an existing ASA appliance.

   See Define a CSC SSM in MARS Manually, page 32-2.

Related Documents

Related Topics	Document Title
See "Configuring System Log Message Settings" to specify the MARS appliances as a target syslog server.	*Cisco Content Security and Control SSM Administrator Guide*

Define a CSC SSM in MARS Manually

To manually define a CSC SSM, you must have previously define the host ASA appliance in which the module is installed and configured. When the module is defined and the changes are activated, MARS normalizes the syslog message receive by the module against known event types.

To define a CSC SSM module on an ASA appliances in MARS, follow these steps:

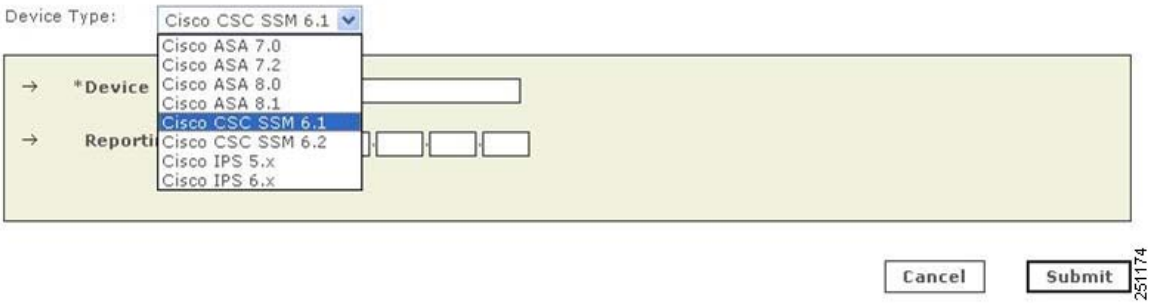
Step 1 From the list of devices, select the ASA appliances under which you want to define the CSC SSM module, and click **Edit**.

Tip You can filter the list of devices selectable devices by typing the device name in the Search field and clicking **Search**.

The ASA appliance settings page appears.

Step 2 Click **Add Module** at the bottom of the page.

The Device Type page appears.



Step 3 Select **Cisco CSC SSM 6.1** or **Cisco CSC SSM 6.2** for the Device Type list.

Step 4 Type the name of this module in the **Device Name** field.

Step 5 Type the IP address of the CSC-SSM module in the **Reporting IP** field.

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

The module name appears under the Module Names list. 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 7 To enable MARS to start sessionizing events from this module, click **Activate**.

MARS begins to sessionize events generated by this module 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. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

PART 14

Database Applications

CHAPTER 33

Oracle Database Server Generic

Database applications are typically high-value assets, and as such, they are common targets for attacks. Database applications provide MARS with user activity, such as successful and failed login attempts, session durations, and activities indicative of privilege escalation. This chapter explains how to bootstrap and add database applications to MARS.

To configure CS-MARS to collect information from the Oracle database server, you must perform three tasks:

- configure the Oracle database server to generate a audit trail and record those events the database.
- represent the device in the web interface
- configure the interval at which MARS should pull the logs from the Oracle database server.

Configuring the pull interval is a one-time operation that applies to all of the Oracle database servers monitored by the MARS Appliance.

This chapter contains the following topics:

- Configure the Oracle Database Server to Generate Audit Logs, page 33-1
- Add the Oracle Database Server to MARS, page 33-2
- Configure Interval for Pulling Oracle Event Logs, page 33-3

Configure the Oracle Database Server to Generate Audit Logs

You must configure the Oracle database server to write audit logs to the database. You may need your DBA support to perform most of these configurations. Once configured, MARS can retrieve the audit logs from your Oracle database server. The following examples are for an Oracle instance running on a UNIX/Linux application host.

To configure an Oracle database server to write audit logs, follow these steps:

Step 1 As sysdba execute cataudit.sql to create audit trail views:

```
[oracle@server]$ sqlplus /nolog

SQL> conn / as sysdba;
SQL> @$ORACLE_HOME/rdbms/admin/cataudit.sql
```

Step 2 Enable auditing to the database by adding the following entry to the Oracle instance initialization file, usually named init<SID>.ora

```
AUDIT_TRAIL=DB
```

This file is usually located in `$ORACLE_BASE/admin/<SID>/pfile`, where ***<SID>*** is the name of the Oracle instance.

If a binary initialization file is used for this instance, make sure you update it first. This file is usually located in `$ORACLE_HOME/dbs and named spfile<SID>.ora`. Ask your DBA about the location of these files as well as the policies applied for this server.

Step 3 Restart the database to activate the change made to the initialization file.

```
[oracle@server]$ sqlplus /nolog

SQL> conn / as sysdba;
SQL> shutdown immediate;
SQL> startup;
```

Step 4 Turn on all the logs that you want to audit. The following example is turning on the "audit session".

```
SQL> audit session;
Audit succeeded.
```

Note Support for new AUDIT_ACTIONS found in Oracle 11g is supported as of Cisco Secure MARS releases 4.3.3/5.3.3.

Step 5 Repeat the previous step for all the logs that you want to audit.

Step 6 Create a user account on this server and grant select privilege for the view dba_audit_trail. Our example assumes the user has login name "pnuser".

```
SQL> grant select on dba_audit_trail to pnuser
```

You'll use "pnuser" as the value for "User Name" in the MARS setup.

Step 7 To test that everything was properly configured, audit logs are written to the database and "pnuser" has read access to them, execute the following commands:

```
[oracle@server]$ sqlplus pnuser/<password>@<oracle_server>

SQL> select count(*) from dba_audit_trail;

  COUNT(*)
----------
         3
```

If the above count is anything but zero, congratulations, you have successfully configured the Oracle Server! You will have to repeat the above procedure for every Oracle server that you want to report audit logs to MARS.

Add the Oracle Database Server to MARS

To represent the Oracle database server in the web interface, follow these steps:

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

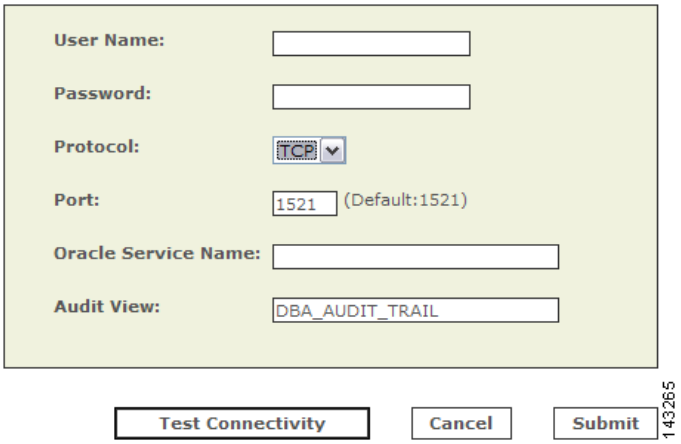
Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 From the Select Application list, select **Oracle Database Server Generic**.

Step 6 Click **Add**.



Step 7 Enter values for the following fields:

- **User Name**—The Oracle Database User Name.
- **Password**—The Oracle Database User password.
- **Oracle Service Name**—The Oracle Service Name.

  The Oracle Service Name is the GLOBAL_DBNAME=username.server found inside the file named `listener.ora`.

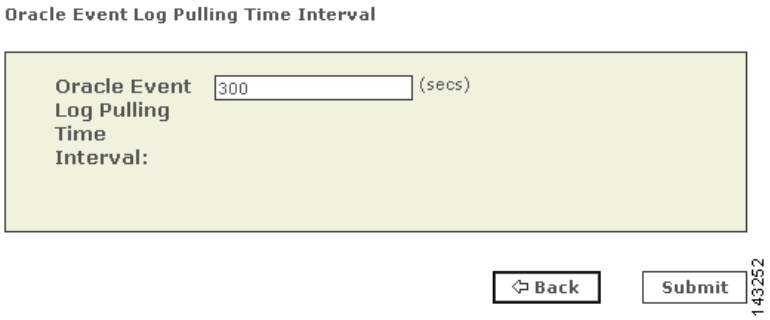
Step 8 Click **Test Connectivity** to verify the configuration.

Step 9 Click **Submit** .

Configure Interval for Pulling Oracle Event Logs

To specify the interval at which MARS should pull the event logs from all Oracle database servers on your network, follow these steps:

Step 1 Click **Admin > System Parameters > Oracle Event Log Pulling Time Interval**.



Step 2 Enter the new time interval in seconds.

The default value is 300 (five minutes).

Step 3 Click **Submit**.

PART 15

Web Servers

CHAPTER 34

Configuring Web Server Devices

To use web logging with MARS, you need to configure the host, the webserver, and MARS. MARS can process up to 100 MB of web log data per receive from your host. This chapter explains how to bootstrap and add web sever devices to MARS

Note Web logging is only supported on hosts running Microsoft IIS on Windows, Apache on Solaris or Linux, or iPlanet on Solaris.

This chapter contains the following topics:

- Microsoft Internet Information Sever, page 34-1
- Apache Web Server on Solaris or RedHat Linux, page 34-7
- Sun Java System Web Server on Solaris, page 34-7
- Generic Web Server Generic, page 34-7

Microsoft Internet Information Sever

You can add computers running Microsoft Windows to MARS as reporting devices. The Microsoft Windows computer needs to run InterSect Alliance SNARE for IIS, from which MARS receives web log data.

Note Synchronize clocks of the Microsoft Windows system and the MARS to ensure times match between them.

This section contains the following topics:

- Install and Configure the Snare Agent for IIS, page 34-1
- MARS-side Configuration, page 34-5

Install and Configure the Snare Agent for IIS

To configure IIS to publish logs to MARS, you must install and configure a log agent. This agent is free from the InterSect Alliance. You can download the Snare Agent for IIS Servers from the following URL:

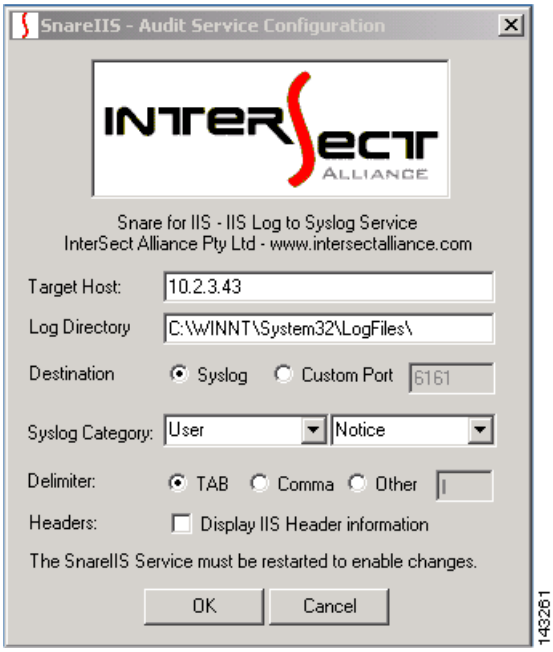
http://www.intersectalliance.com/projects/SnareIIS/index.html#Download

After you have downloaded and install the SNARE on the the Windows webserver, you can continue with the procedures in this section that detail the correct configuration for MARS,

To configure SNARE for web logging, follow thees steps:

Step 1 Click **Start > Programs > InterSect Alliance > Audit Configuration**.

Figure 34-1 Configure SNARE for Web Logging



Step 2 In Target Host enter the IP address of the MARS.

Step 3 In Log Directory, enter the directory where the logs are to be placed.

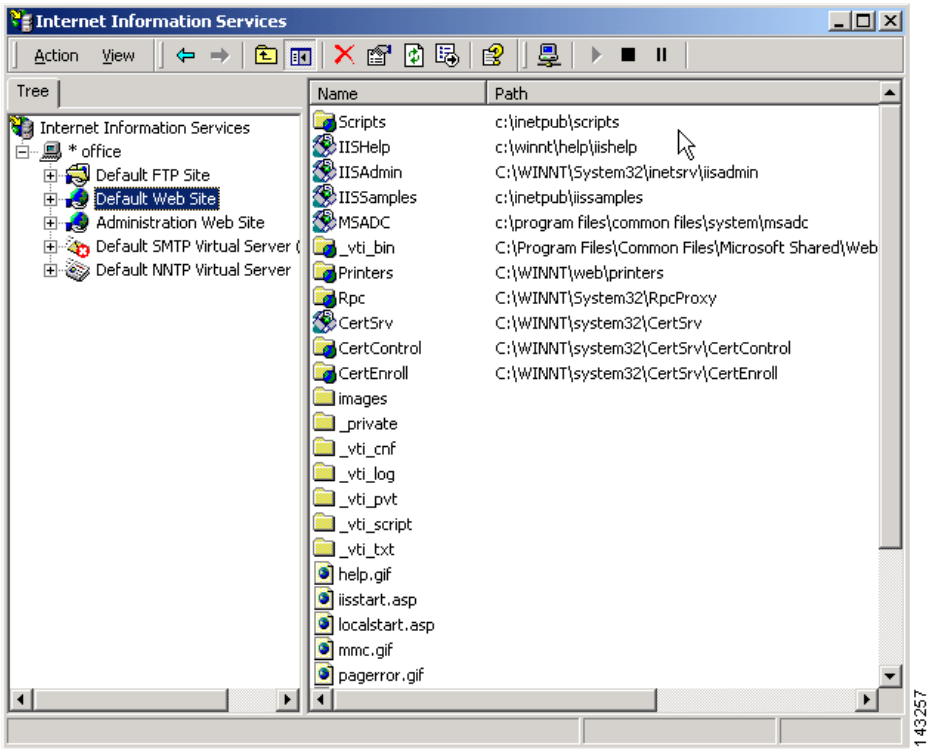
Step 4 In Destination, click the **Syslog** radio button.

Step 5 Click **OK**.

To configure IIS for web logging

Step 1 Click **Start > Programs > Administrative Tools > Internet Services Manager**.

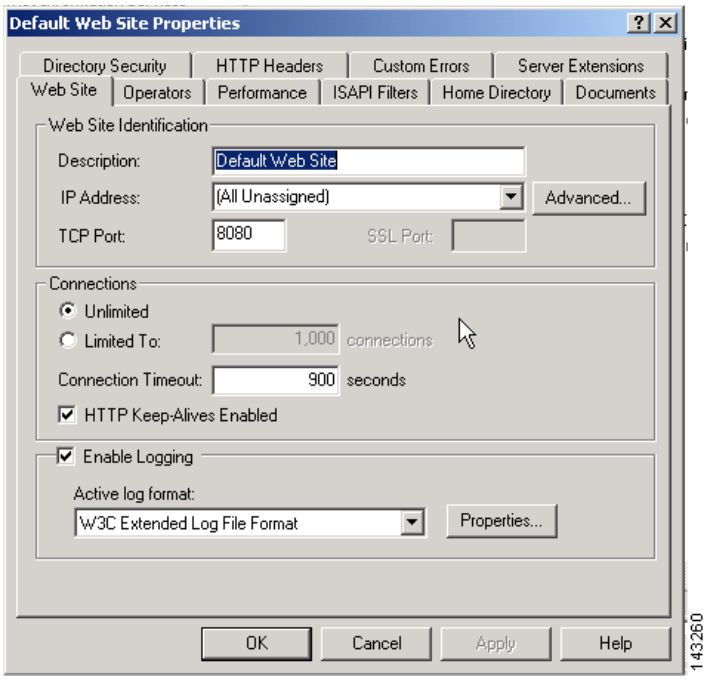
Figure 34-2 Configure IIS for Web Logging



Step 2 In the Tree tab on the left, right-click **Default Web Site**.

Step 3 On the shortcut menu, select **Properties**.

Figure 34-3 Enable Logging



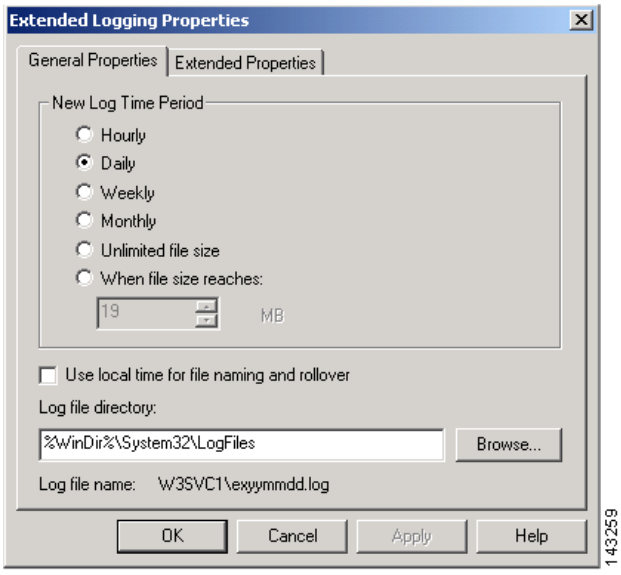
Step 4 In the Web Site tab:

a. Make sure **Enable Logging** is checked.

b. From the Active log format list, select **W3C Extended Log Format**.

c. Click **Properties**.

Figure 34-4 Select General Log Settings

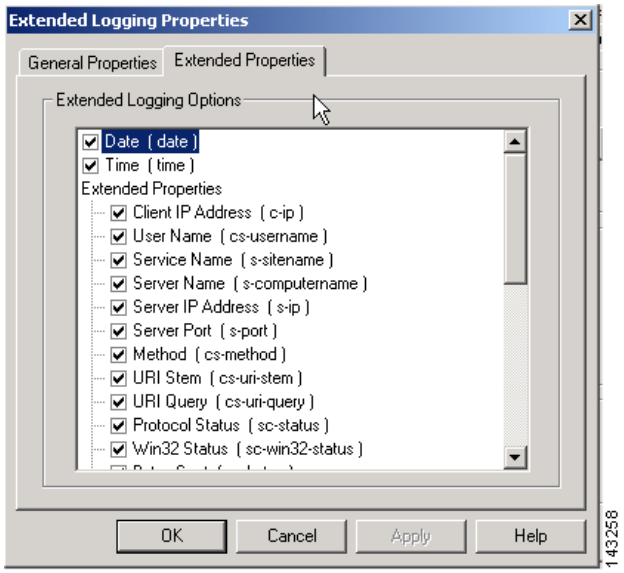


d. In the General Properties tab, set the **New Log Time Period** to **Daily**.

Note The ***Log file directory****must* match the one previously set using the Audit Configuration program.

e. In the Extended Properties tab, make sure all available properties are selected.

Figure 34-5 Select Extended Log Events



f. Click **OK**.

Step 5 Click **OK**.

MARS-side Configuration

To add configuration information for the host

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

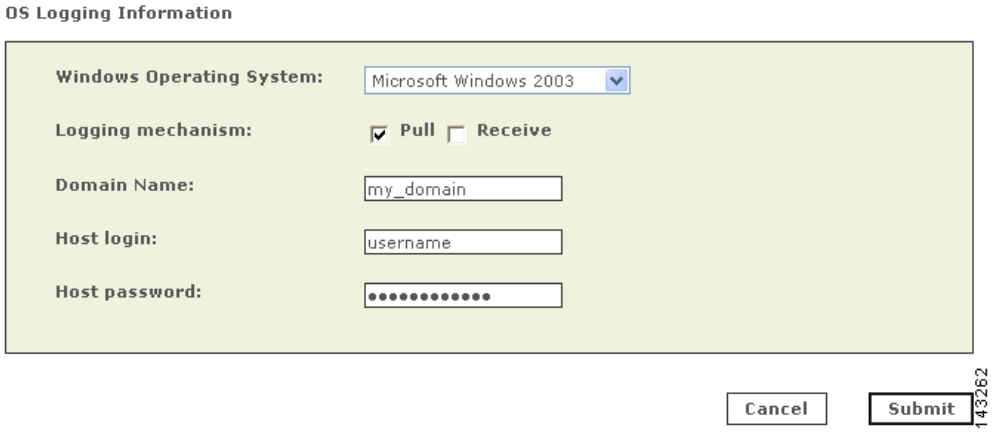
Step 3 Enter the **Device Name** and **IP Addresses** if adding a new host.

Step 4 Select the **Windows** from Operation System list

Step 5 Click **Logging Info**.

Step 6 For this configuration, you must check the **Receive host log** box.

Figure 34-6 Windows Web Server Logging mechanisms



Step 7 Click **Submit**.

Step 8 Continue adding the interfaces.

- For the first interface, enter its name, IP address, and mask.
- For multiple interfaces, click **Add Interface**, and add each new interface's name, IP address, and mask.

Step 9 Add as many IP addresses and masks to the interface as you need by clicking **Add IP/Network Mask**.

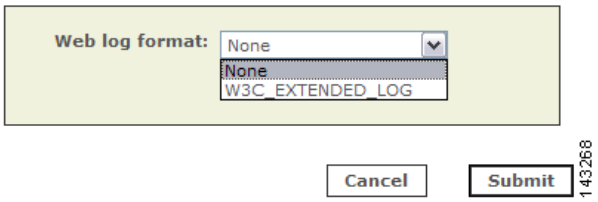
Step 10 Click **Apply**.

Step 11 Click **Reporting Applications** tab.

Step 12 From the Select Application list, select **Generic Web Server Generic**.

Step 13 Click **Add**.

Figure 34-7 Selecting the Windows Web Log format



Step 14 Select **W3C_EXTENDED_LOG** format

Step 15 Click **Submit**.

Note Once you have configured and activated both sides, it takes two pulling intervals (default time of 10 minutes) before new events appear.

Apache Web Server on Solaris or RedHat Linux

Sun Java System Web Server on Solaris

Note The Sun Java System Web Sever was formerly known by the following product names: Netscape Enterprise Server, iPlanet Web Server, and Sun ONE Web Server,

Generic Web Server Generic

You can add computers running Solaris or Linux to MARS as reporting devices. The computer needs to run an opensource agent that sends web log data to MARS.

Solaris or Linux-side Configuration

Cisco provides an opensource logging agent and an associated configuration file for you to use. This agent can be downloaded from the software download center at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

Note Synchronize clocks of the UNIX or Linux system and the MARS to ensure times match between them.

Install and Configure the Web Agent on UNIX or Linux

For MARS to recieve logs from a webserver, you must install the Web agent, (agent.pl version 1.1) on the target webserv and direct the agent to publish logs to the MARS Appliance.

Note Before you install the agent, you must have **perl** and **curl** installed on your system.

To install the agent on a UNIX or Linux hosts, follow these steps:

Step 1 Log into the host as the root user.

Step 2 Create a directory called ***/opt/webagent***.

Step 3 Copy the files ***agent.pl*** and ***webagent.conf*** to the ***/opt/webagent*** directory.

Step 4 Set the protection of the agent script (***agent.pl***) so it can be read and executed by all:

```
cd /opt/webagent
chmod 755 agent.pl
```

Step 5 Edit the configuration file (weblogagent.conf):

```
logfile_location = access_log_path
MARS_ip_port = MARS_ip_address
username = a
```

```
password = b
```

Where the following values are provided:

- *access_log_path* identifies the absolute path name to the web server's access log
- *MARS_ip_address* is the IP address of the MARS Appliance

You do not need to edit the username or password in the file.

Note You need a separate weblogagent.conf file for each access log you want to pull. We recommend naming them weblogagent1.conf, weblogagent2.conf, and so forth. Put these in the /opt/webagent directory also.

To run the agent using a configuration file other than weblogagent.conf, use the command:

```
agent.pl other_config_file
```

replacing *other_config_file* with the name of the web agent configuration file.

Step 6 Edit the crontab file to push the logs to the MARS at regular intervals. The following example gets new entries from the access log and pushes them to MARS every five minutes:

```
crontab -e
5,10,15,20,25,30,35,40,45,50,55,0 * * * *
       (cd /opt/webagent;./agent.pl weblogagent1.conf)
5,10,15,20,25,30,35,40,45,50,55,0 * * * *
       (cd /opt/webagent;./agent.pl weblogagent2.conf)
```

Web Server Configuration

To configure the Apache web server for the agent

Step 1 In the file httpd.conf, make sure the LogFormat is either common or combined and matches the format set on the MARS.

Step 2 Stop and restart the Apache server for your changes to take effect.

To configure the iPlanet web server for the agent

Step 1 In the iPlanet server administration tool, click the **Preferences** tab.

Step 2 In the left menu, click the **Logging Options** link.

Step 3 Make sure the Log File matches the log file name set on the MARS.

Step 4 Make sure the Format radio button **Use Common Logfile Format** is checked.

Step 5 If you have made any changes, click **OK**.

Step 6 If necessary, shut down and restart the iPlanet web server.

MARS-side Configuration

To add configuration information for the host

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

Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

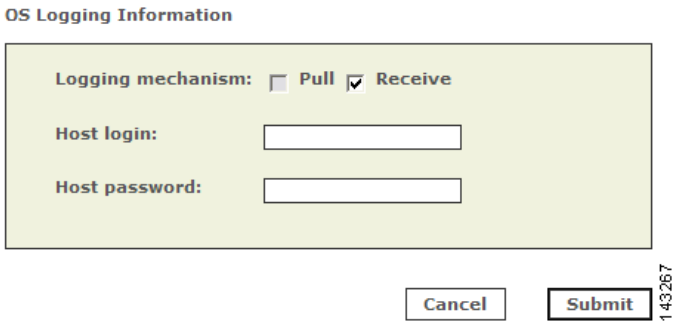
Step 3 Enter the **Device Name** and **IP Addresses** if adding a new host.

Step 4 Select the either **Solaris** or **Linux** from Operation System list.

Step 5 Click **Logging Info**.

Step 6 For this configuration, you must check the **Receive host log** box.

Figure 34-8 Unix or Linux Web Server Logging mechanism



Step 7 Click **Submit**.

Step 8 Continue adding the interfaces.

- For the first interface, enter its name, IP address, and mask.
- For multiple interfaces, click **Add Interface**, and add each new interface's name, IP address, and mask.

Step 9 Add as many IP addresses and masks to the interface as you need by clicking Add IP/Network Mask..

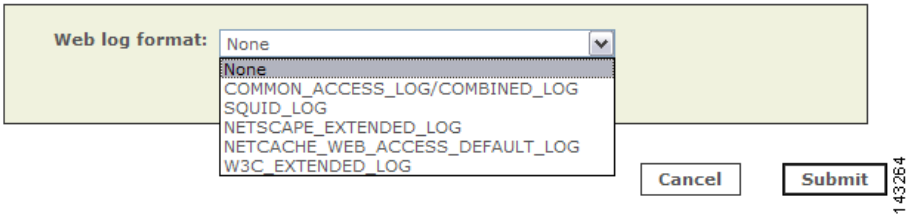
Step 10 Click **Apply**.

Step 11 Click **Reporting Applications** tab.

Step 12 From the Select Application list, select **Generic Web Server Generic**.

Step 13 Click **Add**.

Figure 34-9 Linux Operating System Web Log Format



Step 14 From the Web Log Format list, select appropriately.

Step 15 Click **Submit**.

Note Once you have edited a device you must click **Activate** for the changes to take effect.

PART 16

Web Proxies

CHAPTER 35

Network Appliance NetCache Generic

Web proxy devices provide MARS with additional data surrounding user requests of network services, such as HTTP, FTP, NNTP, and DNS. These device cache data and provide additional services around requests for that data. These additional services provide MARS with data about session requests, including authentication logs, denied session requests based on ACLs enforced by the web proxy device, and traffic logs.

This chapter contains the following topics:

- Configure NetCache to Send Syslog to MARS, page 35-1
- Add and Configure NetCache in MARS, page 35-2

Configure NetCache to Send Syslog to MARS

Synchronize clocks of the NetCache device and the MARS to make sure times match between them.

Note MARS supports only HTTP proxy logs and MMS streaming media proxy logs.

To configure NetCache to send syslog to MARS, follow these steps:

Step 1 In Internet Explorer, enter the URL and log in to the NetCache device.

Step 2 Click the **Setup** tab.

Step 3 In the left side of the window, select **HTTP**, then **Logging**.

Step 4 In the right side of the window, under Web Access Log Enable, select the **Enable the Web Access Log** checkbox.

Step 5 Under Log Format, select one of the first four formats:

- Web Access Log Default Format
- Common Log Format
- Netscape Extended Format
- Squid Type Format

Step 6 Under Web Details Log Enable, verify the box is *not* selected.

Step 7 Click **Commit Changes** to save your changes.

Step 8 In the left side of the window, select **Streaming**, then **Logging**.

Step 9 In the right side of the window, under Streaming Access Log Enable, select the **Enables access logging for streaming protocol clients** check box.

Note You can only enable access logging for streaming protocol clients if you have a streaming cache license.

Step 10 Under Streaming Access Log Format, select either of the options. If you select **Custom**, replace ***"x-client-port"*** with ***"x-username"***.

Step 11 Under Streaming Details Log Enable, verify that the box is *not* selected.

Step 12 Click **Commit Changes** to save your changes.

Step 13 In the left side of the window, select **Streaming**, then **MMS**.

Step 14 Under MMS Enable, verify that the **Enables MMS protocol support** check box is selected.

Step 15 Click **Commit Changes** to save your changes.

Step 16 In the left side of the window, select **System**, then **Logging**.

Step 17 In the right side of the window, under Maximum Log File Size, enter a number less than or equal to 100 (megabytes).

Step 18 Under How to Switch Log Files, select **Push the log file to the following URL**.

Step 19 For the URL, enter:

http://MARS_HOST/upload/UploadWebLogServlet

Replace *MARS_HOST* with the hostname or IP address of the MARS Appliance.

Step 20 Verify that the **User** and **Password** fields are blank.

Step 21 Verify that the **Push the log files in compressed gzip format** check box is *not* selected.

Step 22 Under When to Switch, select the option that prevents the log files from becoming greater than 100 megabytes.

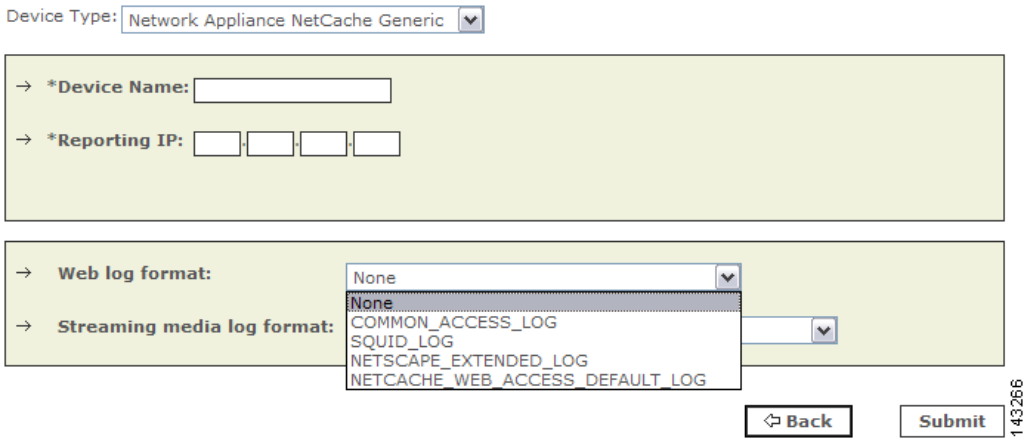
Step 23 Click **Commit Changes** to save your changes.

Add and Configure NetCache in MARS

To add the NetCache device in MARS, follow these steps:

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

Step 2 From the Device Type list, select **Network Appliance NetCache Generic**.



Step 3 Enter the device name and its reporting IP address.

Step 4 From the Web log format list, select the web log format that matches the value you selected in ERROR: BROKEN STEPREF of Configure NetCache to Send Syslog to MARS, page 35-1.

Step 5 From the Streaming media log format list, select a streaming media log format.

Step 6 Click **Submit** .

PART 17

Host Nodes

CHAPTER 36

Configuring Generic, Solaris, Linux, and Windows Application Hosts

Revised: June 19, 2007

Application hosts are simply hosts on your network that are running important applications. Many of the supported reporting devices and mitigation devices cannot be represented in MARS until the base host on which they are running is defined. Examples of such applications include CheckPoint Firewalls and all forms of web servers.

MARS provides for the definition of the following host types:

- **Generic**—Identifies no specific operating system, as well as any that are not directly supported.
- **Windows**—Identifies one of the Microsoft operating systems.
- **Solaris**—Identifies any of the Solaris family of operating systems.
- **Linux**—Identifies any of the Linux family of operating systems.

You should define the application host as exactly as possible. This guideline applies to the vulnerability assessment information and general settings. This detail information helps MARS determine if the host is susceptible to known attacks, such as one that targeta specific operating system or application/service running on the host.

This chapter contains the following topics:

- Adding Generic Devices, page 36-1
- Sun Solaris and Linux Hosts, page 36-2
- Microsoft Windows Hosts, page 36-4
- Define Vulnerability Assessment Information, page 36-12

Adding Generic Devices

The MARS can 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. For more information on free form queries, see To Run a Keyword Query.

Sun Solaris and Linux Hosts

To configure MARS to receive and process Solaris or Linux host log information, you must perform three tasks.

This section contains the following topics:

- Configure the Solaris or Linux Host to Generate Events, page 36-2
- Configure Syslogd to Publish to the MARS Appliance, page 36-2
- Configure MARS to Receive the Solaris or Linux Host Logs, page 36-3

Configure the Solaris or Linux Host to Generate Events

MARS Appliance can receive syslog information from a Linux/Solaris host. To configure the Linux/Solaris applications, you must configure the following applications to write to syslog:

To configure these applications to write to the system log, follow these steps:

Step 1 xferlog (which provides transfer logging information from the FTP server)

```
   For ftpd, add the following to /etc/ftpd/ftpaccess:
log transfers real,guest,anonymous inbound,outbound log syslog+xferlog
```

Step 2 inetd trace messages (which provide the authentication information for services provided using inetd)

```
For inetd, the line in /etc/rc2.d/S72inetsvc that reads:
 /usr/sbin/inetd -s
needs to be changed to:
/usr/sbin/inetd -t -s
```

Other messages will automatically appear in the syslog and do not need to be specifically configured.

Step 3 Once you have enabled the message generation, you must configure the sylogd deamon to publish messages to the MARS Appliance. For more information, see Configure Syslogd to Publish to the MARS Appliance, page 36-2.

Configure Syslogd to Publish to the MARS Appliance

Once you have enabled the correct applications to write to the system log, you must configure the syslog daemon on the Solaris or Linux host to publish syslog messages to the MARS Appliance.

To configure the Solaris or Linux host to publish syslogs to the MARS Appliance, follow these steps:

Step 1 Edit /etc/syslog.conf file and add the line below:

```
*.debug @MARS_hostname
```

where *MARS_hostname* is the hostname or IP address of the MARS Appliance.

Step 2 Run following commands to restart syslogd so that the changes are process:

```
/etc/init.d/syslog stop
/etc/init.d/syslog start
```

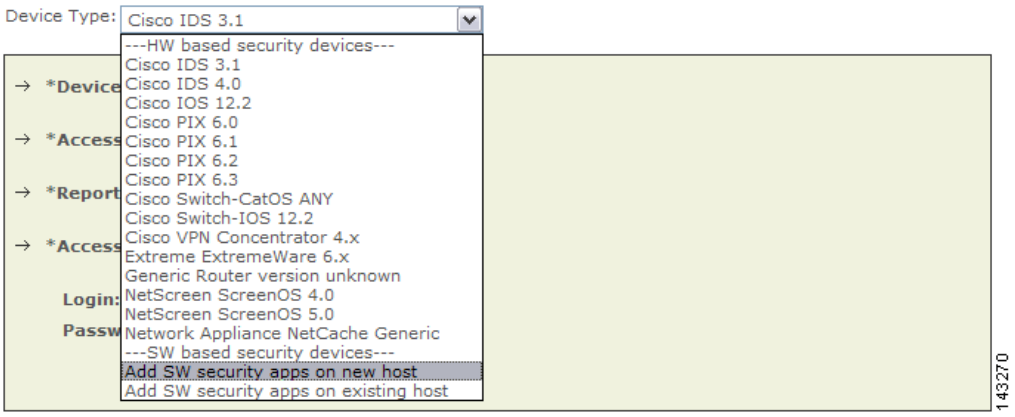
Once this line is added to the syslog.conf file and you have restarted syslogd, any messages sent to console are also sent to the MARS Appliance.

Configure MARS to Receive the Solaris or Linux Host Logs

To add a Solaris or Linux device to MARS, follow these steps:

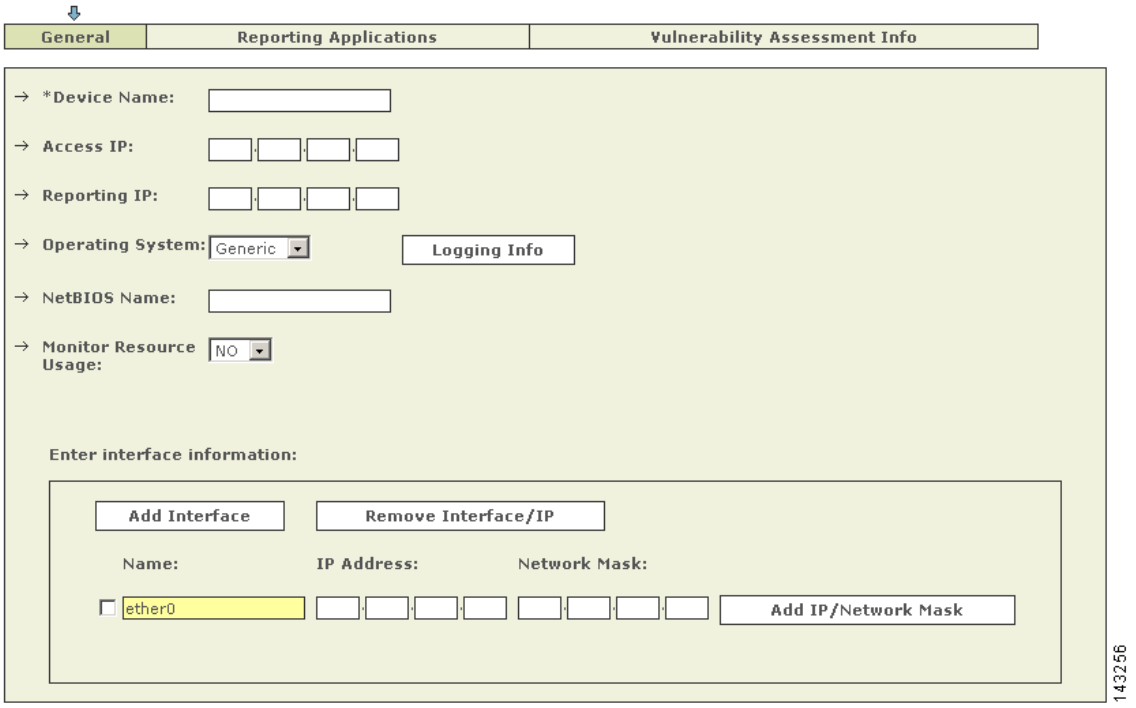
Step 1 Click **Admin > Security and Monitor Devices > Add**.

Figure 36-1 Adding a Solaris or Linux Device



Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

Figure 36-2 Identifying a Solaris or Linux Device From Which to Receive Logs



Step 3 Enter values for the following fields:

- **Device Name**—Enter the hostname for this device.
- **Reporting IP**—Enter the IP address from which the logs will be pulled.

Step 4 In the Operating System list, select either **Solaris** or **Linux** to match the operating system running on the host.

Step 5 Select **Logging Info** and select **Receive** , then click **Submit**.

Step 6 Cclick **Apply** to add the device.

Microsoft Windows Hosts

MARS processes data pulled from hosts running Microsoft Windows. This data includes the events found in the security event log as well application event and system event logs. You can use one of two methods to retrieve the logs from a host running Microsoft Windows, whether it is a server or workstation version:

- You can configure MARS to pull the logs from the host.
- You can configure the host to send the log data to the MARS Appliance.

These two methods are mutually exclusive; in other words, you cannot configure both methods. Your decision in which method to use depends on how much time you can spend preparing the host, the desired load on the MARS Appliance, and how near real-time you want MARS to process the event data.

The *pull method* not only requires system resources for correlating, but also for contacting and pulling the event data from each host. It also operates in a single process, completing the pull from one device before moving to the next. As a result, the pull method may take much longer to cycle through all of the reporting devices as the number of devices grows.

The *push method* is more efficient in terms of resource utilization on the MARS Appliance and in terms of how quickly the MARS Appliance can be made aware of event data, but it requires that you install and configure the Snare Agent for Windows on the Microsoft Windows host. The Snare Agent pushes event data from the servers to MARS in near real time, when an audit event occurs, the agent sends a syslog message to MARS that details the event. It is also more efficient and timely in that each Snare Agent is able to act independently rather than being bound by a single process as with the pull method.

This section contains the following topics:

- Push Method: Configure Generic Microsoft Windows Hosts, page 36-5
- Pull Method: Configure the Microsoft Windows Host, page 36-7
- Configure the MARS to Pull or Receive Windows Host Logs, page 36-9
- Windows Event Log Pulling Time Interval, page 36-11

Push Method: Configure Generic Microsoft Windows Hosts

MARS can treat hosts running Microsoft Windows as reporting devices, monitoring the event log data generated by the host. The host needs to run InterSect Alliance SNARE Agent for Windows, which captures event log data and sends it to MARS. The push method requires four steps:

1. Install the SNARE agent on the Microsoft Windows host. For more information, see Install the SNARE Agent on the Microsoft Windows Host, page 36-5.
2. Configure the SNARE agent to forward event data to the MARS Appliance. For more information, see Enable SNARE on the Microsoft Windows Host, page 36-6
3. Ensure that UDP 514 traffic can pass between the hosts and the MARS Appliance.
4. Identify that host in MARS so that it can correctly parse and correlate the event data. For more information, see Configure the MARS to Pull or Receive Windows Host Logs, page 36-9.

Install the SNARE Agent on the Microsoft Windows Host

To install the SNARE agent, follow these steps:

Step 1 Log in to the target host using a username with proper administrative privileges.

The username must have the permission to publish audit data as well as to install new programs.

Step 2 Download the SNARE Agent for Windows from the following URL that corresponds to the operating system type installed on the target host:

http://www.intersectalliance.com/projects/SnareWindows/index.html#Download

Step 3 Double-click the **SnareSetup<version>.exe** file to start the install program.

Step 4 Click **Next**.

Step 5 Select the target install folder and click **Next**.

Step 6 Select **Normal Installation** in the Components list and click **Next**.

Step 7 Select the target Start menu location and click **Next**.

Step 8 Verify the selection options and click **Install**.

SNARE is installed and started on the local host. A dialog box appears, prompting you to specify whether to allow SNARE to control the EventLog configuration for the Microsoft Windows host.

Step 9 Select **Yes** to enable SNARE to control the EventLog configuration for this Microsoft Windows host.

The SNARE - Remote Event Logging for Windows user interface appears.

Step 10 To configure the Snare agent, continue with Enable SNARE on the Microsoft Windows Host, page 36-6.

Enable SNARE on the Microsoft Windows Host

Once you have downloaded and installed the SNARE agent on the target Microsoft Windows host, you must configure the agent to forward the correct event data in the correct format to the MARS Appliance.

To configure the SNARE agent, follow these steps:

Step 1 Click **All Programs > InterSect Alliance > Snare for Windows** to run the SNARE - Remote Event Logging for Windows user interface.

Step 2 Click **Setup > Network Configuration...**.

The Network Configuration page appears.

Step 3 Specify values for the following fields:

- **Override detected DNS Name with**—Specify the IP address or DNS name of the local host in the field.
- **Destination Snare Server address**—Specify the IP address or the DNS name of the MARS Appliance.

Step 4 Verify that the following options are selected:

- **Allow SNARE to automatically set audit configuration**
- **Allow SNARE to automatically set file audit configuration**
- **Enable SYSLOG Header**

Note Verify the syslog port is 514.

Step 5 Click **Apply the Latest Audit Configuration** on the Network Configuration page.

Step 6 Click **File > Close** to close SNARE - Remote Event Logging for Windows user interface.

The SNARE agent is stopped and restarted to pick up the configuration changes.

Pull Method: Configure the Microsoft Windows Host

As an alternative to the push method, you can configure MARS to pull event log data (security, application, and system event logs) from Microsoft Windows hosts. The pull method requires the following steps:

1. Ensure that the Windows host and MARS Appliance clocks are synchronized. It is recommend that you configure a NTP server for this purpose.
2. Select an existing or define a new user account on the Windows host that the MARS Appliance can use to pull event log records.
3. Ensure that the user account has the correct credentials. Verify that the user account belongs to the Administrator group and verity the it includes the privilege for managing and auditing security logs. For more information, see the procedure that corresponds to the operating system running on the host:
   - Enable Windows Pulling Using a Domain User, page 36-7
   - Enable Windows Pulling from Windows NT, page 36-7
   - Enable Windows Pulling from a Windows 2000 Server, page 36-8
   - Windows Pulling from a Windows Server 2003 or Windows XP Host, page 36-8
   - Enable Windows Pulling Using a Domain User, page 36-7
   - Enable Windows Pulling from Windows NT, page 36-7
   - Enable Windows Pulling from a Windows 2000 Server, page 36-8
   - Windows Pulling from a Windows Server 2003 or Windows XP Host, page 36-8
4. Configure the Windows host to generate the correct event data.
5. Identify that host in MARS so that it can correctly parse and correlate the event data. For more information, see Configure the MARS to Pull or Receive Windows Host Logs, page 36-9.
6. Specify the time interval at which the event log data should be pulled from all identified host running Microsoft. For more information, see Windows Event Log Pulling Time Interval, page 36-11.

Enable Windows Pulling Using a Domain User

To enable Windows pulling using a domain user (***domain\username***), for example, CORP\syslog, do the following on the domain controller *before* you enable Windows pulling on your client:

Step 1 On the domain controller, click **Administrative Tools > Default Domain Security Policy > Security Settings > Local Policies > User Rights Management**.

Step 2 Grant the permission Manage auditing and security log to the domain user (domain\username).

Enable Windows Pulling from Windows NT

To enable MARS to pull event log data from a Windows NT host, follow these steps:

Step 1 From **Start > Programs > Administrative Tools > User Manager**, in the menu bar, choose **Policies**.

Step 2 In the submenu, choose **User Rights**, make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.

Step 3 In the submenu, choose **Audit**. Configure the audit policy according to your site's security auditing policy.

Enable Windows Pulling from a Windows 2000 Server

When there is no Active Directory Service (ADS) server sending domain information to your Windows 2000 server, you must set this property to *Disabled* on each host from which you want the MARS Appliance to pull syslogs.

To enabled MARS to pull event log data from a Windows 2000 host, follow these steps:

Step 1 Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

The Local Security Settings applet appears.

Step 2 Configure the settings under the following Local Policy groups as specified:

- Security Settings > Local Security Policy > User Rights Management

  Make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.

- Security Settings > Local Security Policy > Audit Policy

  Configure the audit policy according to your site's security auditing policy and ensure that all entries under Effective Setting are set to **Success, Failure**.

Windows Pulling from a Windows Server 2003 or Windows XP Host

To enable MARS to pull event log data from a Windows Server 2003 or Windows XP host, follow these steps:

Step 1 Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

The Local Security Settings applet appears.

Step 2 Configure the settings under the following Local Policy groups as specified:

- Security Settings > Local Security Policy > User Rights Management

  Make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.

- Security Settings > Local Security Policy > Audit Policy

  Configure the audit policy according to your site's security auditing policy.

Step 3 To grant the pulling account the privileges to read security, application and system event logs, use the method described in the Microsoft Knowledge Base Article Q323076, at the following URL:

http://support.microsoft.com/kb/323076/en-us

Note The pulling of an event log itself generates security event logs if certain events, such as **Log on/off**, are audited. We recommend you either set a default domain policy, or set the retention method for security event logs on your Windows system to be **Overwrite as needed**. Otherwise, when the log is full no new event log can be generated on the Windows system.

Example Configuration of Event Log Security Privileges on a Microsoft Windows 2003 Server

The following procedure is an example of the *Microsoft Configure Event Log Security Locally* procedure. Complete this procedure to give the pulling account the following event log privileges:

Step 1 Launch the Microsoft Windows regedit program. (Enter **regedit** from the **Start > Run** menu)

Step 2 Append (***A;;0x1;;; sid-of-the-pulling-account***) to the end of the following registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\CustomSD
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\CustomSD
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\CustomSD

Use the Security Identifier [SID] of the pulling account to replace the variable *sid-of-the-pulling-account* . For example, if the pulling account's SID is ***S-1-5-21-1801671234-2025421234-839521234-123456*** and the original value of CustomSD is as follows:

```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)
(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)
```

Change the CustomSD registry key as follows:

```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)
(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x1;;;S-1-5-21-1801671234-2025421234-839521234-123456)
```

Step 3 Save changes and exit regedit.

Configure the MARS to Pull or Receive Windows Host Logs

Once you've prepared the Microsoft Windows host, you must identify that host in MARS and identify whether the push or pull method is being used on that host.

To configure the MARS Appliance to either pull or receive logs, follow these steps:

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

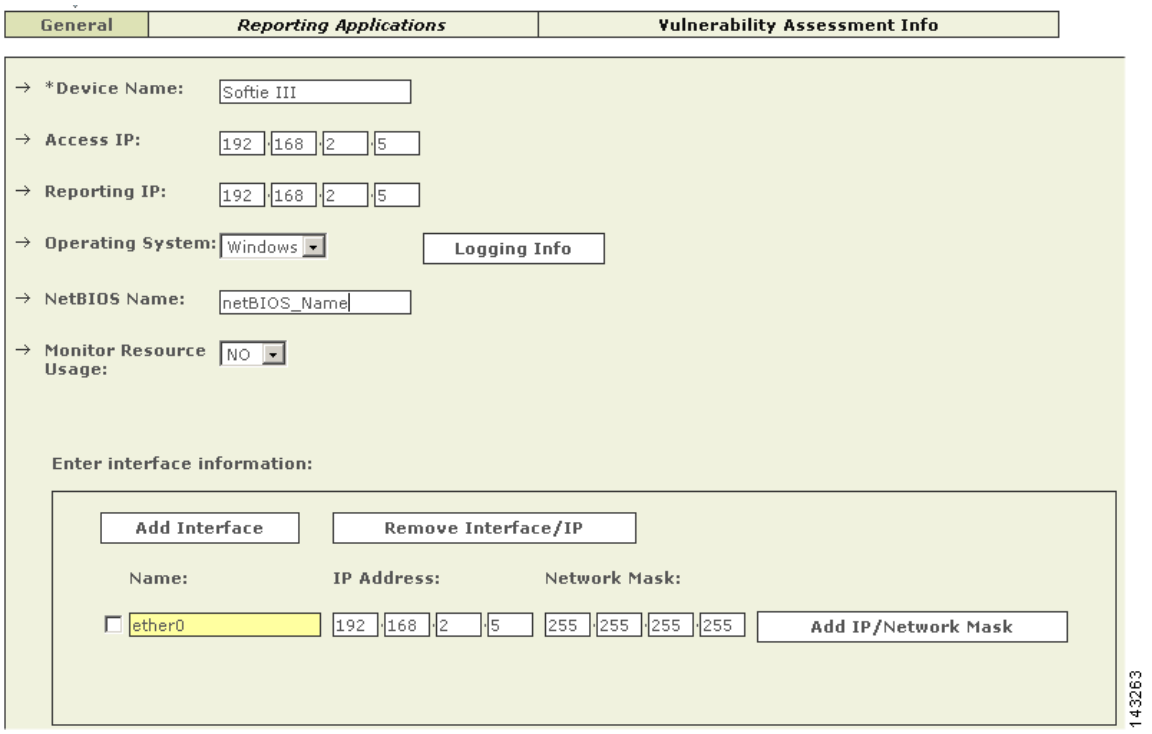
Step 2 From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3 Enter the Device Name and IP addresses if adding a new host.

Step 4 Select the **Operating System > Windows** from the list.

Step 5 (Optional) Enter **NetBIOS name**.

Figure 36-3 Window Log Configuration



Step 6 Click on **Logging Info** to configure OS Logging Information.

A new pop-up window appears.

Step 7 From the Windows Operating System, select the correct option for either the server or workstation version:

- Microsoft Windows 2000
- Microsoft Windows 2003 (Also used for Microsoft Windows XP platforms.)
- Microsoft Windows Generic
- Microsoft Windows NT

Note If you are selecting Microsoft Windows XP Home Edition, you must enable the Remote Procedure Call services under All Programs > Control Panel > Administrative Tools > Services.

Step 8 Select either the **Pull** or the **Receive** checkbox, based on the host configuration that you have performed.

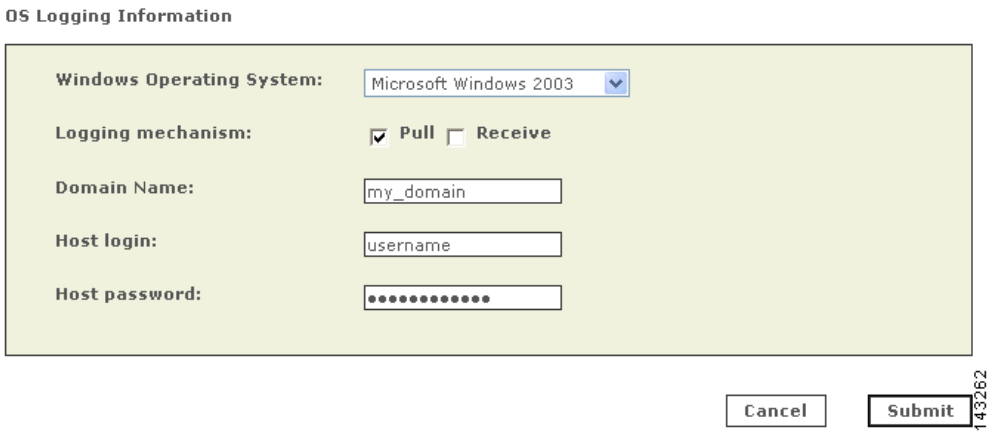
Caution Do not select both checkboxes. Doing so generates unpredictable results.

Step 9 If you selected the Pull method, enter values for the following fields:

- **Domain name**—Identifies the domain name to which the host belongs.
- **Host login**—Identifies the username with security audit and log permissions.
- **Host password**—Identifies that password that authenticates the username provided in the Host login field.

Step 10 Click **Submit**.

Figure 36-4 Windows Logging



Step 11 Click **Submit** to save your changes.

Step 12 Add Interface IP Address and Network Mask.

Step 13 Cclick **Apply**.

Step 14 Click the **Vulnerability Assessment Info** link to define the host information that MARS uses to determine false positive attacks against this host. Continue with Define Vulnerability Assessment Information, page 36-12.

Step 15 Click **Done** to save the changes.

Step 16 To activate the device, click **Activate**.

If you selected the pull check box in Step 8, verfiy that a value has been specified for the interval at which which MARS pulls an event log from the host. For more information, see Windows Event Log Pulling Time Interval, page 36-11.

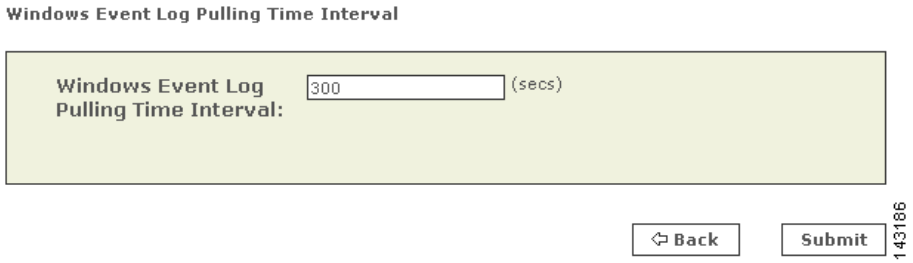
Windows Event Log Pulling Time Interval

You can now set the interval at which MARS pulls an event log from all Microsoft Windows host that are defined as reporting devices. This feature determines how often MARS requests logs from the Windows hosts that are configured a reporting devices.

Note If you are using SNARE to push the log data to MARS, then you do not need to enable this setting.

To configure the Windows event log pulling time interval, follow these steps:

Step 1 Click **Admin > System Parameters > Windows Event Log Pulling Time Interval**.



Step 2 Enter the new time interval in seconds.

The default value is 300 seconds (five minutes).

Step 3 Click **Submit**.

Define Vulnerability Assessment Information

For each host that you define in MARS, you can specify information about that host that assists MARS in assessing whether that host is vulnerable to the attacks that MARS detects. For example, you can identify the operating system running on the host, even providing the latest or nearest patch level. When an attack is detected that is targeted toward a specific operating system, then MARS can quickly determine whether the host is running the operating system that is targeted.

For hosts that are defined as the base platform of a reporting device, you should define this information as part of that device definition.

However, as MARS, it begins to add discovered hosts to the list of hosts under Management > IP Management. You should periodically review these hosts to update their information if you do not have a vulnerability assessment software device or service, such as Qualys QualysGuard, running on your network.

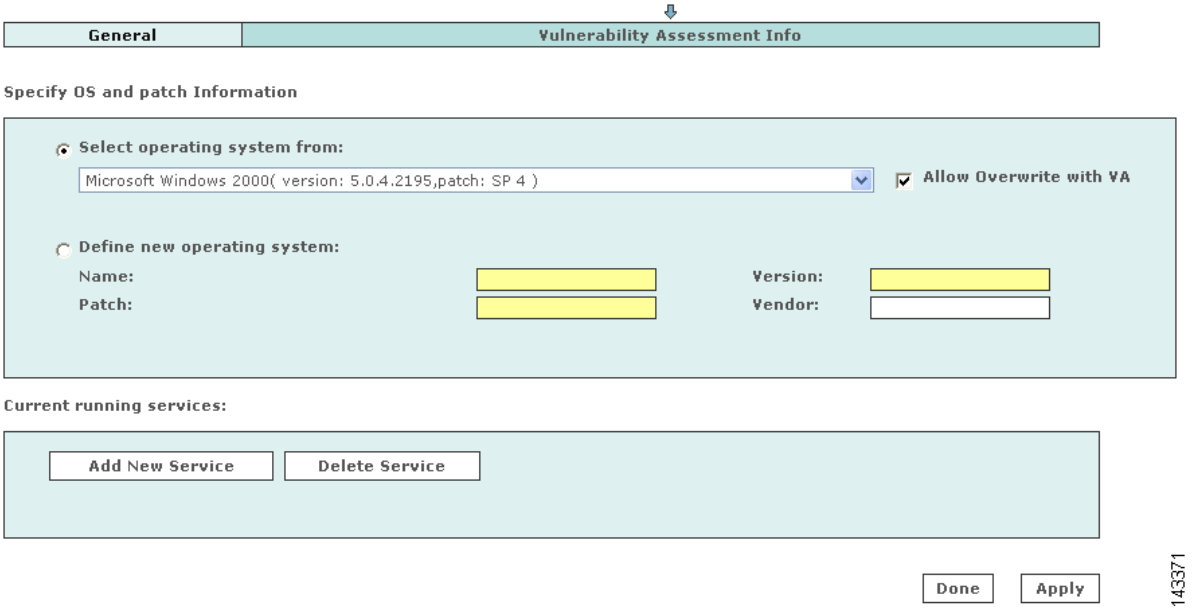
To specify the vulnerability assessment information for a host, follow these steps:

Step 1 To select the desired host, do one of the following:

- Select **Management > IP Management**, select the check box next to the desired host, and click **Edit**.
- Select **Admin > Security and Monitor Devices**, select the check box next to the desired host, and click **Edit**.

Step 2 Click the **Vulnerability Assessment Info** tab.

Figure 36-5 Vulnerability Assessment Info for a Host



Step 3 Under Specify OS and patch Information, do one of the following:

- Select **Select operating system from**, and then select the operating system that matches the one running on this host from the list. Continue with Step 4.
- Select **Define new operating system**, and continue with Step a..

a. Enter the name of the operating system in the Name field.

b. Enter the version number for this operating system in the Version field.

c. Enter the patch level associated with the version number the Patch field.

d. Enter the name of manufacturer of the operating system in the Vendor field.

e. Click **Apply** to save the operating system definition.

The new operating system definition is added to the Select operating system from list, and it is the selected option.

If you define a custom operating system, you must select **Generic** in the Operating System list on the General page of the host and click **Apply**. Otherwise, you cannot select the new operating system in the Select operating system from list.

Step 4 To allow the information that you provided to be overridden by a vulnerability assessment service running on your network, select the **Allow Overwrite with VA** checkbox.

Step 5 To add more detailed information about the host, continue with Identify Network Services Running on the Host, page 36-14.

Step 6 Click **Apply** to save the changes made to this host.

Step 7 Click **Done** to close the Host page.

Identify Network Services Running on the Host

By identifying the network services that are running on a host, you are specifying the types of network activities that you expect for this host. This data is helpful in eliminating expected activities that might otherwise be flagged as suspicious by MARS; for example, if you have administrative servers that run network discovery applications or perform vulnerability assessment probes at scheduled times.

To identify the network services running on a host, follow these steps:

Step 1 To select the desired host, do one of the following:

- Select **Management > IP Management**, select the check box next to the desired host, and click **Edit**.
- Select **Admin > Security and Monitor Devices**, select the check box next to the desired host, and click **Edit**.

Step 2 Click **Add New Service** under Current running services.

Note It may take five minutes or more for this dialog box to load. You can place the cursor over the title bar of the window that opens. This allows you to see if the window is still loading.

Step 3 Enter as much detail on the service and its applications as you can.

- You can choose between selecting a service and defining a new service.
- You can also choose between select an application or defining a new application.

Step 4 Click **Submit**.

Step 5 You can enter more services here by clicking **Add New Service**, or you can click **Submit** to continue.

Step 6 Click **Submit** to complete the addition of the host.

INDEX

Numerics

802.1x, logging in Cisco Secure ACS 26-6

A

AAA devices 26-1
Activate button
  activating reporting devices 1-15
  what it does 1-15
  when to use 1-15
adding
  CSV file 1-34
  devices 1-33
    manually 1-33
    seed file 1-34
  seed file 1-34

C

cautions
  significance of i-xvi
Cisco Adaptive Security Appliance, see Cisco ASA 19-1
Cisco ASA
  add to MARS 19-14
  bootstrapping 19-2
  security context
    add discovered 19-19
    define reporting options for 19-20
    make MARS aware of 19-17
Cisco Firewall Services Modules, see Cisco FWSM 19-1
Cisco FWSM
  add to MARS 19-14
  bootstrapping 19-2
  security context
    add discovered 19-19
    define reporting options for 19-20
    make MARS aware of 19-17
Cisco Secure ACS, 802.1x feature support 26-6
Cisco Secure ACS, 802.1x support 26-1
Cisco Secure ACS, audit logs required by MARS 26-4
Cisco Secure ACS, bootstrap 26-3
Cisco Secure ACS, event logs studied by MARS 26-1
Cisco Secure ACS, MARS agent 26-8
Cisco Secure ACS, NAC support 26-1
Cisco Secure ACS, representing in MARS 26-13, 26-15
Cisco Secure ACS, sever support 26-2
Cisco Secure ACS, solution engine 3x support 26-2
Cisco Secure ACS, solution engine 4.x support 26-2
Cisco Secure ACS, supported versions 26-1
Cisco Secure ACS, TACACS+ command authorization 26-8
community strings 1-16
conventions i-xv
credentials
  bulk update 1-46
CSC SSM 32-1
  bootstrap to report to MARS 32-1
  define module manually 32-2
CSV files 1-34

D

discovering networks
  automatic 1-18
discovery

scheduling 1-18
updating 1-18
documentation
conventions i-xv
ordering i-xvi

E

error messages, list of 26-16
event log
changing pulling time interval for Windows 36-11

I

IPS
virtual sensor 4-5

L

Linux host, bootstrap 36-2
loading
MARS
seed file 1-45

M

Microsoft Windows host, bootstrap 36-4

N

NAC, AAA server support 26-1
NAC Appliance
define appliance manually 23-2
NetFllow, enable processing 20-7
NetFlow
Global NetFlow UPD Port 20-8
NetFlow,enable processing 20-8
NetFlow,examined networks 20-9
NetFlow, store ASA NetFlow 20-8
NetScreen
IDP 2.x 3-1
IDP 3.x 3-1
IDP 4.0 3-1
IDP-Management Server 3-1
Security Manager 3-1
network discovery
auto-populate MARS 1-15
exceptions to discovery 1-16
how it works 1-16
restricting list 1-17, 1-18
work around exceptions 1-16

P

PIX
add to MARS 19-14
bootstrapping 19-2
security context
add discovered 19-19
define reporting options for 19-20
make MARS aware of 19-17
PIX Security Appliance, see PIX 19-1
PN Log agent 26-8
PN Log Agent, error messages 26-11
public networks 1-17

S

scheduling
discovery 1-18
Secure Syslog 20-6
security contexts
add discovered 19-19
define reporting options 19-20
make MARS aware of 19-17
security guidelines

obtaining i-xvi
seed file
credentials
bulk update 1-46
CSV file 1-34
loading 1-45
SNMP RO, unsupported characters 1-10, 1-40
Snort
syslog format expectation 6-1
Solaris host, bootstrap 36-2
support
obtaining i-xvi

T

troubleshoot
error messages 26-16
troubleshooting
Cisco Secure ACS integration 26-15

V

valid networks 1-17

W

warnings
significance of i-xvi