



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 software 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 Incident 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 separate 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	<i>italic font</i>
Displayed session and system information, paths and file names	<code>screen font</code>
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
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.