



Preface

Introduction

Thank you for purchasing the Cisco Security Monitoring, Analysis, and Response System (MARS) Local Controller. appliance. This guide will help you get the most value from your MARS Appliance.



Note

The information in this document referring to a “MARS appliance” also applies to MARS use as Local Controller in a Global Controller architecture.

The MARS Appliance

The Cisco Security Monitoring, Analysis, and Response System Appliance (MARS Appliance)– the MARS 20, MARS 50, MARS 100, and MARS 200 – is a Security Threat Mitigation (STM) appliance. It delivers a range of information about your networks’ health as seen through the “eyes” and “ears” of the reporting devices in your networks. It takes in all of the raw events from your reporting devices, sessionizes them across different devices, fires default rules for incidents, determines false positives, and delivers consolidated information through diagrams, charts, queries, reports, and rules.

The MARS operates at distinct and separate levels based on how much information is provided about your networks’ devices. At its most basic level, MARS functions as a syslog server. As you add information about reporting devices, it starts sessionizing, and when fully enabled, it presents a bird’s-eye view of your networks with the ability to quickly drill-down to a specific MAC address.

The MARS Web Interface

The MARS user interface uses a tabbed, hyperlinked, browser-based interface. If you have used the Web, you have used similar Web pages.



Note

When using the MARS user interface, avoid using the Back and Forward arrows in the browser. Using these arrows can lead to unpredictable behavior.

About This Manual

This manual describes the features and functionality of the Local Controller. The layout of this manual is as follows:

- [Chapter 1, “STM Task Flow Overview,”](#) recommends a taskflow for planning and implementing your security threat mitigation system. It ties back to your corporate security policies and presents a structure deployment and configuration strategy based on two phases: provisioning and monitoring.

Part I: Provisioning Phase. This part details provisioning your network devices to communicate with MARS. It involves performing device inventories, bootstrapping and configuring the reporting devices and mitigation devices to communicate with the MARS Appliance, and performing device-side tuning.

- [Chapter 2, “Reporting and Mitigation Devices Overview,”](#) discusses concepts important to a successful deployment of MARS. These concepts include selecting among the devices on your network, understanding the levels of operation, and performing those tasks that affect many devices, such as defining data pulling schedules.
- [Chapter 3, “Configuring Router and Switch Devices.”](#)
- [Chapter 4, “Configuring Firewall Devices.”](#)
- [Chapter 5, “Configuring VPN Devices.”](#)
- [Chapter 6, “Configuring Network-based IDS and IPS Devices.”](#)
- [Chapter 7, “Configuring Host-Based IDS and IPS Devices.”](#)
- [Chapter 8, “Configuring Antivirus Devices.”](#)
- [Chapter 9, “Configuring Vulnerability Assessment Devices.”](#)
- [Chapter 10, “Configuring Generic, Solaris, Linux, and Windows Application Hosts.”](#)
- [Chapter 11, “Configuring Database Applications.”](#)
- [Chapter 12, “Configuring Web Server Devices.”](#)
- [Chapter 13, “Configuring Web Proxy Devices.”](#)
- [Chapter 14, “Configuring AAA Devices.”](#)
- [Chapter 15, “Configuring Custom Devices.”](#)

Part II: Monitoring Phase. This part concepts important to successfully using MARS to monitor your network. These concepts include defining inspection rules and investigating incidents.

- [Chapter 16, “Policy Table Lookup on Cisco Security Manager”](#) explains how to integrate with Cisco Security Manager and use the policy lookup features in MARS.
- [Chapter 17, “Network Summary”](#) covers the Summary pages which includes the Dashboard, the Network Status, and the My Reports pages.
- [Chapter 18, “Case Management”](#) covers using cases to provide accountability and improve workflow.
- [Chapter 19, “Incident Investigation and Mitigation”](#) covers incidents and false positives and provides a starting point for configuring a Layer 2 path and mitigation to work with a MARS.
- [Chapter 20, “Queries and Reports”](#) covers working with scheduled and on-demand reports and queries. It also discussing using the real-time event viewer.
- [Chapter 21, “Rules”](#) covers defining and use inspection rules.

- [Chapter 22, “Sending Alerts and Incident Notifications”](#) explains how to configure the MARS to send an alert based on an inspection rule.
- [Chapter 23, “Management Tab Overview”](#) covers managing events, networks, variables, hosts, services, and MARS users.
- [Chapter 24, “System Maintenance”](#) covers some of the maintenance chores for the MARS.

Additionally, the following appendices are provided:

- [Appendix A, “Cisco Security MARS XML API Reference,”](#) presents the XML schema used by MARS for XML-based notifications.
- [Appendix B, “Regular Expression Reference,”](#) The syntax and semantics of the regular expressions supported by PCRE are described in this appendix.
- [Appendix C, “Date/Time Format Specification,”](#) The date/time field parsing is supported using the Unix `strptime()` standard C library function.
- [Appendix D, “System Rules and Reports,”](#) lists descriptions of all system rules and reports.
- [Glossary](#) — A glossary of terms as they relate to MARS.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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.

