



Preface

Introduction

Global Controller helps network administrators, network operators, and security analysts be more productive by:

- Reducing the amount of raw data you have to wade through
- Enabling you to see your network security posture as it evolves
- Identifying Hot Spots of malicious activity
- Removing unwanted traffic from your network.

Global Controller Overview

The Global Controller is a Security Threat Mitigation (STM) system. It summarizes information about the health of your network as viewed through the reporting devices.

The Global Controller:

- Collects all raw events,
- 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 Global Controller User Interface

The Global Controller system employs a Global Controller to monitor and manage Local Controllers and their monitored devices in the network. The Global Controller user interface uses a tabbed, hyperlinked, browser-based interface. If you have used the Web, you have used similar pages.



Note

When using the Global Controller user interface, avoid using the browser's **Back** and **Forward** buttons. Using these buttons can lead to unpredictable behavior.

About This Manual

This manual describes the features and functionality of the Global Controller.

The layout of this manual is as follows:

- [Chapter 1, “Introduction,”](#)— This chapter introduces the Global Controller and presents its basic features and deployment options.
- [Chapter 2, “Configuring the Global Controller,”](#)— This chapter covers connecting to the Global Controller for the first time, and setting up and configuring your network security devices to connect to the Global Controller.

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 3, “Authenticating MARS Accounts with External AAA Servers,”](#) describes how to configure AAA servers to authenticate MARS users.
- [Chapter 4, “Network Summary,”](#) covers the Summary pages which includes the Dashboard, the Network Status, and the My Reports pages.
- [Chapter 5, “Case Management,”](#) covers using cases to provide accountability and improve workflow.
- [Chapter 6, “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 7, “Queries and Reports,”](#) covers working with scheduled and on-demand reports and queries. It also discussing using the real-time event viewer.
- [Chapter 8, “Rules,”](#) covers defining and use inspection rules.
- [Chapter 9, “Sending Alerts and Incident Notifications,”](#) explains how to configure the MARS to send an alert based on an inspection rule.
- [Chapter 10, “Management Tab Overview,”](#) covers managing events, networks, variables, hosts, services, and MARS users.
- [Chapter 11, “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,”](#) represents 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 all MARS system rules and reports with their descriptions.
- [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.

