



User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x

October 2010

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-16777-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xlv

Audience xlv

Organization xlv

Conventions xlv

Obtaining Documentation and Submitting a Service Request i-xlvii

CHAPTER 1

Introduction to MARS 1-1

System Description 1-1

Local Controller 1-2

Global Controller 1-3

Advantages of a Distributed Global/Local Architecture 1-3

MARS Web Interface 1-4

Reporting and Mitigation Devices 1-4

Basic Functions of the Global Controller 1-4

Incidents 1-5

Rules 1-5

Centralized Maintenance 1-5

Deployment 1-5

Incremental Deployment 1-5

Green-field, Multi-box Deployment 1-6

Zone Planning 1-6

CHAPTER 2

Security Threat Mitigation (STM) Task Flow Overview 2-1

Policy Objectives 2-1

Security Policy Objectives 2-1

Monitoring Policy Objectives 2-2

Mitigation Policy Objectives 2-2

Remediation Policy Objectives 2-2

Cisco Security Wheel 2-3

Checklist for Provisioning Phase 2-3

Checklist for Monitoring Phase 2-9

Strategies for Monitoring, Notification, Mitigation, Remediation, and Audit 2-14

Appliance-side Tuning Guidelines 2-15

Device Inventory Worksheet 2-16

User Role Worksheet 2-18

CHAPTER 3

Reports and Mitigation Devices Overview 3-1

Levels of Operation 3-1

Selection of the Devices to Monitor 3-2

Understanding Access IP, Reporting IP, and Interface Settings 3-7

Access IP 3-8

Reporting IP 3-8

Interface Settings 3-9

Selection of the Access Type 3-9

Configure SNMP Access for Devices in MARS 3-10

Configure Telnet Access for Devices in MARS 3-11

Configure SSH Access for Devices in MARS 3-12

Configure FTP Access for Devices in MARS 3-12

Operating Upon Reporting and Mitigating Devices 3-13

Edit a Device 3-13

Upgrade the Device Type to a Newer Version 3-13

Delete a Device 3-14

Delete All Displayed Reporting Devices 3-15

Verifying Connectivity with the Reporting and Mitigation Devices 3-15

Discovering and Testing Connectivity Options 3-16

Run a Reporting Device Query 3-16

Activate the Reporting and Mitigation Devices 3-17

Data Enabling Features 3-17

Layer 2 Discovery and Mitigation 3-18

Networks for Dynamic Vulnerability Scanning 3-19

Select a Network for Scanning 3-19

Create a Network IP Address for Scanning 3-19

Create a Network IP Range for Scanning 3-20

Understanding NetFlow Anomaly Detection 3-20

How MARS Uses NetFlow Data 3-21

Guidelines for Configuring NetFlow on Your Network 3-21

Enable Cisco IOS Routers and Switches to Send NetFlow to MARS 3-22

Configuring Cisco CatIOS Switch 3-23

Enable NetFlow Processing in MARS 3-23

Host and Device Identification and Detail Strategies 3-27

Discovering Your Network: Layer 3 Topology Discovery 3-27

Define SNMP Discovery Settings for a Network or IP Range 3-28

Add Valid Networks to Discovery List	3-30
Remove Networks from Discovery List	3-30
Discover Layer 3 Data On Demand	3-31
Scheduling Topology Updates	3-31
Schedule a Network Discovery	3-32
Edit a Scheduled Topology Discovery	3-33
Delete a Scheduled Topology Discovery	3-33
Run a Topology Discovery on Demand	3-33
Troubleshoot Layer 3 Network Discovery	3-34
Configuring Resource Usage Data	3-34
Enabling the Required SNMP OIDs for Resource Monitoring	3-36
Configuring Network Admission Control Features	3-39
Integrating MARS with 3rd-Party Applications	3-41
Forwarding Alert Data to 3rd -Party Syslog and SNMP Servers	3-41
Syslog Relay Support	3-41
Enable the Syslog Relay Feature	3-42
Disable the Syslog Relay Feature	3-43
MARS Events, System Rule, and Report Details for the Syslog Relay Feature	3-43
Troubleshooting the Syslog Forwarding Feature	3-44
MARS MIB Format	3-44
Relaying Syslog Messages from 3rd-Party Syslog Servers	3-45
Configuring Syslog-ng Server to Forward Events to MARS	3-46
Configure Kiwi Syslog Server to Forward Events to MARS	3-46
Add Syslog Relay Server to MARS	3-47
Adding Devices Monitored by Syslog Relay Server	3-48

CHAPTER 4

Rules 4-1

Rules Overview	4-1
Prioritizing and Identifying	4-2
Thinking Like a Black Hat	4-2
Planning an Attack	4-2
Back to Being the Admin	4-3
Types of Rules	4-4
Inspection Rules	4-4
Global User Inspection Rules	4-4
Drop Rules	4-5
Constructing a Rule	4-5
Working Examples	4-12
Example A: Excessive Denies to a Particular Port on the Same Host	4-13

Example B: Same Source Causing Excessive Denies on a Particular Port	4-13
Example C: Same Host, Same Destination, Same Port Denied	4-13
Working with System and User Inspection Rules	4-14
Change Rule Status—Active and Inactive	4-14
Duplicate a Rule	4-15
Editing a Rule	4-15
Edit a Rule with Inline Editing	4-15
Edit a Rule with the Rule Wizard	4-16
Add an Inspection Rule	4-16
Working with Drop Rules	4-18
Change Drop Rule Status—Active and Inactive	4-18
Duplicate a Drop Rule	4-19
Edit a Drop Rule	4-19
Add a Drop Rule	4-19
Setting Alerts	4-21
Configure an Alert for an Existing Rule	4-21
Rule and Report Groups	4-22
Rule and Report Group Overview	4-22
Global Controller and Local Controller Restrictions for Rule and Report Groups	4-24
Adding, Modifying, or Deleting a Rule Group	4-24
Add a Rule Group	4-25
Modify a Rule Group	4-26
Delete a Rule Group	4-27
Adding, Modifying, or Deleting a Report Group	4-27
Add a New Report Group	4-27
Modify a Report Group	4-29
Delete a Report Group	4-29
Display Incidents Related to a Rule Group	4-30
Create Query Criteria with Report Groups	4-30
Use Rule Groups in Query Criteria	4-31

CHAPTER 5

Alerts and Incident Notifications 5-1

Notification Methods	5-1
MARS Incident Notification Examples	5-3
MARS Email Notification	5-4
MARS Syslog Notification	5-5
MARS SNMP Trap Notification	5-6
MARS XML Notification Email Attachment	5-6
MARS SMS Notification Example	5-7

Configure the E-mail Server Settings	5-7
Configure a Rule to Send an Alert Action	5-8
Create a User—Role, Identity, Password, and Notification Information	5-13
Create a Custom User Group	5-15
Add a User to a Custom User Group	5-16

CHAPTER 6

Management Tab Overview	6-1
Understanding the Activate Button	6-1
Event Management	6-2
Search for an Event Description or CVE Names	6-2
View a List of All Currently Supported CVEs	6-2
Using Event Groups	6-2
Filtering by Event Groups or Severity	6-2
Edit a Group of Events	6-2
Add an Event Group	6-3
IP Management	6-3
Search for an Address, Network, Variable, or Host	6-4
Filter IP Management List	6-4
Edit an IP Group	6-4
Add an IP Group	6-4
Add a Network, IP Range, or Variable	6-5
Add a Host to a Local Controller	6-5
Edit Host Information on a Local Controller	6-7
Service Management	6-8
Search for a Service	6-8
Add a Group of Services	6-9
Edit a Group of Services	6-9
Add a Service	6-10
Edit a Service	6-10
Delete a Service	6-10
User Management	6-11
Top Level Control	6-11
Basic User Management	6-11
Global and Local Controller User Management Functions	6-12
User Credentials	6-12
Adding a New User	6-12
Adding a Service Provider (Cell phone/Pager)	6-14
Searching for a User	6-14

Editing or Removing a User	6-15
Creating a User Group	6-15
Adding or Removing a User from a Custom User Group	6-15
Filtering by Groups	6-16
Promoting Global User Roles on Local Controller	6-16

CHAPTER 7

Network Summary 7-1

Global Controller Network Summary Page Concepts	7-1
Global Controller Technologies	7-1
Navigation within the MARS Appliance	7-2
Log In to the Local Controller	7-2
Log In to the Global Controller	7-3
Basic Navigation	7-4
Links, Icons, and Filters for Navigation	7-4
Tabs for Navigation	7-4
Help Page	7-6
Your Suggestions Welcomed	7-6
Set the GUI and CLI Timeout Interval	7-7
Set the Logon Banner Message	7-9
Activate Button	7-10
Activate Button Color Changes	7-11
Global Controller Activation Considerations	7-12
Automatic Activation Settings Page	7-12
Set the Activation Interval	7-13
Summary Pages	7-13
Dashboard	7-14
Recent Incidents	7-16
Sessions and Events	7-16
Inactive Device Events	7-17
Data Reduction	7-17
Page Refresh	7-17
Diagrams	7-18
Diagram Manipulation	7-19
Display Devices in Topology	7-20
Network Status	7-20
Improving Status Display Refresh	7-21
Chart Reading	7-21
Hotspots	7-23
My Reports	7-24

Set up Reports for Viewing 7-24

CHAPTER 8

Queries and Reports 8-1

Understanding Queries 8-1

Global Controller Query Interface 8-2

Local Controller Query Interface 8-3

Selecting the Query Type 8-3

Result Format 8-4

Order/Rank By 8-6

Filter By Time 8-6

Use Only Firing Events 8-7

Maximum Number of Rows Returned 8-7

Select Query Criteria 8-7

Query Criteria Descriptions 8-9

Source IP 8-9

Destination IP 8-9

Service 8-9

Events 8-10

Device 8-10

Reported User 8-10

IPS Risk Rating 8-10

IPS Threat Rating 8-10

IPS Global Correlation Score 8-10

Keyword 8-11

Operation 8-11

Rule 8-12

Action 8-12

Saving the Query 8-12

Query Operations 8-12

Run a Quick Query 8-12

Run a Keyword Query 8-13

Batch Query Operations 8-14

Define and Run a Batch Query 8-15

Stop a Batch Query 8-16

Resubmit a Batch Query 8-17

Delete a Batch Query 8-17

Perform a Long-Duration Query Using a Report 8-17

Select Custom Columns for Query Result Display 8-19

View a Query Result in the Report Tab 8-21

Viewing Events in Real-time	8-22
Restrictions for Real-time Event Viewer	8-22
Invoke the Real-Time Event Viewer on a Local Controller	8-23
Reports	8-26
Global Controller Reports	8-27
Local Controller Reports	8-27
Report Type Views: Total vs. Peak vs. Recent	8-27
Report Charts and Graphs	8-29
Report Creation	8-29
Create a New Local Controller Report	8-29
Create a New Global Controller Report	8-30
Operations on Existing Reports	8-30
View a Report	8-31
Run a Report	8-31
Delete a Report	8-31
Edit a Report	8-31
Duplicate a Report	8-32

CHAPTER 9

Incident Investigation and Mitigation 9-1

Incidents Overview	9-1
The Incidents Page	9-2
Time ranges for Incidents	9-4
Incident Details Page	9-4
Search for a Session ID or Incident ID	9-5
Incident Details Table	9-5
False Positive Confirmation	9-7
The False Positive Page	9-9
Tune a False Positive	9-10
Tune an Unconfirmed False Positive to False Positive	9-11
Tune an Unconfirmed False Positive to True Positive	9-11
Activate False Positive Drop Rules	9-11
Mitigation	9-11
802.1X Mitigation Example	9-12
Prerequisites for Mitigation with 802.1X Network Mapping	9-12
Perform Mitigation with 802.1X Network Mapping	9-13
Display Dynamic Device Information	9-16
Virtual Private Network Considerations	9-18
Layer 2 Path and Mitigation Configuration Example	9-18
Prerequisites for Layer 2 Path and Mitigation	9-18

Components Used	9-18
Network Diagram	9-18
Procedures for Layer 2 Path and Mitigation	9-20
Add the Cisco Catalyst 5000 with SNMP as the Access Type	9-20
Add the Cisco Catalyst 6500 with SNMP as Access Type (Layer 2 only)	9-21
Add the Cisco 7500 Router with TELNET as the Access Type	9-22
Verify the Connectivity Paths for Layer 3 and Layer 2	9-22
View Session via a Query	9-23
Perform Mitigation	9-26

CHAPTER 10

Case Management 10-1

Case Management Overview	10-1
Case Management Considerations for the Global Controller	10-3
Hide and Display the Case Bar	10-3
Hiding the Case Bar	10-4
Displaying the Case Bar	10-4
Create a New Case	10-5
Edit and Change the Current Case	10-6
Deselecting the Current Case	10-6
Add Data to a Case	10-7
Generate and Email a Case Report	10-7

CHAPTER 11

Security Manager Policy Table Lookup from a MARS Event 11-1

Taskflow for Policy Table Query from MARS Events	11-2
Understanding Security Manager Device Lookup	11-4
Understanding Access Rule Table Lookup	11-5
Security Appliance and Router System Log Messages Supported for Policy Lookup	11-7
Understanding Signature Table Lookup	11-8
Issues Regarding Policy Table Lookup from MARS	11-8
Checklist for Policy Table Lookup from MARS	11-14
Devices and OS Versions Supported by Both Security Manager and MARS	11-15
Bootstrapping Security Manager Server to Communicate with MARS	11-16
Adding a Security Manager Server to MARS GC	11-16
Adding a Security Manager Server to MARS LC	11-20
Navigating to Access Rule Policy in Security Manager from MARS	11-24
Navigating to IPS Signature Policy in Security Manager from MARS	11-28
Read-Only Security Manager Policy Lookup Page for Access Rules	11-35

[Read-Only Security Manager Policy Lookup Page for an IPS Signature](#) 11-39

CHAPTER 12

Botnet Traffic Filtering 12-1

- [Information About Botnet Traffic Filtering](#) 12-1
- [Query Criteria, System Reports, and Rules Related to Botnet Traffic Filtering](#) 12-3
 - [Botnet Site Query Criteria for Queries, Reports, and Rules](#) 12-3
 - [Query Result Formats for Botnet Traffic Filter](#) 12-4
 - [Site Ranking Query Result Format](#) 12-5
 - [All Matching Events With Botnet Sites Result Format](#) 12-6
- [System Reports](#) 12-8
- [MARS System Rules and Notifications for Botnet Traffic Filtering](#) 12-11
 - [Botnet Traffic Filter Notifications](#) 12-11
 - [MARS Events for Botnet Traffic Filter](#) 12-12
- [Site Management Page](#) 12-14
 - [Deleting Sites](#) 12-14

CHAPTER 13

System Maintenance 13-1

- [Setting Runtime Logging Levels](#) 13-1
- [Viewing the MARS Backend Log Files](#) 13-2
- [Viewing the Audit Trail](#) 13-2
- [Retrieving Raw Messages](#) 13-3
 - [About Raw Message Size Limitations and Storage Location](#) 13-3
 - [Retrieve Raw Messages](#) 13-4
- [Change the Default Password of the Administrator Account](#) 13-7
- [Understanding Certificate and Fingerprint Validation and Management](#) 13-7
 - [Setting the Global Certificate and Fingerprint Response](#) 13-8
 - [Upgrading from an Expired Certificate or Fingerprint](#) 13-9
 - [Upgrade a Certificate or Fingerprint Interactively](#) 13-9
 - [Upgrade a Certificate Manually](#) 13-9
 - [Upgrade a Fingerprint Manually](#) 13-10
 - [Monitoring Certificate Status and Changes](#) 13-10
- [Database Tuning and Query Optimization](#) 13-11
 - [About Database Indexing](#) 13-11
 - [Understanding the Data Indexing/Query Optimization Page](#) 13-12
 - [Data Indexing/Query Optimization Procedures](#) 13-13
 - [Calculate Cardinality](#) 13-14
 - [Create Database Index](#) 13-14
 - [Schedule Database Optimization](#) 13-15

Drop Index 13-15

CHAPTER 14

Authenticating MARS Accounts with External AAA Servers 14-1

Information About Authenticating MARS User Accounts with External AAA Servers 14-1

Supported AAA Protocols and Servers 14-2

Configuration Overview 14-2

Summary of MARS Appliance AAA Configuration Tasks 14-2

Summary of AAA Server Configuration Tasks 14-3

Global Controller Considerations with External AAA Servers 14-3

Failed Authentication Lockout (Login Failure) 14-4

System Events related to Authentication and Login Attempts 14-4

System Reports and Rules Related to Authentication Method 14-8

System Reports 14-8

System Rules 14-8

Procedure for First-time Configuration of MARS AAA Feature 14-9

Edit an External AAA Server 14-15

Delete an External AAA Server 14-16

Unlock an Account after Login Failure 14-16

CHAPTER 15

Monitoring Events from Custom and Unsupported Devices or Versions 15-1

Overview of the Device Support Framework 15-3

Specify the Provider Configuration 15-4

Checklist for Defining and Exporting a Device Support Package 15-5

Create a Device Type 15-7

Create Device Event Types for a Custom Device Type 15-8

Editing a Device Type 15-17

Overriding Existing Parsers 15-17

Extending Existing Device Types 15-18

Add a Reporting Device based on a Custom Appliance Device Type 15-18

Add a Reporting Device based on a Custom Software Device Type 15-19

Import a Device Support Package 15-20

Export a Device Support Package 15-24

Remove an Installed Device Support Package 15-28

Events and Reports About Device Support Package Activities 15-28

MARS Forum on NetPro: An Overview 15-31

Uploading a Device Support Package to the MARS Forum 15-31

Download a Device Support Package from the MARS Forum on NetPro 15-32

Subscribe to Package Sharing Page of the MARS Forum 15-33

Example Custom Device Type: Custom Software Application 15-34

APPENDIX A

Date/Time Format Specification A-1

Using strftime() A-1

APPENDIX B

Regular Expression Reference B-1

PCRE Regular Expression Details B-2

Backslash B-3

Non-printing Characters B-3

Generic Character Types B-4

Unicode Character Properties B-5

Simple Assertions B-6

Circumflex and Dollar B-7

Full Stop (Period, Dot) B-8

Matching a Single Byte B-8

Square Brackets and Character Classes B-8

Posix Character Classes B-9

Vertical Bar B-10

Internal Option Setting B-10

Subpatterns B-11

Named Subpatterns B-12

Repetition B-12

Atomic Grouping and Possessive Quantifiers B-14

Back References B-15

Assertions B-16

Lookahead Assertions B-16

Lookbehind Assertions B-17

Using Multiple Assertions B-18

Conditional Subpatterns B-18

Comments B-19

Recursive Patterns B-19

Subpatterns as Subroutines B-21

Callouts B-21

APPENDIX C

DSF Event Type Group Reference C-1

DSF Event Type Group Descriptions C-1

APPENDIX D**Cisco Security MARS XML API Reference D-1**

- XML Schema Overview D-1
- XML Incident Notification Data File and Schema D-1
 - XML Incident Notification Data File Sample Output D-2
 - XML Incident Notification Schema D-6
 - Usage Guidelines and Conventions for XML Incident Notification D-6

APPENDIX E**System Rules and Reports E-1**

- System Rules by Category E-1
 - System: ASA Botnet Traffic Filter E-2
 - System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter E-2
 - System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter E-2
 - System: Access E-2
 - System Rule: Password Attack: Remote VPN Access - Success Likely E-3
 - System Rule: Password Attack: System - Success Likely E-3
 - System Rule: Password Attack: Database - Attempt E-3
 - System Rule: Password Attack: Database - Success Likely E-3
 - System Rule: Password Attack: FTP Server - Attempt E-3
 - System Rule: Password Attack: Mail Server - Attempt E-3
 - System Rule: Password Attack: Remote VPN Access - Attempt E-3
 - System Rule: Password Attack: Network Share - Attempt E-4
 - System Rule: Password Attack: SNMP - Attempt E-4
 - System Rule: Password Attack: System - Attempt E-4
 - System Rule: Password Attack: Misc. Application - Attempt E-4
 - System Rule: Password Attack: Web Server - Attempt E-4
 - System Rule: Password Attack: FTP Server - Success Likely E-4
 - System Rule: Password Attack: Mail Server - Success Likely E-4
 - System Rule: Password Attack: Network Share - Success Likely E-5
 - System Rule: Password Attack: SNMP - Success Likely E-5
 - System Rule: Password Attack: Disabled Accounts E-5
 - System Rule: Password Scan: Disabled Accounts: Distinct Hosts E-5
 - System Rule: Password Scan: Disabled Accounts: Same Host E-5
 - System Rule: Password Scan: Distinct Hosts E-5
 - System Rule: Password Scan: Same Host E-5
 - System: CS-MARS Distributed Threat Mitigation (Cisco DTM) E-5
 - System Rule: Connectivity Issue: IOS IPS DTM E-5
 - System Rule: Resource Issue: IOS IPS DTM E-6
 - System: CS-MARS Incident Response E-6
 - System Rule: CS-MARS Host Mitigation - Failure E-6

System Rule: CS-MARS Host Mitigation - Success	E-6
System Rule: Connectivity Issue: IOS IPS DTM	E-6
System Rule: Resource Issue: IOS IPS DTM	E-6
System: CS-MARS Issue	E-6
System Rule: CS-MARS Database Partition Usage	E-7
System Rule: Resource Issue: CS-MARS	E-7
System Rule: CS-MARS Failure Saving Certificates/Fingerprints	E-7
System Rule: CS-MARS Authentication Method Modified - AAA to Local	E-7
System Rule: CS-MARS IPS Signature Update Failure	E-7
System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch	E-7
System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue	E-8
System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions	E-8
System Rule: CS-MARS Login Failures - Admin User	E-8
System Rule: CS-MARS Login Failures - Non-Admin User	E-8
System Rule: CS-MARS SMTP Server Communication Failure	E-8
System: Client Exploits, Virus, Worm and Malware	E-8
System Rule: Backdoor: Connect	E-9
System Rule: Client Exploit - Attempt	E-9
System Rule: Backdoor: Covert Channel	E-9
System Rule: Worm Propagation - Success Likely	E-9
System Rule: Client Exploit - Sysbug Trojan	E-9
System Rule: Backdoor: Spyware	E-10
System Rule: Network Activity: Windows Popup Spam	E-10
System Rule: Worm Propagation - Attempt	E-10
System Rule: Backdoor: Active	E-10
System Rule: Client Exploit - Success Likely	E-10
System Rule: Network Activity: Excessive Denies - Host Compromise Likely	E-10
System Rule: Client Exploit - Mass Mailing Worm	E-10
System Rule: Client Exploit - Sasser Worm	E-11
System Rule: Virus Found - Cleaned	E-11
System Rule: Virus Found - Not Cleaned	E-11
System Rule: New Malware Discovered	E-11
System Rule: New Malware Prevention Deployed	E-11
System Rule: New Malware Prevention Deployment Failed	E-11
System Rule: New Malware Traffic Match	E-11
System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter	E-11
System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter	E-11
System: Configuration Issue	E-12
System Rule: Configuration Issue: Firewall	E-12
System Rule: Configuration Issue: Server	E-12

System Rule: Modify Network Config	E-12
System Rule: Modify Server: SCADA Modbus	E-12
System: Database Server Activity	E-12
System Rule: Database Privileged Command - Failures	E-12
System: Host Activity	E-13
System Rule: Modify Host: Files	E-13
System Rule: Modify Host: Service	E-13
System Rule: Modify Host: Logs	E-13
System Rule: Modify Host: Registry	E-13
System Rule: Modify Host: Security	E-13
System Rule: Modify Host: User Group	E-13
System Rule: Modify Host: Database Object - Failures	E-13
System Rule: Modify Host: Database User/Group - Failures	E-14
System: Network Attacks and DoS	E-14
System Rule: Sudden Traffic Increase To Port	E-14
System Rule: DoS: Network - Attempt	E-14
System Rule: Misc. Attacks: ARP Poisoning	E-14
System Rule: Misc. Attacks: Session Hijacking	E-14
System Rule: Misc. Attacks: Identity Spoofing	E-14
System Rule: DoS: Network - Success Likely	E-15
System Rule: DoS: Network Device - Attempt	E-15
System Rule: DoS: Network Device - Success Likely	E-15
System Rule: WLAN DoS Attack Detected	E-15
System: New Malware Outbreak (Cisco ICS)	E-15
System Rule: New Malware Discovered	E-15
System Rule: New Malware Prevention Deployed	E-15
System Rule: New Malware Prevention Deployment Failed	E-16
System Rule: New Malware Traffic Match	E-16
System: Operational Issue	E-16
System Rule: Network Errors - Likely Routing Related	E-16
System Rule: State Change: Host	E-17
System Rule: State Change: SCADA Modbus	E-17
System Rule: Operational Issue: Firewall	E-17
System Rule: Operational Issue: IDS	E-17
System Rule: Operational Issue: Server	E-17
System Rule: Operational Issue: Router / Switch	E-17
System Rule: State Change: Network Device	E-17
System Rule: Inactive CS-MARS Reporting Device	E-17
System Rule: Connectivity Issue: IOS IPS DTM	E-17
System Rule: CS-MARS Database Partition Usage	E-18

System Rule: CS-MARS Failure Saving Certificates/Fingerprints	E-18
System Rule: CS-MARS IPS Signature Update Failure	E-18
System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch	E-18
System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue	E-18
System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions	E-18
System Rule: Operational Issue: WLAN	E-18
System Rule: Rogue WLAN AP Detected	E-18
System: Reconnaissance	E-19
System Rule: Scans: SCADA Modbus	E-19
System Rule: Scans: Stealth	E-19
System Rule: Scans: Targeted	E-19
System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter	E-19
System: Resource Issue	E-19
System Rule: Resource Issue: Host	E-20
System Rule: Resource Issue: Network Device	E-20
System Rule: Resource Issue: IOS IPS DTM	E-20
System Rule: Resource Issue: CS-MARS	E-20
System: Restricted Network Traffic	E-20
System Rule: Network Activity: Excessive IRC	E-20
System Rule: Network Activity: Chat/IM - File Transfer	E-20
System Rule: Network Activity: P2P File Sharing - File Transfer	E-21
System Rule: Network Activity: Chat/IM - Active	E-21
System Rule: Network Activity: P2P File Sharing - Active	E-21
System Rule: Network Activity: Recreational	E-21
System Rule: Network Activity: Uncommon Traffic	E-21
System: Security Posture Compliance (Cisco NAC)	E-21
System Rule: Vulnerable Host Found	E-22
System Rule: Security Posture: Audit Server Issue - Network wide	E-22
System Rule: Security Posture: Audit Server Issue - Single Host	E-22
System Rule: Security Posture: Infected - Network wide	E-22
System Rule: Security Posture: Infected - Single Host	E-22
System Rule: Security Posture: Excessive NAC Status Query Failures - Network wide	E-22
System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host	E-23
System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD	E-23
System Rule: Security Posture: Quarantined - Network wide	E-23
System Rule: Security Posture: Quarantined - Single Host	E-23
System: Server Exploits	E-23
System Rule: Local Attack - Attempt	E-24
System Rule: Server Attack: Sniffer - Attempt	E-24
System Rule: Server Attack: Sniffer - Success Likely	E-24

System Rule: Local Attack - Success Likely	E-24
System Rule: Server Attack: SCADA Modbus - Attempt	E-24
System Rule: Misc. Attacks: Application Admin Escalation	E-25
System Rule: Misc. Attacks: Evasion	E-25
System Rule: Misc. Attacks: TCP/IP Protocol Anomaly	E-25
System Rule: Misc. Attacks: Replay	E-25
System Rule: Server Attack: Database - Attempt	E-25
System Rule: Server Attack: DNS - Attempt	E-25
System Rule: Server Attack: FTP - Attempt	E-25
System Rule: Server Attack: Login - Attempt	E-25
System Rule: Server Attack: Mail - Attempt	E-26
System Rule: Server Attack: Misc. - Attempt	E-26
System Rule: Server Attack: RPC - Attempt	E-26
System Rule: Server Attack: SNMP - Attempt	E-26
System Rule: Server Attack: Web - Attempt	E-26
System Rule: Misc. Attacks: Access Web Customer Data	E-26
System Rule: Server Attack: Database - Success Likely	E-26
System Rule: Server Attack: DNS - Success Likely	E-27
System Rule: Server Attack: FTP - Success Likely	E-27
System Rule: Server Attack: Login - Success Likely	E-27
System Rule: Server Attack: Mail - Success Likely	E-27
System Rule: Server Attack: Misc. - Success Likely	E-27
System Rule: Server Attack: RPC - Success Likely	E-27
System Rule: Server Attack: SNMP - Success Likely	E-28
System Rule: Server Attack: Web - Success Likely	E-28
System Reports by Category	E-28
System: ASA Botnet Traffic Filter	E-29
Activity: ASA Botnet Traffic Filter: Phone Home - All Events	E-30
Activity: ASA Botnet Traffic Filter - Top Botnet Sites	E-30
Activity: ASA Botnet Traffic Filter - Top Botnet Ports	E-30
Activity: ASA Botnet Traffic Filter - Top Infected Hosts	E-30
Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events	E-30
System: Access	E-30
Attacks: Password - Top Event Types	E-31
Activity: Host Login Failures - Top Destinations	E-31
Activity: Host Login Failures - Top Users	E-31
Activity: Host Login Success - Top Host	E-31
Attacks: Password - Top Destinations	E-31
Activity: Host Privilege Escalation - Top Hosts	E-31
Activity: Remote Access Login - Top User	E-31

Activity: Database Login Failures - All Events	E-32
Activity: Database Login Failures - Top Servers	E-32
Activity: Database Login Successes - Top Servers	E-32
Activity: Database Login Successes - Top Users	E-32
Activity: Host Login Failures - All Events	E-32
Activity: Host Login Success - All Events	E-32
Activity: Host Privilege Escalation - All Events	E-32
Activity: Remote Access Login - All Events	E-32
Activity: Remote Access Login Failures - All Events	E-32
Activity: AAA Based Access Failure - All Events	E-32
Activity: Accounts Locked - All Events	E-32
Activity: Accounts Locked - Top Hosts	E-33
Attacks: Password: Locked Accounts - All Events	E-33
Attacks: Password: Restricted Times - All Events	E-33
Activity: AAA Based Access - All Events	E-33
Activity: Database Login Failures - Top Users	E-33
Activity: Database Login Successes - All Events	E-33
Activity: CS-MARS Login Failures	E-33
System: All Events - Aggregate View	E-33
Activity: All - Top Destination Ports	E-34
Activity: All - Top Destinations	E-34
Activity: All - Top Event Type Groups	E-34
Activity: All - Top Event Types	E-34
Activity: All - Top Reporting Devices	E-34
Activity: All - Top Sources	E-34
Activity: All - Top Users	E-34
Activity: All - NAT Connections	E-34
Activity: All - Top Reporting Device Types	E-34
Activity: All Sessions - Top Destinations by Bytes	E-34
Detailed NAC Report	E-35
System: All Exploits - Aggregate View	E-35
Activity: Attacks Prevented - Top Reporting Devices	E-35
Activity: Attacks Seen - Top Reporting Devices	E-35
Attacks: All - Top Sources	E-35
Attacks: All - Top Event Type Groups	E-35
Attacks: All - All Events	E-35
Activity: Attacks Seen - Top Event Types	E-35
Attacks: All - Top Destinations	E-36
Activity: Attacks Prevented by Cisco IPS - All Events	E-36
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-36

System: COBIT DS3.3 - Monitoring and Reporting	E-36
Operational Issues: Network - Top Reporting Devices	E-36
Operational Issues: Server - Top Reporting Devices	E-36
Resource Issues: Network - Top Reporting Devices	E-37
Resource Issues: Server - Top Reporting Devices	E-37
Resource Utilization: Bandwidth: Inbound - Top Interfaces	E-37
Resource Utilization: CPU - Top Devices	E-37
Resource Utilization: Bandwidth: Outbound - Top Interfaces	E-37
Resource Utilization: Concurrent Connections - Top Devices	E-37
Resource Utilization: Errors: Inbound - Top Interfaces	E-37
Resource Utilization: Errors: Outbound - Top Interfaces	E-37
Resource Utilization: Memory - Top Devices	E-37
Activity: Sudden Traffic Increase To Port - All Destinations	E-37
Activity: Sudden Traffic Increase To Port - All Sources	E-38
Operational Issues: Network - All Events	E-38
Operational Issues: Server - All Events	E-38
Resource Issues: Network - All Events	E-38
Resource Issues: Server - All Events	E-38
System: COBIT DS5.10: Security Violations	E-38
Activity: IDS Evasion - Top Event Types	E-39
Activity: Scans - Top Destination Ports	E-39
Activity: Scans - Top Destinations	E-39
Activity: Stealth Scans - Top Sources	E-39
Attacks: Database Server - Top Event Types	E-39
Attacks: FTP Server - Top Event Types	E-39
Attacks: Identity Spoofing - Top Event Types	E-39
Attacks: Login Services - Top Event Types	E-40
Attacks: Mail Server - Top Event Types	E-40
Attacks: Network DoS - Top Event Types	E-40
Attacks: RPC Services - Top Event Types	E-40
Attacks: SNMP - Top Event Types	E-40
Attacks: Web Server/App - Top Event Types	E-40
Attacks: All - Top Event Type Groups	E-40
Attacks: All - All Events	E-40
Attacks: Uncommon or Anomalous Traffic - Top Event Types	E-40
Activity: Database Privileged Command Failures - All Events	E-40
Activity: Database User/Group Change Failures - All Events	E-41
Activity: Host Login Failures - All Events	E-41
Activity: Remote Access Login Failures - All Events	E-41
Activity: Sudden Traffic Increase To Port - All Destinations	E-41

Activity: Sudden Traffic Increase To Port - All Sources	E-41
Attacks: Password - All Events	E-41
Activity: Security Posture: Not Healthy - All Events	E-41
System: COBIT DS5.19: Malicious software	E-41
Activity: Backdoor - Top Event Types	E-42
Activity: Virus/Worms - Top Event Types	E-42
Attacks: Virus/Worms - Top Sources	E-42
Activity: Backdoor - Top Destinations	E-42
Activity: Backdoor - Top Hosts	E-42
Activity: Spyware - Top Hosts	E-42
Activity: Virus/Worms - Top Infected Hosts	E-42
Activity: Virus: Detected - Top Users	E-42
Activity: Virus: Infections - Top Users	E-42
System: COBIT DS5.20: Firewall control	E-42
Activity: Attacks Prevented - Top Reporting Devices	E-43
Activity: Denies - Top Destination Ports	E-43
Activity: Denies - Top Destinations	E-43
Activity: Web Usage - Top Sources	E-43
Activity: Network Usage - Top Destination Ports	E-43
Activity: Web Usage - Top Destinations by Bytes	E-43
Activity: Web Usage - Top Destinations by Sessions	E-43
Resource Utilization: Concurrent Connections - Top Devices	E-44
Activity: Network Usage - Top Destination Ports By Bytes	E-44
Activity: Attacks Prevented by Cisco IPS - All Events	E-44
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-44
System: COBIT DS5.2: Authentication and Access	E-44
Activity: Host Login Success - Top Host	E-44
Activity: Host Privilege Escalation - Top Hosts	E-45
Activity: Remote Access Login - Top User	E-45
Activity: Host Login Success - All Events	E-45
Activity: Host Admin Login Success - All Events	E-45
Activity: Host Privilege Escalation - All Events	E-45
Activity: Remote Access Login - All Events	E-45
Activity: AAA Based Access Failure - All Events	E-45
Activity: Accounts Locked - All Events	E-45
Activity: Accounts Locked - Top Hosts	E-45
Attacks: Password: Locked Accounts - All Events	E-45
Attacks: Password: Restricted Times - All Events	E-46
Activity: AAA Based Access - All Events	E-46
Activity: Database Login Successes - All Events	E-46

Activity: CS-MARS Login Failures	E-46
System: COBIT DS5.4: User Account Changes	E-46
Activity: Host User/Group Management - All Events	E-46
Activity: Host User/Group Management - Top hosts	E-46
Activity: Database User/Group Change Successes - All Events	E-46
Activity: Database User/Group Change Successes - Top Users	E-46
System: COBIT DS5.7: Security Surveillance	E-46
Activity: All - Top Event Types	E-47
Activity: All - Top Reporting Devices	E-47
Activity: Attacks Seen - Top Reporting Devices	E-47
Activity: All - Top Reporting Device Types	E-47
Activity: Inactive Reporting Device - Top Devices	E-47
System: COBIT DS9.4: Configuration Control	E-47
Activity: Host Registry Changes - All Events	E-47
Activity: Database Object Modification Successes - All Events	E-48
Configuration Changes: Network - All Events	E-48
Configuration Changes: Server - All Events	E-48
Activity: Host Security Policy Changes - All Events	E-48
System: COBIT DS9.5: Unauthorized Software	E-48
Activity: IRC - All Events	E-48
Activity: Recreational - All Events	E-48
Activity: Spyware - All Events	E-48
Activity: P2P Filesharing/Chat - All Events	E-48
Activity: Uncommon or Anomalous Traffic - All Events	E-49
System: CS-MARS Distributed Threat Mitigation (Cisco DTM)	E-49
Activity: IOS IPS DTM Successful Signature Tuning - All Events	E-49
Connectivity Issue: IOS IPS DTM - All Events	E-49
Resource Issues: IOS IPS DTM - Top Devices	E-49
Resource Issues: IOS IPS DTM - All Events	E-49
System: CS-MARS Incident Response	E-49
Activity: CS-MARS Host Mitigation - Failure - All Events	E-50
Activity: CS-MARS Host Mitigation - Success - All Events	E-50
Activity: IOS IPS DTM Successful Signature Tuning - All Events	E-50
Activity: WLAN Successful Mitigations	E-50
System: CS-MARS Issue	E-50
Activity: Unknown Events - All Events	E-51
Resource Issues: CS-MARS - All Events	E-51
Resource Utilization: CS-MARS - All Events	E-51
Activity: CS-MARS Accepted New Certificates/Fingerprints	E-51
Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints	E-51

Activity: CS-MARS Detected Conflicting Certificates/Fingerprints	E-51
Activity: CS-MARS Failure Saving Certificates/Fingerprints	E-51
Activity: CS-MARS Device Connectivity Errors	E-51
Activity: CS-MARS Authentication Method Modifications	E-51
Activity: CS-MARS pnaadmin User Password Status	E-52
Activity: CS-MARS Accounts Locked	E-52
Activity: CS-MARS IPS Signature Update Success - All Events	E-52
Activity: CS-MARS Successful Logins	E-52
Activity: CS-MARS IPS Signature Update Failure - All Events	E-52
Activity: CS-MARS Login Failures	E-52
Activity: CS-MARS LC-GC Communication Recovered	E-52
Activity: CS-MARS Accounts Unlocked	E-52
Activity: CS-MARS LC-GC Communication Failures	E-52
System: Client Exploits, Virus, Worm and Malware	E-53
Activity: Backdoor - Top Event Types	E-53
Activity: Virus/Worms - Top Event Types	E-53
Attacks: Virus/Worms - Top Sources	E-53
Activity: Backdoor - Top Destinations	E-54
Activity: Backdoor - Top Hosts	E-54
Attacks: Client Exploits - Top Sources	E-54
Activity: Virus/Worms - Top Infected Hosts	E-54
Activity: Virus: Detected - Top Users	E-54
Activity: Virus: Infections - Top Users	E-54
Activity: New Malware Discovered - All Events	E-54
Activity: New Malware Prevention Deployment Failure - All Events	E-54
Activity: New Malware Prevention Deployment Success - All Events	E-54
Activity: New Malware Traffic Match - All Events	E-54
Activity: New Malware Traffic Match - Top Sources	E-55
Activity: Sudden Traffic Increase To Port - All Destinations	E-55
Activity: Sudden Traffic Increase To Port - All Sources	E-55
Activity: ASA Botnet Traffic Filter: Phone Home - All Events	E-55
Activity: ASA Botnet Traffic Filter - Top Botnet Sites	E-55
Activity: ASA Botnet Traffic Filter - Top Botnet Ports	E-55
Activity: ASA Botnet Traffic Filter - Top Infected Hosts	E-55
Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events	E-55
System: Configuration Changes	E-55
Configuration Changes: Network - Top Event Types	E-56
Configuration Changes: Server - Top Event Types	E-56
Configuration Changes: Server - Top Reporting Devices	E-56
Configuration Changes: Network - All Events	E-56

Configuration Changes: Server - All Events	E-56
System: Configuration Issue	E-56
Configuration Issues: Network - Top Reporting Devices	E-56
Configuration Issues: Server - Top Reporting Devices	E-56
Configuration Issues: Network - All Events	E-57
Configuration Issues: Server - All Events	E-57
System: Database Server Activity	E-57
Activity: Database Object Modification Failures - All Events	E-57
Activity: Database Object Modification Failures - Top Users	E-57
Activity: Database Object Modification Successes - All Events	E-57
Activity: Database Object Modification Successes - Top Users	E-58
Activity: Database Privileged Command Failures - All Events	E-58
Activity: Database Privileged Command Failures - Top Users	E-58
Activity: Database Privileged Command Successes - All Events	E-58
Activity: Database Privileged Command Successes - Top Users	E-58
Activity: Database Regular Command Failures - All Events	E-58
Activity: Database Regular Command Failures - Top Users	E-58
Activity: Database Regular Command Successes - All Events	E-58
Activity: Database Regular Command Successes - Top Users	E-58
Activity: Database User/Group Change Failures - All Events	E-58
Activity: Database User/Group Change Failures - Top Users	E-58
Activity: Database User/Group Change Successes - All Events	E-58
Activity: Database User/Group Change Successes - Top Users	E-59
System: FISMA Compliance Reports	E-59
Activity: All - Top Reporting Devices	E-61
Activity: Attacks Prevented - Top Reporting Devices	E-61
Activity: Denies - Top Destination Ports	E-61
Activity: Denies - Top Destinations	E-62
Activity: Denies - Top Sources	E-62
Activity: IDS Evasion - Top Event Types	E-62
Activity: P2P Filesharing/Chat - Top Event Types	E-62
Activity: Scans - Top Destination Ports	E-62
Activity: Scans - Top Destinations	E-62
Activity: Stealth Scans - Top Sources	E-62
Activity: Virus/Worms - Top Event Types	E-62
Activity: All - Top Rules Fired	E-62
Attacks: All - Top Sources	E-63
Attacks: Database Server - Top Event Types	E-63
Attacks: FTP Server - Top Event Types	E-63
Attacks: Identity Spoofing - Top Event Types	E-63

Attacks: Login Services - Top Event Types	E-63
Attacks: Mail Server - Top Event Types	E-63
Attacks: Network DoS - Top Event Types	E-63
Attacks: RPC Services - Top Event Types	E-63
Attacks: Virus/Worms - Top Sources	E-63
Attacks: Web Server/App - Top Event Types	E-63
Configuration Changes: Network - Top Event Types	E-63
Activity: All - Top Users	E-64
Activity: IRC - All Events	E-64
Attacks: All - Top Event Type Groups	E-64
Activity: All - Top Reporting Device Types	E-64
Activity: Host Login Failures - Top Destinations	E-64
Activity: Host Login Failures - Top Users	E-64
Activity: Host Login Success - Top Host	E-64
Activity: Host Registry Changes - All Events	E-64
Activity: Host Registry Changes - Top Host	E-64
Activity: Host Security Policy Changes - Top Host	E-64
Attacks: All - Top Destinations	E-64
Activity: Host User/Group Management - All Events	E-65
Activity: Host User/Group Management - Top hosts	E-65
Activity: Network Usage - Top Destination Ports	E-65
Attacks: Password - Top Destinations	E-65
Attacks: Uncommon or Anomalous Traffic - Top Event Types	E-65
Configuration Changes: Server - Top Event Types	E-65
Activity: Spyware - Top Hosts	E-65
Configuration Changes: Server - Top Reporting Devices	E-65
Activity: All Events and Netflow - Top Destination Ports	E-65
Activity: Host Privilege Escalation - Top Hosts	E-66
Activity: P2P Filesharing/Chat - Top Hosts	E-66
Activity: Recreational - Top Sources	E-66
Activity: Remote Access Login - Top User	E-66
Activity: Virus/Worms - Top Infected Hosts	E-66
Activity: Database Login Failures - All Events	E-66
Activity: Database Login Failures - Top Servers	E-66
Activity: Database Login Successes - Top Servers	E-66
Activity: Database Login Successes - Top Users	E-66
Activity: Database Object Modification Failures - All Events	E-66
Activity: Database Object Modification Failures - Top Users	E-66
Activity: Database Object Modification Successes - All Events	E-67
Activity: Database Object Modification Successes - Top Users	E-67

Activity: Database Privileged Command Failures - All Events	E-67
Activity: Virus: Detected - Top Users	E-67
Activity: Database Privileged Command Failures - Top Users	E-67
Activity: Virus: Infections - Top Users	E-67
Activity: Database Regular Command Failures - All Events	E-67
Activity: Database Regular Command Failures - Top Users	E-67
Activity: Database User/Group Change Failures - All Events	E-67
Activity: Database User/Group Change Failures - Top Users	E-67
Activity: Database User/Group Change Successes - All Events	E-67
Activity: Database User/Group Change Successes - Top Users	E-67
Resource Utilization: Concurrent Connections - Top Devices	E-68
Activity: Host Login Failures - All Events	E-68
Activity: Host Login Success - All Events	E-68
Activity: CS-MARS Host Mitigation - Failure - All Events	E-68
Activity: CS-MARS Host Mitigation - Success - All Events	E-68
Activity: Host Admin Login Success - All Events	E-68
Activity: Host Privilege Escalation - All Events	E-68
Activity: Network Usage - Top Destination Ports By Bytes	E-68
Activity: Remote Access Login - All Events	E-68
Activity: Remote Access Login Failures - All Events	E-68
Activity: Vulnerable Host Found via VA Scanner	E-69
Activity: Vulnerable Host Found	E-69
Attacks: Password - All Events	E-69
Configuration Changes: Network - All Events	E-69
Configuration Changes: Server - All Events	E-69
Activity: Host Security Policy Changes - All Events	E-69
Activity: AAA Based Access Failure - All Events	E-69
Activity: Database Login Failures - Top Users	E-69
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-69
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-69
Activity: Security Posture: Not Healthy - All Events	E-70
Activity: AAA Failed Auth - All Events	E-70
Activity: AAA Failed Auth - Top Users	E-70
Activity: Attacks Prevented by Cisco IPS - All Events	E-70
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-70
Activity: CS-MARS padmin User Password Status	E-70
Activity: CS-MARS Successful Logins	E-70
System: GLBA Compliance Reports	E-70
Activity: All - Top Reporting Devices	E-72
Activity: Attacks Prevented - Top Reporting Devices	E-73

Activity: Denies - Top Destination Ports	E-73
Activity: Denies - Top Destinations	E-73
Activity: Denies - Top Sources	E-73
Activity: IDS Evasion - Top Event Types	E-73
Activity: Scans - Top Destination Ports	E-73
Activity: Scans - Top Destinations	E-73
Activity: Stealth Scans - Top Sources	E-73
Activity: All - Top Rules Fired	E-73
Attacks: All - Top Sources	E-73
Attacks: Database Server - Top Event Types	E-74
Attacks: FTP Server - Top Event Types	E-74
Attacks: Identity Spoofing - Top Event Types	E-74
Attacks: Login Services - Top Event Types	E-74
Attacks: Mail Server - Top Event Types	E-74
Attacks: Network DoS - Top Event Types	E-74
Attacks: RPC Services - Top Event Types	E-74
Attacks: Web Server/App - Top Event Types	E-74
Configuration Changes: Network - Top Event Types	E-74
Configuration Issues: Network - Top Reporting Devices	E-74
Configuration Issues: Server - Top Reporting Devices	E-75
Activity: IRC - All Events	E-75
Activity: All - Top Reporting Device Types	E-75
Activity: Host Login Failures - Top Destinations	E-75
Activity: Host Login Failures - Top Users	E-75
Activity: Host Registry Changes - All Events	E-75
Activity: Host Registry Changes - Top Host	E-75
Activity: Host Security Policy Changes - Top Host	E-75
Attacks: All - Top Destinations	E-75
Activity: Network Usage - Top Destination Ports	E-75
Attacks: Password - Top Destinations	E-76
Configuration Changes: Server - Top Event Types	E-76
Activity: Spyware - Top Hosts	E-76
Configuration Changes: Server - Top Reporting Devices	E-76
Activity: All Events and Netflow - Top Destination Ports	E-76
Activity: Host Privilege Escalation - Top Hosts	E-76
Activity: P2P Filesharing/Chat - Top Hosts	E-76
Activity: Database Login Failures - All Events	E-76
Activity: Database Object Modification Failures - All Events	E-76
Activity: Database Object Modification Failures - Top Users	E-76
Activity: Database Object Modification Successes - All Events	E-77

Activity: Database Object Modification Successes - Top Users	E-77
Activity: Database Privileged Command Failures - All Events	E-77
Activity: Database Privileged Command Failures - Top Users	E-77
Activity: Database Privileged Command Successes - All Events	E-77
Activity: Database Privileged Command Successes - Top Users	E-77
Activity: Database Regular Command Failures - All Events	E-77
Activity: Database Regular Command Failures - Top Users	E-77
Activity: Database Regular Command Successes - All Events	E-77
Activity: Database Regular Command Successes - Top Users	E-77
Activity: Database User/Group Change Failures - All Events	E-77
Activity: Database User/Group Change Failures - Top Users	E-77
Activity: Database User/Group Change Successes - All Events	E-78
Activity: Database User/Group Change Successes - Top Users	E-78
Resource Utilization: Concurrent Connections - Top Devices	E-78
Activity: Host Login Failures - All Events	E-78
Activity: Spyware - All Events	E-78
Activity: Host Privilege Escalation - All Events	E-78
Activity: Network Usage - Top Destination Ports By Bytes	E-78
Activity: Remote Access Login Failures - All Events	E-78
Activity: Vulnerable Host Found via VA Scanner	E-78
Activity: Vulnerable Host Found	E-78
Attacks: Password - All Events	E-78
Configuration Changes: Network - All Events	E-79
Configuration Changes: Server - All Events	E-79
Configuration Issues: Network - All Events	E-79
Configuration Issues: Server - All Events	E-79
Activity: Host Security Policy Changes - All Events	E-79
Activity: AAA Based Access Failure - All Events	E-79
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-79
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-79
Activity: Security Posture: Not Healthy - All Events	E-79
Activity: AAA Failed Auth - All Events	E-80
Activity: Attacks Prevented by Cisco IPS - All Events	E-80
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-80
System: HIPAA Compliance Reports	E-80
Activity: All - Top Reporting Devices	E-82
Activity: Attacks Prevented - Top Reporting Devices	E-83
Activity: Denies - Top Destination Ports	E-83
Activity: Denies - Top Destinations	E-83
Activity: Denies - Top Sources	E-83

Activity: IDS Evasion - Top Event Types	E-83
Activity: P2P Filesharing/Chat - Top Event Types	E-83
Activity: Scans - Top Destination Ports	E-83
Activity: Scans - Top Destinations	E-83
Activity: Stealth Scans - Top Sources	E-83
Activity: Virus/Worms - Top Event Types	E-83
Activity: All - Top Rules Fired	E-84
Attacks: All - Top Sources	E-84
Attacks: Database Server - Top Event Types	E-84
Attacks: FTP Server - Top Event Types	E-84
Attacks: Identity Spoofing - Top Event Types	E-84
Attacks: Login Services - Top Event Types	E-84
Attacks: Mail Server - Top Event Types	E-84
Attacks: Network DoS - Top Event Types	E-84
Attacks: RPC Services - Top Event Types	E-84
Attacks: Virus/Worms - Top Sources	E-84
Attacks: Web Server/App - Top Event Types	E-85
Configuration Changes: Network - Top Event Types	E-85
Activity: All - Top Users	E-85
Activity: IRC - All Events	E-85
Attacks: All - Top Event Type Groups	E-85
Activity: All - Top Reporting Device Types	E-85
Activity: Host Login Failures - Top Destinations	E-85
Activity: Host Login Failures - Top Users	E-85
Activity: Host Login Success - Top Host	E-85
Activity: Host Registry Changes - All Events	E-85
Activity: Host Registry Changes - Top Host	E-85
Activity: Host Security Policy Changes - Top Host	E-86
Attacks: All - Top Destinations	E-86
Activity: Host User/Group Management - All Events	E-86
Activity: Host User/Group Management - Top hosts	E-86
Activity: Network Usage - Top Destination Ports	E-86
Attacks: Password - Top Destinations	E-86
Attacks: Uncommon or Anomalous Traffic - Top Event Types	E-86
Configuration Changes: Server - Top Event Types	E-86
Activity: Spyware - Top Hosts	E-86
Configuration Changes: Server - Top Reporting Devices	E-86
Activity: All Events and Netflow - Top Destination Ports	E-87
Activity: Host Privilege Escalation - Top Hosts	E-87
Activity: P2P Filesharing/Chat - Top Hosts	E-87

Activity: Recreational - Top Sources	E-87
Activity: Remote Access Login - Top User	E-87
Activity: Virus/Worms - Top Infected Hosts	E-87
Activity: Database Login Failures - All Events	E-87
Activity: Database Login Failures - Top Servers	E-87
Activity: Database Login Successes - Top Servers	E-87
Activity: Database Login Successes - Top Users	E-87
Activity: Database Object Modification Failures - All Events	E-88
Activity: Database Object Modification Failures - Top Users	E-88
Activity: Database Object Modification Successes - All Events	E-88
Activity: Database Object Modification Successes - Top Users	E-88
Activity: Database Privileged Command Failures - All Events	E-88
Activity: Virus: Detected - Top Users	E-88
Activity: Database Privileged Command Failures - Top Users	E-88
Activity: Virus: Infections - Top Users	E-88
Activity: Database Regular Command Failures - All Events	E-88
Activity: Database Regular Command Failures - Top Users	E-88
Activity: Database User/Group Change Failures - All Events	E-88
Activity: Database User/Group Change Failures - Top Users	E-88
Activity: Database User/Group Change Successes - All Events	E-89
Activity: Database User/Group Change Successes - Top Users	E-89
Resource Utilization: Concurrent Connections - Top Devices	E-89
Activity: Host Login Failures - All Events	E-89
Activity: Host Login Success - All Events	E-89
Activity: CS-MARS Host Mitigation - Failure - All Events	E-89
Activity: CS-MARS Host Mitigation - Success - All Events	E-89
Activity: Host Admin Login Success - All Events	E-89
Activity: Host Privilege Escalation - All Events	E-89
Activity: Remote Access Login - All Events	E-89
Activity: Remote Access Login Failures - All Events	E-89
Activity: Vulnerable Host Found via VA Scanner	E-90
Activity: Vulnerable Host Found	E-90
Attacks: Password - All Events	E-90
Configuration Changes: Network - All Events	E-90
Configuration Changes: Server - All Events	E-90
Activity: Host Security Policy Changes - All Events	E-90
Activity: AAA Based Access Failure - All Events	E-90
Activity: Database Login Failures - Top Users	E-90
Activity: Database Login Successes - All Events	E-90
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-90

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-91
Activity: Security Posture: Not Healthy - All Events	E-91
Activity: AAA Failed Auth - All Events	E-91
Activity: AAA Failed Auth - Top Users	E-91
Activity: Attacks Prevented by Cisco IPS - All Events	E-91
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-91
Activity: CS-MARS padmin User Password Status	E-91
Activity: CS-MARS Successful Logins	E-91
Activity: CS-MARS Login Failures	E-91
System: Host Activity	E-92
Activity: Host Object Access - All Events	E-92
Activity: Host Privileged Access - All Events	E-92
Activity: Host Registry Changes - All Events	E-92
Activity: Host Registry Changes - Top Host	E-92
Activity: Host Security Policy Changes - Top Host	E-92
Activity: Host System Events - All Events	E-92
Activity: Host User/Group Management - All Events	E-92
Activity: Host User/Group Management - Top hosts	E-93
Activity: Host Process Tracking - All Events	E-93
System: Network Attacks and DoS	E-93
Attacks: Network DoS - Top Event Types	E-93
Activity: Sudden Traffic Increase To Port - All Destinations	E-93
Activity: Sudden Traffic Increase To Port - All Sources	E-93
Activity: WLAN DoS Attacks Detected	E-93
Activity: WLAN Probes Detected	E-93
Activity: WLAN Rogue AP or Adhoc Hosts Detected	E-94
System: New Malware Outbreak (Cisco ICS)	E-94
Activity: New Malware Discovered - All Events	E-94
Activity: New Malware Prevention Deployment Failure - All Events	E-94
Activity: New Malware Prevention Deployment Success - All Events	E-94
Activity: New Malware Traffic Match - All Events	E-94
Activity: New Malware Traffic Match - Top Sources	E-94
System: Operational Issue	E-94
Operational Issues: Network - Top Reporting Devices	E-95
Operational Issues: Server - Top Reporting Devices	E-95
Resource Utilization: Errors: Inbound - Top Interfaces	E-95
Resource Utilization: Errors: Outbound - Top Interfaces	E-95
Activity: Inactive Reporting Device - Top Devices	E-95
Operational Issues: Network - All Events	E-95
Operational Issues: Server - All Events	E-95

Connectivity Issue: IOS IPS DTM - All Events	E-96
Resource Utilization: CS-MARS - All Events	E-96
Activity: CS-MARS Failure Saving Certificates/Fingerprints	E-96
Activity: CS-MARS Device Connectivity Errors	E-96
Activity: CS-MARS IPS Signature Update Failure - All Events	E-96
Activity: CS-MARS LC-GC Communication Failures	E-96
System: PCI DSS01: Install, Maintain FW, Protect Cardholder Data	E-96
Activity: All - Top Destination Ports	E-97
Activity: P2P Filesharing/Chat - Top Event Types	E-97
Attacks: Login Services - Top Event Types	E-97
Configuration Changes: Network - Top Event Types	E-98
Activity: Network Usage - Top Destination Ports	E-98
Configuration Changes: Server - Top Event Types	E-98
Configuration Changes: Server - Top Reporting Devices	E-98
Activity: All Sessions - Top Destination Ports by Bytes	E-98
Activity: P2P Filesharing/Chat - Top Hosts	E-98
Activity: Network Usage - Top Destination Ports By Bytes	E-98
Configuration Changes: Network - All Events	E-98
Configuration Changes: Server - All Events	E-98
Activity: Security Posture: Healthy - Top Users	E-98
Activity: Security Posture: NAC - Top NADs	E-99
Activity: Security Posture: NAC - Top Tokens	E-99
Activity: Security Posture: NAC L2IP - Top Tokens	E-99
Activity: Security Posture: NAC Audit Server Issues - All Events	E-99
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-99
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-99
Activity: Security Posture: NAC L2 802.1x - Top Tokens	E-99
Activity: Security Posture: NAC Static Auth - Top Hosts	E-99
Activity: Security Posture: NAC Static Auth - Top NADs	E-100
Activity: Security Posture: NAC Status Query Failure - Top Hosts	E-100
Activity: Security Posture: Not Healthy - All Events	E-100
Activity: Security Posture: NAC - Top NADs and Tokens	E-100
Activity: Security Posture: NAC Agentless - Top Tokens	E-100
Activity: Security Posture: NAC End Host Details - All Events	E-100
Activity: AAA Failed Auth - All Events	E-100
Activity: AAA Failed Auth - Top NADs	E-100
Activity: AAA Failed Auth - Top Users	E-101
Activity: Security Posture: NAC Agentless - Top Hosts	E-101
Activity: Security Posture: NAC Agentless - Top NADs	E-101
System: PCI DSS02: Do Not Use Default PWD & Security Parameters	E-101

Activity: All - Top Destination Ports	E-102
Activity: P2P Filesharing/Chat - Top Event Types	E-102
Attacks: Login Services - Top Event Types	E-102
Configuration Changes: Network - Top Event Types	E-102
Activity: Host Object Access - All Events	E-102
Activity: Host Privileged Access - All Events	E-102
Activity: Host Registry Changes - All Events	E-102
Activity: Host Registry Changes - Top Host	E-102
Activity: Host Security Policy Changes - Top Host	E-102
Activity: Host System Events - All Events	E-103
Activity: Host User/Group Management - All Events	E-103
Activity: Host User/Group Management - Top hosts	E-103
Activity: Network Usage - Top Destination Ports	E-103
Configuration Changes: Server - Top Reporting Devices	E-103
Activity: P2P Filesharing/Chat - Top Hosts	E-103
Activity: Network Usage - Top Destination Ports By Bytes	E-103
Activity: P2P Filesharing/Chat - All Events	E-103
Configuration Changes: Network - All Events	E-103
Activity: Host Process Tracking - All Events	E-103
System: PCI DSS03: Protect Store Cardholder Data	E-103
Attacks: SNMP - Top Event Types	E-104
Attacks: Web Server/App - Top Event Types	E-104
Activity: Host Registry Changes - All Events	E-104
Activity: Host Registry Changes - Top Host	E-104
Activity: Host Security Policy Changes - Top Host	E-105
Activity: Database Login Failures - All Events	E-105
Activity: Database Login Failures - Top Servers	E-105
Activity: Database Login Successes - Top Servers	E-105
Activity: Database Login Successes - Top Users	E-105
Activity: Database Object Modification Failures - All Events	E-105
Activity: Database Object Modification Failures - Top Users	E-105
Activity: Database Object Modification Successes - All Events	E-105
Activity: Database Object Modification Successes - Top Users	E-105
Activity: Host Login Failures - All Events	E-105
Activity: Host Login Success - All Events	E-105
Activity: Host Privilege Escalation - All Events	E-106
Activity: Remote Access Login - All Events	E-106
Activity: Remote Access Login Failures - All Events	E-106
Activity: Host Security Policy Changes - All Events	E-106
Activity: Database Login Failures - Top Users	E-106

Activity: Database Login Successes - All Events	E-106
Activity: AAA Failed Auth - All Events	E-106
Activity: AAA Failed Auth - Top NADs	E-106
Activity: AAA Failed Auth - Top Users	E-106
System: PCI DSS04: Encrypt Transmission of Cardholder Data	E-107
Configuration Issues: Network - Top Reporting Devices	E-107
Operational Issues: Network - Top Reporting Devices	E-107
Activity: Remote Access Login - Top User	E-107
Activity: Remote Access Login - All Events	E-107
Activity: Remote Access Login Failures - All Events	E-107
Configuration Issues: Network - All Events	E-107
Operational Issues: Network - All Events	E-107
System: PCI DSS05: Use and Regularly Update Anti-Virus Software	E-108
Activity: Vulnerable Host Found via VA Scanner	E-108
Activity: Vulnerable Host Found	E-108
Activity: Security Posture: Healthy - Top Users	E-108
Activity: Security Posture: NAC - Top NADs	E-109
Activity: Security Posture: NAC - Top Tokens	E-109
Activity: Security Posture: NAC L2IP - Top Tokens	E-109
Activity: Security Posture: NAC Audit Server Issues - All Events	E-109
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-109
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-109
Activity: Security Posture: NAC L2 802.1x - Top Tokens	E-109
Activity: Security Posture: NAC Static Auth - Top Hosts	E-109
Activity: Security Posture: NAC Static Auth - Top NADs	E-110
Activity: Security Posture: NAC Status Query Failure - Top Hosts	E-110
Activity: Security Posture: Not Healthy - All Events	E-110
Activity: Security Posture: NAC - Top NADs and Tokens	E-110
Activity: Security Posture: NAC Agentless - Top Tokens	E-110
Activity: Security Posture: NAC End Host Details - All Events	E-110
Activity: AAA Failed Auth - All Events	E-110
Activity: AAA Failed Auth - Top NADs	E-110
Activity: AAA Failed Auth - Top Users	E-111
Activity: Security Posture: NAC Agentless - Top Hosts	E-111
Activity: Security Posture: NAC Agentless - Top NADs	E-111
System: PCI DSS06: Develop, Maintain Secured System/Application	E-111
Attacks: Web Server/App - Top Event Types	E-112
Activity: Host Registry Changes - Top Host	E-112
Activity: Host Security Policy Changes - Top Host	E-112
Activity: New Malware Discovered - All Events	E-112

Activity: New Malware Prevention Deployment Failure - All Events	E-112
Activity: New Malware Prevention Deployment Success - All Events	E-112
Activity: New Malware Traffic Match - All Events	E-113
Activity: New Malware Traffic Match - Top Sources	E-113
Activity: AAA Based Access Failure - All Events	E-113
Activity: Security Posture: Healthy - Top Users	E-113
Activity: AAA Based Access - All Events	E-113
Activity: Security Posture: NAC - Top NADs	E-113
Activity: Security Posture: NAC - Top Tokens	E-113
Activity: Security Posture: NAC L2IP - Top Tokens	E-113
Activity: Security Posture: NAC Audit Server Issues - All Events	E-113
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-114
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-114
Activity: Security Posture: NAC L2 802.1x - Top Tokens	E-114
Activity: Security Posture: NAC Static Auth - Top Hosts	E-114
Activity: Security Posture: NAC Static Auth - Top NADs	E-114
Activity: Security Posture: NAC Status Query Failure - Top Hosts	E-114
Activity: Security Posture: Not Healthy - All Events	E-114
Activity: Security Posture: NAC - Top NADs and Tokens	E-114
Activity: Security Posture: NAC Agentless - Top Tokens	E-115
Activity: Security Posture: NAC End Host Details - All Events	E-115
Activity: AAA Failed Auth - All Events	E-115
Activity: AAA Failed Auth - Top NADs	E-115
Activity: AAA Failed Auth - Top Users	E-115
Activity: Security Posture: NAC Agentless - Top Hosts	E-115
Activity: Security Posture: NAC Agentless - Top NADs	E-115
System: PCI DSS07: Restrict Access to Cardholder Data	E-116
Activity: Host Login Failures - Top Destinations	E-116
Activity: Host Login Failures - Top Users	E-116
Activity: Host Login Success - Top Host	E-116
Activity: Host Privilege Escalation - Top Hosts	E-117
Activity: Remote Access Login - Top User	E-117
Activity: Database Login Failures - All Events	E-117
Activity: Database Login Failures - Top Servers	E-117
Activity: Database Login Successes - Top Servers	E-117
Activity: Database Login Successes - Top Users	E-117
Activity: Host Login Failures - All Events	E-117
Activity: Host Login Success - All Events	E-117
Activity: Host Privilege Escalation - All Events	E-117
Activity: Remote Access Login - All Events	E-117

Activity: Remote Access Login Failures - All Events	E-117
Activity: AAA Based Access Failure - All Events	E-118
Activity: Accounts Locked - All Events	E-118
Activity: Accounts Locked - Top Hosts	E-118
Attacks: Password: Locked Accounts - All Events	E-118
Attacks: Password: Restricted Times - All Events	E-118
Activity: AAA Based Access - All Events	E-118
Activity: Database Login Failures - Top Users	E-118
Activity: Database Login Successes - All Events	E-118
System: PCI DSS08: Assign Unique ID to Person with Comp Access	E-118
Activity: Host Login Failures - Top Destinations	E-119
Activity: Host Login Failures - Top Users	E-119
Activity: Host Login Success - Top Host	E-119
Activity: Host Privilege Escalation - Top Hosts	E-119
Activity: Remote Access Login - Top User	E-119
Activity: Database Login Failures - All Events	E-119
Activity: Database Login Failures - Top Servers	E-120
Activity: Database Login Successes - Top Servers	E-120
Activity: Database Login Successes - Top Users	E-120
Activity: Host Login Failures - All Events	E-120
Activity: Host Login Success - All Events	E-120
Activity: Host Privilege Escalation - All Events	E-120
Activity: Remote Access Login - All Events	E-120
Activity: Remote Access Login Failures - All Events	E-120
Activity: AAA Based Access Failure - All Events	E-120
Activity: Accounts Locked - All Events	E-120
Activity: Accounts Locked - Top Hosts	E-120
Attacks: Password: Locked Accounts - All Events	E-121
Attacks: Password: Restricted Times - All Events	E-121
Activity: AAA Based Access - All Events	E-121
Activity: Database Login Failures - Top Users	E-121
Activity: Database Login Successes - All Events	E-121
System: PCI DSS09: Restrict Physical Access to Cardholder Data	E-121
Activity: Host Login Failures - Top Users	E-121
Activity: Host Login Success - Top Host	E-121
Activity: Host Login Success - All Events	E-121
Activity: AAA Based Access Failure - All Events	E-122
Activity: Accounts Locked - All Events	E-122
Activity: Accounts Locked - Top Hosts	E-122
Activity: AAA Based Access - All Events	E-122

System: PCI DSS10: Track, Monitor All Network Access, Card Data	E-122
Activity: Host Login Failures - Top Destinations	E-123
Activity: Host Login Failures - Top Users	E-123
Activity: Host Login Success - Top Host	E-123
Activity: Host Privilege Escalation - Top Hosts	E-123
Activity: Remote Access Login - Top User	E-123
Activity: Database Login Failures - All Events	E-123
Activity: Database Login Failures - Top Servers	E-123
Activity: Database Login Successes - Top Servers	E-123
Activity: Database Login Successes - Top Users	E-123
Activity: Host Login Failures - All Events	E-124
Activity: Host Login Success - All Events	E-124
Activity: Host Privilege Escalation - All Events	E-124
Activity: Remote Access Login - All Events	E-124
Activity: Remote Access Login Failures - All Events	E-124
Activity: AAA Based Access Failure - All Events	E-124
Activity: Accounts Locked - All Events	E-124
Activity: Accounts Locked - Top Hosts	E-124
Attacks: Password: Locked Accounts - All Events	E-124
Attacks: Password: Restricted Times - All Events	E-124
Activity: AAA Based Access - All Events	E-124
Activity: Database Login Failures - Top Users	E-125
Activity: Database Login Successes - All Events	E-125
Activity: WLAN DoS Attacks Detected	E-125
Activity: WLAN Probes Detected	E-125
Activity: WLAN Rogue AP or Adhoc Hosts Detected	E-125
System: PCI DSS11: Regularly Test Security Systems and Processes	E-125
Activity: Attacks Seen - Top Reporting Devices	E-126
Activity: Backdoor - Top Event Types	E-126
Activity: Denies - Top Destinations	E-126
Activity: Denies - Top Sources	E-126
Activity: IDS Evasion - Top Event Types	E-126
Activity: Virus/Worms - Top Event Types	E-126
Activity: Backdoor - Top Destinations	E-126
Activity: Attacks Seen - Top Event Types	E-126
Activity: Backdoor - Top Hosts	E-127
Activity: Spyware - Top Hosts	E-127
Activity: Host Privilege Escalation - Top Hosts	E-127
Activity: Virus/Worms - Top Infected Hosts	E-127
Activity: Virus: Detected - Top Users	E-127

Activity: Virus: Infections - Top Users	E-127
Activity: New Malware Traffic Match - Top Sources	E-127
Activity: Vulnerable Host Found via VA Scanner	E-127
Activity: Vulnerable Host Found	E-127
Activity: Attacks Prevented by Cisco IPS - All Events	E-127
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-128
Activity: CS-MARS IPS Signature Update Success - All Events	E-128
Activity: CS-MARS IPS Signature Update Failure - All Events	E-128
Activity: WLAN DoS Attacks Detected	E-128
Activity: WLAN Probes Detected	E-128
Activity: WLAN Rogue AP or Adhoc Hosts Detected	E-128
System: PCI DSS12: Maintain InfoSec Policy for All Personnel	E-128
Activity: Attacks Seen - Top Reporting Devices	E-129
Activity: Backdoor - Top Event Types	E-129
Activity: Denies - Top Destinations	E-129
Activity: Denies - Top Sources	E-129
Activity: IDS Evasion - Top Event Types	E-129
Activity: Virus/Worms - Top Event Types	E-129
Activity: Backdoor - Top Destinations	E-129
Activity: Attacks Seen - Top Event Types	E-130
Activity: Backdoor - Top Hosts	E-130
Activity: Spyware - Top Hosts	E-130
Activity: Host Privilege Escalation - Top Hosts	E-130
Activity: Virus/Worms - Top Infected Hosts	E-130
Activity: Virus: Detected - Top Users	E-130
Activity: Virus: Infections - Top Users	E-130
Activity: Attacks Prevented by Cisco IPS - All Events	E-130
Activity: Attacks Prevented by Cisco IPS - Top Event Types	E-130
Activity: CS-MARS IPS Signature Update Success - All Events	E-130
Activity: CS-MARS IPS Signature Update Failure - All Events	E-131
System: Reconnaissance	E-131
Activity: Denies - Top Destination Ports	E-131
Activity: Denies - Top Destinations	E-131
Activity: Denies - Top Sources	E-131
Activity: Scans - Top Destination Ports	E-131
Activity: Scans - Top Destinations	E-131
Activity: Scans - Top Sources	E-132
Activity: Stealth Scans - Top Sources	E-132
Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events	E-132
System: Resource Issue	E-132

Resource Issues: Network - Top Reporting Devices	E-132
Resource Issues: Server - Top Reporting Devices	E-132
Resource Issues: Network - All Events	E-132
Resource Issues: Server - All Events	E-133
Resource Issues: IOS IPS DTM - Top Devices	E-133
Resource Issues: IOS IPS DTM - All Events	E-133
Resource Issues: CS-MARS - All Events	E-133
System: Resource Usage	E-133
Activity: All - Top Destinations	E-134
Activity: All - Top Reporting Devices	E-134
Activity: All - Top Sources	E-134
Activity: All - Top Reporting Device Types	E-134
Activity: Network Usage - Top Destination Ports	E-134
Activity: All Events and Netflow - Top Destination Ports	E-134
Activity: All Sessions - Top Destination Ports by Bytes	E-134
Activity: All Sessions - Top Destinations by Bytes	E-134
Resource Utilization: Bandwidth: Inbound - Top Interfaces	E-134
Resource Utilization: CPU - Top Devices	E-134
Resource Utilization: Bandwidth: Outbound - Top Interfaces	E-135
Resource Utilization: Concurrent Connections - Top Devices	E-135
Resource Utilization: Memory - Top Devices	E-135
Activity: Network Usage - Top Destination Ports By Bytes	E-135
System: Restricted Network Traffic	E-135
Activity: P2P Filesharing/Chat - Top Event Types	E-135
Activity: IRC - All Events	E-135
Activity: Spyware - Top Hosts	E-136
Activity: P2P Filesharing/Chat - Top Hosts	E-136
Activity: Recreational - Top Sources	E-136
Activity: Recreational - All Events	E-136
Activity: Spyware - All Events	E-136
Activity: P2P Filesharing/Chat - All Events	E-136
Activity: Uncommon or Anomalous Traffic - All Events	E-136
System: SOX 302(a)(4)(A)	E-136
Activity: Database Object Modification Successes - All Events	E-137
Activity: Database Privileged Command Successes - All Events	E-137
Activity: Database User/Group Change Successes - All Events	E-137
Activity: Host Login Success - All Events	E-137
Activity: Host Admin Login Success - All Events	E-137
Activity: Host Security Policy Changes - All Events	E-137
Activity: Database Login Successes - All Events	E-137

System: SOX 302(a)(4)(D)	E-137
Activity: Host Registry Changes - All Events	E-138
Activity: Host User/Group Management - All Events	E-138
Activity: Database Privileged Command Successes - All Events	E-138
Activity: Database User/Group Change Successes - All Events	E-138
Activity: Host Login Success - All Events	E-138
Activity: Host Admin Login Success - All Events	E-138
Activity: Host Security Policy Changes - All Events	E-138
Activity: Database Login Successes - All Events	E-138
System: SOX Compliance Reports	E-138
Activity: All - Top Reporting Devices	E-141
Activity: Attacks Prevented - Top Reporting Devices	E-141
Activity: Attacks Seen - Top Reporting Devices	E-141
Activity: Denies - Top Destination Ports	E-141
Activity: Denies - Top Destinations	E-141
Activity: Denies - Top Sources	E-141
Activity: IDS Evasion - Top Event Types	E-141
Activity: P2P Filesharing/Chat - Top Event Types	E-141
Activity: Scans - Top Destination Ports	E-141
Activity: Scans - Top Destinations	E-141
Activity: Stealth Scans - Top Sources	E-142
Activity: Virus/Worms - Top Event Types	E-142
Activity: All - Top Rules Fired	E-142
Attacks: All - Top Sources	E-142
Attacks: Database Server - Top Event Types	E-142
Attacks: FTP Server - Top Event Types	E-142
Attacks: Identity Spoofing - Top Event Types	E-142
Attacks: Login Services - Top Event Types	E-142
Attacks: Mail Server - Top Event Types	E-142
Attacks: Network DoS - Top Event Types	E-142
Attacks: RPC Services - Top Event Types	E-143
Attacks: Virus/Worms - Top Sources	E-143
Attacks: Web Server/App - Top Event Types	E-143
Operational Issues: Network - Top Reporting Devices	E-143
Operational Issues: Server - Top Reporting Devices	E-143
Resource Issues: Network - Top Reporting Devices	E-143
Resource Issues: Server - Top Reporting Devices	E-143
Activity: IRC - All Events	E-143
Attacks: All - Top Event Type Groups	E-143
Activity: All - Top Reporting Device Types	E-143

Activity: Host Login Failures - Top Destinations	E-144
Activity: Host Login Failures - Top Users	E-144
Activity: Host Registry Changes - All Events	E-144
Attacks: All - Top Destinations	E-144
Activity: Host User/Group Management - All Events	E-144
Activity: Host User/Group Management - Top hosts	E-144
Activity: Network Usage - Top Destination Ports	E-144
Attacks: Password - Top Destinations	E-144
Attacks: Uncommon or Anomalous Traffic - Top Event Types	E-144
Activity: Spyware - Top Hosts	E-144
Activity: Host Privilege Escalation - Top Hosts	E-145
Activity: P2P Filesharing/Chat - Top Hosts	E-145
Activity: Virus/Worms - Top Infected Hosts	E-145
Activity: Database Privileged Command Failures - All Events	E-145
Activity: Virus: Detected - Top Users	E-145
Activity: Database Privileged Command Failures - Top Users	E-145
Activity: Virus: Infections - Top Users	E-145
Activity: Database Regular Command Failures - All Events	E-145
Activity: Database Regular Command Failures - Top Users	E-145
Activity: Database User/Group Change Failures - All Events	E-145
Activity: Database User/Group Change Failures - Top Users	E-145
Activity: Database User/Group Change Successes - All Events	E-146
Activity: Database User/Group Change Successes - Top Users	E-146
Activity: Recreational - All Events	E-146
Resource Utilization: Bandwidth: Inbound - Top Interfaces	E-146
Resource Utilization: CPU - Top Devices	E-146
Resource Utilization: Bandwidth: Outbound - Top Interfaces	E-146
Resource Utilization: Concurrent Connections - Top Devices	E-146
Resource Utilization: Errors: Inbound - Top Interfaces	E-146
Resource Utilization: Errors: Outbound - Top Interfaces	E-146
Resource Utilization: Memory - Top Devices	E-146
Activity: Host Login Failures - All Events	E-146
Activity: Spyware - All Events	E-147
Activity: Host Login Success - All Events	E-147
Activity: Host Admin Login Success - All Events	E-147
Activity: Host Privilege Escalation - All Events	E-147
Activity: Network Usage - Top Destination Ports By Bytes	E-147
Activity: Remote Access Login - All Events	E-147
Activity: Vulnerable Host Found via VA Scanner	E-147
Activity: Vulnerable Host Found	E-147

Attacks: Password - All Events	E-147
Configuration Changes: Network - All Events	E-147
Operational Issues: Network - All Events	E-147
Operational Issues: Server - All Events	E-148
Activity: Host Security Policy Changes - All Events	E-148
Activity: Database Login Successes - All Events	E-148
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-148
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-148
Activity: Security Posture: NAC Status Query Failure - Top Hosts	E-148
Activity: Security Posture: Not Healthy - All Events	E-148
System: Security Posture Compliance (Cisco NAC)	E-148
Activity: Vulnerable Host Found via VA Scanner	E-149
Activity: Vulnerable Host Found	E-149
Activity: Security Posture: Healthy - Top Users	E-149
Activity: Security Posture: NAC - Top NADs	E-149
Activity: Security Posture: NAC - Top Tokens	E-149
Activity: Security Posture: NAC L2IP - Top Tokens	E-150
Activity: Security Posture: NAC Audit Server Issues - All Events	E-150
Activity: Security Posture: NAC Infected/Quarantine - All Events	E-150
Activity: Security Posture: NAC Infected/Quarantine - Top Hosts	E-150
Activity: Security Posture: NAC L2 802.1x - Top Tokens	E-150
Activity: Security Posture: NAC Static Auth - Top Hosts	E-150
Activity: Security Posture: NAC Static Auth - Top NADs	E-150
Activity: Security Posture: NAC Status Query Failure - Top Hosts	E-150
Activity: Security Posture: Not Healthy - All Events	E-151
Activity: Security Posture: NAC - Top NADs and Tokens	E-151
Activity: Security Posture: NAC Agentless - Top Tokens	E-151
Activity: Security Posture: NAC End Host Details - All Events	E-151
Activity: AAA Failed Auth - All Events	E-151
Activity: AAA Failed Auth - Top NADs	E-151
Activity: AAA Failed Auth - Top Users	E-151
Activity: Security Posture: NAC Agentless - Top Hosts	E-152
Activity: Security Posture: NAC Agentless - Top NADs	E-152
System: Server Exploits	E-152
Activity: IDS Evasion - Top Event Types	E-152
Attacks: Database Server - Top Event Types	E-152
Attacks: FTP Server - Top Event Types	E-152
Attacks: Identity Spoofing - Top Event Types	E-153
Attacks: Login Services - Top Event Types	E-153
Attacks: Mail Server - Top Event Types	E-153

Attacks: RPC Services - Top Event Types E-153

Attacks: SNMP - Top Event Types E-153

Attacks: Web Server/App - Top Event Types E-153

Attacks: Uncommon or Anomalous Traffic - Top Event Types E-153

INDEX



Preface

This guide describes how to use the web interface in the Local or Global Controller to administer and monitor your network.

Audience

This guide should be employed by users and administrators of Cisco Security MARS Local And Global Controllers.

Organization

This document contains the following chapters and appendixes:

- **Chapter 1, “Introduction to MARS”**—This chapter defines components of the Cisco Security Monitoring, Analysis, and Response System (MARS), introduces the Global Controller and the Local Controller, and presents its basic features and deployment options.
- **Chapter 2, “Security Threat Mitigation (STM) Task Flow Overview”**—This chapter 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.
- **Chapter 3, “Reports and Mitigation Devices Overview”**—
- **Chapter 4, “Rules”**—This chapter covers defining and use inspection rules.
- **Chapter 5, “Alerts and Incident Notifications”**—This chapter details the MARS configuration required to send an alert based on an inspection rule.
- **Chapter 6, “Management Tab Overview”**—This chapter details how to manage events, networks, variables, hosts, services, and MARS users.
- **Chapter 7, “Network Summary”**—This chapter details the Summary tab, which includes the Dashboard, the Network Status, and the My Reports pages and, on the Global Controller only, the Hotspots Diagram page.
- **Chapter 8, “Queries and Reports”**—This chapter covers working with scheduled and on-demand reports and queries. It also discussing using the real-time event viewer.
- **Chapter 9, “Incident Investigation and Mitigation”**—This chapter describes incidents and false positives and provides a starting point for configuring a Layer 2 path and mitigation to work with a MARS.

- **Chapter 10, “Case Management”**—This chapter covers using cases to provide accountability and improve workflow.
- **Chapter 11, “Security Manager Policy Table Lookup from a MARS Event”**—This chapter describes how to configure and use Security Manager and MARS so as to enable bi-directional lookup between events received by MARS and access rule and signature policy found in Security Manager.
- **Chapter 12, “Botnet Traffic Filtering”**—This chapter describes how MARS identifies and reports incidents associated with botnet event data captured by the Cisco ASA Botnet Traffic Filter.
- **Chapter 13, “System Maintenance”**—This chapter covers some of the maintenance chores for the MARS.
- **Chapter 14, “Authenticating MARS Accounts with External AAA Servers”**—External Authentication, Authorization and Accounting (AAA) servers can act as the authentication mechanism for MARS Appliance GUI logins (username and password). This permits authentication and centralized password management for all MARS Appliances. This chapter describes the AAA feature for the MARS Appliances.
- **Chapter 15, “Monitoring Events from Custom and Unsupported Devices or Versions”**—This chapter explains how to define custom device types and event types. These definitions enable a MARS Appliance to process events generated by an unsupported device type or version. This chapter also explains how to create custom packages to share across MARS Appliances. These packages include custom device types, event types definitions, rules, and reports. Last, it explains how to import and export custom packages from a MARS Appliance, as well as how to upload and download packages from the MARS forum on NetPro website.
- **Appendix A, “Date/Time Format Specification”**—The date/time field parsing is supported using the Unix `strptime()` standard C library function.
- **Appendix B, “Regular Expression Reference”**—The syntax and semantics of the regular expressions supported by PCRE are described in this appendix.
- **Appendix C, “DSF Event Type Group Reference”**—
- **Appendix D, “Cisco Security MARS XML API Reference”**—This appendix presents the XML schema used by MARS for XML-based notifications.
- **Appendix E, “System Rules and Reports”**—Defines the system rules and reports provided with Cisco Secure MARS

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</i> font

Item	Convention
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 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.



CHAPTER 1

Introduction to MARS

This chapter delineates basic components of the Cisco Security Monitoring, Analysis, and Response System (MARS), introduces the Global Controller and the Local Controller, and presents a basic understanding of features and deployment options.

This chapter contains the following topics:

- [System Description, page 1-1](#)
- [Basic Functions of the Global Controller, page 1-4](#)
- [Deployment, page 1-5](#)

System Description

Cisco Security MARS is a security threat mitigation (STM) system. It delivers a range of information about your networks' health as reported by devices in your network. Cisco Security MARS processes raw events from your reporting devices, sessionizes them across different devices, evaluates for matching inspection rules (system and user-defined), identifies false positives, and consolidates information using diagrams, charts, queries, reports, and rules.



Tip

Sessionize refers to correlating the reported network data, logs, and events into a higher-level interpretation to identify those packets as part of a single session, or a communication, that has a beginning, a body, and an end.

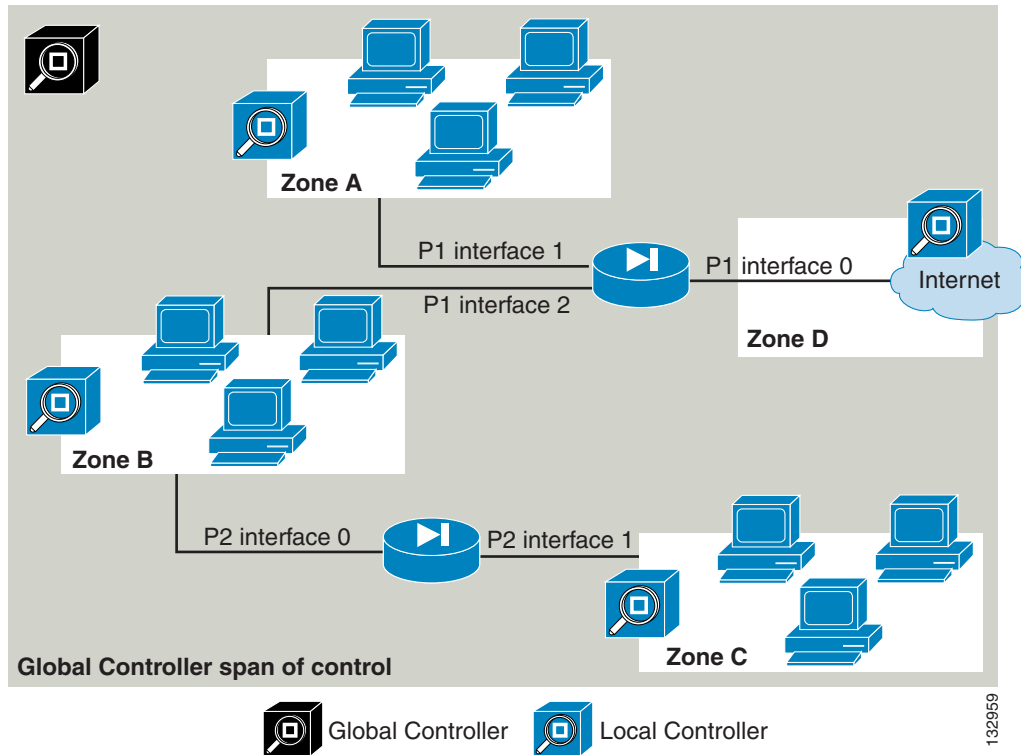
MARS enables you to be more productive by:

- Reducing the amount of raw data that requires manual review
- Enabling an evolving view of the network security posture
- Identifying hot spots of malicious activity
- Blocking undesirable traffic from the network

The MARS system operates at distinct and separate levels based on how much information is provided about your network's reporting devices. At its most basic level, MARS functions as a syslog server. As you add information about reporting devices, MARS begins to sessionize the raw data, and after you configure additional reporting devices and enable the more verbose reporting features, it presents a much more comprehensive view of your network, from which you can quickly drill-down to a specific MAC address, for example.

While it is possible to employ a single MARS appliance, many find that a distributed system preferable. In such a design, a Global Controller controls and communicates with a series of Local Controllers, thereby monitoring events from multiple local zones within the network. [Figure 1-1](#) presents an example deployment of MARS, which identifies these components and their relationships.

Figure 1-1 Relationship of Global Controller to Local Controller to Reporting/Mitigation Device



This section contains the following topics:

- [Local Controller, page 1-2](#)
- [Global Controller, page 1-3](#)
- [Advantages of a Distributed Global/Local Architecture, page 1-3](#)
- [MARS Web Interface, page 1-4](#)
- [Reporting and Mitigation Devices, page 1-4](#)

Local Controller

The Local Controller models are as follows:

- Gen 1: MARS 20, MARS 20R, MARS 50, MARS 100, MARS 100e, and MARS 200.
- Gen 2: MARS 25, MARS 25R, MARS 55, MARS 110R, MARS 110, and MARS 210.

Each model differs in its ability to process and store events from reporting devices, enabling you to accurately address your needs based on the size of your network and the traffic volume.

Local Controllers receive and pull data from reporting devices, which may include firewalls, routers, intrusion detection/prevention systems, and vulnerability assessment systems. Based on the data obtained from those devices, and the established level of integration with them, MARS can present you with suggested mitigation rules for detected attacks and, in some cases, push those rules to the mitigation device, which is a network device that contains the attack by restricting network access to the infected hosts.

A Local Controller summarizes information about the health of your network based on data it receives from the reporting devices that it monitors.

The Local Controller performs the following functions:

- Collects all raw events
- Sessionizes events across different devices
- Fires inspection rules for incidents
- Determines false positives
- Delivers consolidated information in diagrams, charts, queries, reports, and notifications
- Detects inactive reporting devices

Global Controller

A Global Controller summarizes the findings of two or more Local Controllers. In this way, the Global Controller enables you to scale your network monitoring without increasing the management burden. The Global Controller provides a single user interface for defining new device types, inspection rules, and queries, and it enables you to manage the Local Controllers under its control. This management includes defining administrative accounts and performing remote, distributed upgrades of the Local Controllers. The Global Controller is available in the following models:

- MARS GCm and MARS GC
- Gen 2: MARS GC2 and MARS GC2R

A Global Controller monitors two or more local zones. Each zone consists of a cluster of monitored devices and is managed by a Local Controller.

Advantages of a Distributed Global/Local Architecture

The Global Controller/Local Controller architecture has the following advantages:

- It allows for centralized, distributed management of network topology.
- It lets remote sites view their own data while keeping data private between Global Controller and Local Controllers.
- It enables you to view the entire network from the Global Controller.
- It provides linear scalability using a multi-layer hierarchy.
- It enables you to use multiple Local Controllers to isolate departmental functions such as host logging, NIDS, compliance, and for network profiling and anomaly detection.
- It preserves the WAN link by pushing up correlated information instead of raw data from monitoring device.

MARS Web Interface

The MARS web interface operates on a client computer. With many features common to both the Local Controller and Global Controller, the web interface uses a tabbed, hyperlinked, browser-based user interface. You access the web interface from any computer that can access the MARS Appliance on your network. For more information on client requirements, see the *Web Browser Client Requirements* section in the [Deployment Planning Guidelines](#) chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*.

From the web interface, you can perform most of your administrative functions, including all functions that are not supported at the command line.

Reporting and Mitigation Devices

If you consider the MARS system from a top-down perspective, you see that the Global Controller monitors Local Controllers and that Local Controllers monitor one or more reporting devices. Reporting devices provide MARS with a variety of data about the network, from traffic flows (in the case of a router) to the configuration of possible attack targets (such as from a vulnerability assessment system).

A reporting device that can deny a traffic flow is called a *mitigation device* (for example, a switch). MARS provides mitigation support in two forms:

- For supported Layer 3 devices (based on the OSI Network Model), MARS provides you with a suggested device and set of commands that can be used to halt an ongoing, detected attack. You can use this information to manually block the attack.
- For supported Layer 2 devices, MARS recommends a device, a set of commands to halt the ongoing, detected attack, and provides a method for making the configuration changes on your behalf.

How you configure your reporting devices and mitigation devices greatly affects the ability of MARS to detect ongoing attacks.

Basic Functions of the Global Controller

The Global Controller centrally manages a group of Local Controllers. Its user interface displays a listing of all the zones with their respective Local Controllers.

The Global Controller monitors and manages the network with a powerful suite of functions:

- Incidents
- Rules
- Queries and reports
- Centralized maintenance (for example, software upgrades of managed Local Controllers)

A Global Controller Admin user has the ability to create, edit or delete information on the Global Controller and its monitored Local Controllers. Information such as:

- Rules
- Reports and queries
- User, IP and service management
- Management grouping (for example, event and user groupings)

Incidents

The Global Controller can monitor any Local Controller at any time to receive data. It receives summarized information from all its Local Controllers and produces a merged summary of this data. The summary consists of global topologies and incidents reflecting network activities in each of its zones. You can drill down on topologies and incidents to reach their subsets of paths and events at the zonal level.

The summaries provides an account of high-, medium-, and low-priority incidents. All network, port, protocol, applications, and events have to be global in scope to be on the Global Controller.

Rules

The Global Controller uses rules to monitor the zones that report to it. Rules that apply to multiple Local Controllers can be created on the Global Controller and pushed down to them from a central location. These rules trigger incidents that you can review at the global level.

**Note**

Rules created on the Local Controller remain local. Incidents generated from these rules do not get pushed up to the Global Controller.

Centralized Maintenance

The Global Controller leaves most data archiving to the Local Controller. However, some basic archive/restore capability is provided at the global level.

The Global Controller centrally manages all upgrades to the Local Controllers. Global Controller manages Local Controller(s) that are running the same version of the software as it is.

Deployment

The Global Controller system's flexible architecture supports two basic types of deployment: incremental and greenfield. Each of these are discussed in the sections that follow.

This section contains the following topics:

- [Incremental Deployment, page 1-5](#)
- [Green-field, Multi-box Deployment, page 1-6](#)
- [Zone Planning, page 1-6](#)

Incremental Deployment

In this scenario, an administrator deploys one or more Local Controller systems as standalone units. At a later date, the administrator decides to add a Global Controller. You must then ensure that the previously deployed Local Controllers can communicate with the new Global Controller. To enable this communication, you must:

1. Create a zone for each Local Controller
2. Ensure that the reporting devices do not overlap among zones

3. Upgrade the Local Controller version to be the same as that of the Global Controller
4. Add the Local Controller as a monitored controller in the Global Controller.
5. The Global Controller is then configured to communicate with each Local Controller by exchanging security certificate information.

After this communication has been enabled, the Global Controller is able to receive information, such as incidents and rules, from the Local Controller.

Green-field, Multi-box Deployment

In this scenario, the network administrator decides from the very start to deploy two or more Local Controllers and a Global Controller to monitor them. In this case, the administrator defines the zones and their monitored devices ahead of time to complete a smooth installation.

Zone Planning

A zone is a logical collection of one or more subnetworks that are home to the reporting devices monitored by a Local Controller. Zones allow a Global Controller to distinguish among events that are correlated by Local Controllers that monitor unique subnetworks with common network addresses. For example, consider the case where a managed security service provider (MSSP) uses a Global Controller to monitor the Local Controllers of their clients. That MSSP cannot prevent its clients from using the same private network addresses, however, it can use zones to distinguish among those networks and clients.

The requirements for planned zones are few:

- Each zone must be uniquely named.
- A Local Controller cannot belong to more than one zone.
- Each Local Controller corresponds to a single zone.



CHAPTER 2

Security Threat Mitigation (STM) Task Flow Overview

A reasoned approach to employing Cisco Security Monitoring, Analysis, and Response System (MARS) requires that you firmly grasp the objectives you have in mind and the policies by which you'll accomplish them. This chapter first provides basic lists of [Policy Objectives, page 2-1](#) for security, monitoring, mitigation, and remediation and shows how they should each be considered part of a single comprehensive approach. Such a set of explicit policies acts as a comprehensive foundation and enables the application of specific measures.

The chapter then describes two project phases and task flows that you should follow when you deploy MARS as a security threat mitigation (STM) system in your network. These include:

- Provisioning (see [Checklist for Provisioning Phase, page 2-3](#)).
- Monitoring (see [Checklist for Monitoring Phase, page 2-9](#)).

Finally, this chapter concludes with a discussion of [Appliance-side Tuning Guidelines, page 2-15](#), and provides two worksheets that you can use:

- A [Device Inventory Worksheet, page 2-16](#)
- A [User Role Worksheet, page 2-18](#)

Policy Objectives

This section contains the following topics:

- [Security Policy Objectives, page 2-1](#)
- [Monitoring Policy Objectives, page 2-2](#)
- [Mitigation Policy Objectives, page 2-2](#)
- [Remediation Policy Objectives, page 2-2](#)
- [Cisco Security Wheel, page 2-3](#)

Security Policy Objectives

Your security policy should:

- Identify security objectives for your organization.
- Document the resources to protect.

- Identify the network infrastructure with current maps and inventories.
- Identify the critical resources (such as research and development, finance, and human resources) that require extra protection.

Monitoring Policy Objectives

Your monitoring policy should:

- Identify the expected administrative traffic flows across your network, including user, source, destination, services, and hours of operation.
- Identify expected network traffic for security probing and vulnerability testing, including user, source, destination, services, and hours of operation.
- Identify the network infrastructure able to provide audit data in “network proximity” to the critical resources.
- Identify the various event logging levels available from the devices and hosts in the network infrastructure.
- Identify the devices and techniques used to investigate

Mitigation Policy Objectives

Your mitigation policy should:

- Identify the choke points on your network relative to the critical resources.
- Define your process for documenting mitigated attacks on layer 2 and layer 3 devices.
- Define your process for documenting mitigated attacks at the host and application layer.
- Resolve corporate ownership issues among network operations, security operations, host owners, and application owners on shared hosts.
- Identify your policy for notifying security response teams and remediation teams.
- Identify vendor detection tool prioritization process, such as IOS IPS Dynamic Attack Mitigation (DAM).
- Identify how you want to block detected attacks: block them temporarily or permanently, block them using MARS-generated rules, using custom rules defined by security operations team, etc.

Remediation Policy Objectives

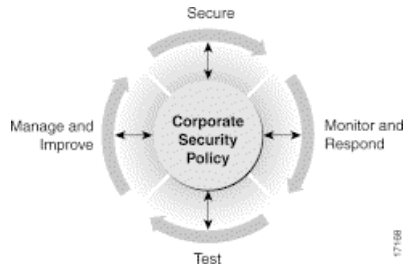
Your remediation policy should:

- Identify the responses to detected but unmitigated attacks for each type of node in your network.
- Identify tool vendor update policies to ensure proper remediation of hosts and applications.
- Identify the policies and procedures for isolating infected legacy hosts where remediation options are unavailable. These procedures may include restoring from backups or network isolation.

Cisco Security Wheel

Your policies, and the objectives they comprise, become the hub of the Cisco Security Wheel, (Figure 2-1).

Figure 2-1 Cisco Security Wheel



The spokes of the Cisco Security Wheel represent network security as a continual process consisting of four steps:

1. Secure your system.
2. Monitor the network for violations and attacks against your security policy and respond to them.
3. Test the effectiveness of the security safeguards in place.
4. Manage and improve corporate security.

You should perform all four steps continually, and you should consider each of them when you create and update your corporate security policy.

Checklist for Provisioning Phase

Provisioning deals with planning, setting up, and configuring the hardware, software, and networks that actually provide access to the data and network resources for the MARS Appliance. This phase takes place after you successfully complete the installation, which is detailed in the [Cisco Security MARS Initial Configuration and Upgrade Guide](#).

The following checklist describes the tasks required to understand the decision-making process and the basic flow required to provision MARS in the most productive manner. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1 Inventory and review possible reporting devices, mitigation devices, and supporting devices.

- **Reporting devices**—provide logs about user and network activities as well as device status and configuration.
- **Mitigation devices**—can be used to respond to detected attacks. They also act as reporting devices.
- **Supporting devices**—provide network services to reporting devices, mitigation devices, or a MARS Appliance.

Identifying which devices on your network to monitor depends on multiple factors, including their placement, the reporting they can provide relative to other devices on the same network segment, and the level of operation that you want to achieve from your MARS Appliance.

When considering which devices to declare as reporting devices and mitigation devices, be sure you know what data is provided to MARS by those devices. Simply adding all possible devices does not guarantee the best monitoring and mitigation strategy. Deliberate selection of the devices can reduce the MARS workload, resulting in improved detection and mitigation times, as well as improved detection of false positives.

As MARS only considers monitored devices, you should take care in identifying which devices to monitor. The following are only a few examples of considerations you should make when identifying devices:

- Consider the types of logs and data available from reporting devices on specific network segments, and select those logs that provide the most complete picture of the activity on your network.
- Identify mitigation devices at natural chokepoints across each segment in your network. You are more likely to stop an attack if these mitigation devices are identified to MARS. When MARS identifies an attack, it studies the topology of your network to identify the best chokepoint; however, it only considers those devices that are monitored.
- Supporting devices can play an important role in the operation of your STM system. Therefore, you should inventory and review the supporting devices on your network, which include e-mail, AAA, DNS, and syslog servers, that will play a role in the envisioned STM system.

Result at Step Completion: The list of devices that you want to monitor is complete. The details of each device include device name, reporting IP address, management IP address, management protocol, administrative account information, and the logging features, levels, and protocols to enable.

For more information, see the following references:

1. [Selection of the Devices to Monitor, page 3-2](#)
2. [Levels of Operation, page 3-1](#)
3. Deployment Planning Guidelines, in *Cisco Security MARS Initial Configuration and Upgrade Guide 6.X*.
4. [Device Inventory Worksheet, page 2-16](#)

Step 2 Identify and enable all required traffic flows.

After you identify the devices, you must verify that the network services they use for management, reporting, and notification are permitted along the required traffic flows. Using the detailed [Device Inventory Worksheet, page 2-16](#) identified in the previous task, ensure that the management, logging, and notification traffic between the MARS Appliance and each supporting device, reporting device, and mitigation device is allowed by intermediate gateways.

In addition, network services of supporting devices, such as DNS, e-mail, AAA, and NTP servers, must also be permitted to flow among the MARS Appliance, the supporting devices, and the reporting devices and mitigation devices on your network.

MARS applies the device time to received events only. For all events pulled from devices such as IDS/IPS devices or Windows, MARS uses the reported time as long as that reported time falls within 3600 seconds of the time on the MARS Appliance.



Tip

It is a recommended security practice to have all devices, including MARS Appliances, synchronized to the same time. Also, since the MARS Appliance is an HTTPS server, it uses certificates which require the time, date, and time zone to be set properly. Otherwise, sessions and incidents are stamped incorrectly and you may experience “time out” errors when accessing the web interface.

To limit troubleshooting, you should test each traffic flow from the source network segment to the destination segment. If possible, you should test all device-to-device flows for each protocol to ensure that “best match” versus “first match” semantics of various gateway ACLs do not hinder required traffic flows. As with any security devices on your network, enabled traffic flows should be restricted to the required protocols, ports, and source/destination pairs.

Result at Step Completion: You have verified that all intermediate gateways permit the log, management, and notification traffic between the devices and the MARS Appliance.

For more information, see the following references:

1. [Event Timestamps and Processing](#) in *Top Issues for the Cisco Security Monitoring, Analysis, and Response System*
2. Deployment Planning Guidelines, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
3. Supporting Devices, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
4. Required Traffic Flows, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
5. Specify the Time Settings, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
6. [Device Inventory Worksheet, page 2-16](#)

Step 3 Bootstrap the reporting devices, mitigation devices, and supporting devices.

For each device identified in the [Device Inventory Worksheet, page 2-16](#) *Device Inventory Worksheet*, you must prepare, or bootstrap, that device to ensure that the desired communications with MARS occur. Bootstrapping a device involves configuring the settings for that device, as determined by its role within the STM system. Perform the following bootstrap tasks as applicable to a device type and its role:

- Enable management of the device by the MARS Appliance for mitigation and access.
- Install an agent that collects the correct logs for MARS Appliance.
- Turn on the correct logging level and logging services.
- Direct the logs to the MARS Appliance or identify the appliance to receive or pull those logs as needed.
- Enable discovery of the device settings.
- Enable the device to receive notifications from the MARS Appliance.

Each device has a different required configuration to ensure that it assumes the role you have envisioned for it in the STM system. As you consider the devices, their expected role in your STM system will correlate directly with the configuration of the tasks listed above. In addition, you identify any restrictions imposed by MARS. For example, MARS may restrict the supported protocols for discovery of a specific device type.

Result at Step Completion: The correct logging levels are enabled on the reporting devices and mitigation devices. The MARS Appliance can receive or pull any necessary logs from those devices, and it can retrieve configuration settings and push ACLS to the supported mitigation devices. Any devices that require notification of detected attacks are configured to receive such notifications from the MARS Appliance. Although the MARS Appliance picks up and stores the events it receives, it does not inspect them until the reporting devices and mitigation devices are defined and activated in web interface.



Tip

Any events published by a device to MARS prior to adding and activating the device in the web interface can be queried using the reporting IP address of the device as a match criterion. This technique can be useful for verifying that the device is properly bootstrapped.

For more information, see the following references:

1. [Device Inventory Worksheet, page 2-16](#)
2. [Supported Reporting and Mitigation Devices](#)
3. Bootstrap Summary Table in the [Configuring Reporting and Mitigation Devices in MARS](#) chapter of the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
4. The log settings sections of the user guides for your reporting devices and mitigation devices

Step 4 Define the devices in MARS.

After you identify and bootstrap the reporting devices and mitigation devices and enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices. You can do this by adding individual devices in the web interface or by importing a comma separated value (CSV) file, which can define the required settings for basic device types and give you a headstart on defining the more complicated devices. In addition, you can use topology discovery to automatically discover reporting devices and mitigation devices and later go back to provide additional detail.

For most device types, you must determine what access protocol to use for device discovery. The selection of this protocol determines what type of data you can discover and whether you can perform mitigation. Understanding the options helps you develop a consistent approach in compliance with your corporate policies.

How you choose to add the devices depends on the number of devices on your network and whether there are CSV device keywords for the devices that you want to add. In addition, device types that use agents, modules, or sensors are defined in multiple steps, where you first define the base host or device, and then add the modules, sensors, and agents to the base device. For example, if you want to add an IPS module to a Cisco ASA device, you must first define the Cisco ASA device and then define the IPS module as a component of that device. In addition, many applications that are not dedicated appliances require that you first define the host (generic, Windows, Unix, or Linux) on which that application runs before you can associate the application with that host.

After you add the devices, you must activate them by clicking Activate on any page in the web interface.

To display all devices that are either added incorrectly or not activated in MARS, you can define one of two queries:

- Select “Unknown Reporting Device” in the Devices field. This query returns the events only for those devices that are reporting events that do not match one of the reporting IPs defined in MARS. When MARS receives events, it first determines whether the IP from which the events are received matches one of reporting IPs identified in the Reporting and Monitor Devices page. Only if MARS finds a match does it attempt to parse the events. Therefore, if the Reporting IP is defined incorrectly for a reporting device, the events from that device are not parsed. This query essentially identifies events that are not parsed.
- Select the “Unknown Device Event Type” in the Events field. This query returns events from known devices where, for some reason, the event is not parsed by MARS (for example, if the MARS signature list is not current with the device event lists), and it returns events reported by unknown devices.

These queries are a recommended good practice after adding the devices, especially when using a CSV seedfile or SNMP discovery. For both queries, if you are looking for a specific reporting IP address, enter that address in the Keyword field to filter the results down to those that include that IP address.

Result at Step Completion: All reporting devices and mitigation devices are defined and activated in MARS. When the devices are bootstrapped and defined in MARS, MARS begins to inspect the logs received from the devices. Until the devices are added in MARS, MARS picks up and stores the events it receives without inspecting them.

For more information, see the following references:

1. [Device Inventory Worksheet, page 2-16](#)
2. [Selection of the Access Type, page 3-9](#)
3. [Configuring Reporting and Mitigation Devices in MARS](#) chapter of *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
4. [Supported Reporting and Mitigation Devices](#) (CSV Keyword column)
5. [Verifying Connectivity with the Reporting and Mitigation Devices, page 3-15](#)
6. [Activate the Reporting and Mitigation Devices, page 3-17](#)

Step 5 Configure global data collection settings and schedules in MARS.

After you add the devices, you can enable the rich data collection features of MARS, which include:

- **Dynamic vulnerability scanning.** When MARS detects an attack, it can probe the network to determine the likely success and severity of the attack. To allow this data collection in response to detected attacks, you must enable the feature and identify which networks to analyze.
- **NetFlow data collection.** NetFlow data enables MARS to identify anomalies by profiling typical data flows across your network, allowing MARS to detect day-zero attacks, including worm outbreaks. Statistical profiling takes between four days and two weeks for a MARS Appliance to complete. When the profiles are developed, MARS begins detecting anomalous traffic flows and creates incidents in response to them. To configure NetFlow data collection, you must configure those devices that can generate NetFlow traffic, and you must configure MARS to listen on a shared community string.
- **Layer 3 topology discovery.** A process-intensive operation that discovers the layer 3 network devices (that is, those devices operating at the IP layer). This layer 3 data is used to determine the attack path vector and to populate the Topology graphs. You can define the schedule for updating this information.
- **Layer 2 device discovery.** This feature allows MARS to determine the attack path vector and to identify attacking hosts and targets by MAC address, which eliminates confusion caused by attacks that spoof IP addresses. This feature is typically configured when adding a switch and enabling mitigation.

There are also several device types from which MARS periodically pulls data. For such devices, you can define the intervals at which the event logs are retrieved and processed. These update features are as follows:

- **Windows event logs.** You can set the frequency by which MARS pulls audit trail records from Windows hosts and servers. This setting is global for all such hosts and has a default value of five minutes.
- **Oracle event logs.** You can set the frequency by which MARS pulls audit trail records from Oracle database servers. This setting is global for all such servers and has a default value of five minutes.
- **Monitored device update scheduler.** You can set the frequency by which MARS pulls data from specific reporting devices, such as Qualys QualysGuard, Foundstone Foundscan, and eEye REM. Schedules are set on a per IP address basis.

After you define the settings, you must activate them by clicking Activate on any page in the web interface.

Result at Step Completion: The schedules for updating cached data pulled from reporting, mitigation, and supporting devices are defined and activated in MARS. After these settings are defined, MARS can probe the network or pull updates from reporting, mitigation, and supporting devices.

For more information, see the following references:

1. [Data Enabling Features, page 3-17](#)
2. *Windows Event Log Pulling Time Interval* section of the [Device Configuration Guide for Cisco Security MARS, Release 6.x](#)
3. [Layer 2 Discovery and Mitigation, page 3-18](#)
4. *Configure Interval for Pulling Oracle Event Logs* section of the [Device Configuration Guide for Cisco Security MARS, Release 6.x](#)
5. [Networks for Dynamic Vulnerability Scanning, page 3-19](#)
6. [Understanding NetFlow Anomaly Detection, page 3-20](#)
7. [Discovering Your Network: Layer 3 Topology Discovery, page 3-27](#)
8. [Scheduling Topology Updates, page 3-31](#)

Step 6 Populate vulnerability assessment information for supporting devices and network assets.

Vulnerability assessment information describes specific hosts on your network. You can detail this information for any host, whether it is a host representing a reporting device, a mitigation device, or an important asset on your network.

This information identifies the operating system, patch levels, and the network services that run on the host.

After you define the hosts, you must activate them by clicking **Activate** on any page in the web interface.

Result at Step Completion: MARS understands more about the hosts on your network and the services that they run.

For more information, see the following references:

1. [Host and Device Identification and Detail Strategies, page 3-27](#)
2. [Device Inventory Worksheet, page 2-16](#)
3. [IP Management, page 6-3](#)
4. [Service Management, page 6-8](#)

Step 7 Monitor and tune event generation and processing.

As with all monitoring applications, tuning log generation and event processing is key to technical accuracy and performance. You can use two methods to tune which events are processed by MARS:

- **Device-side tuning**—This method involves restricting event generation at the device level. MARS never receives events that are not relevant to security or device status. It also involves eliminating superfluous, duplicate data reported by multiple devices on the network, as well as eliminating those events that can be reproduced by reports or queries in MARS, such as traffic summary syslogs.
- **Appliance-side tuning**—This method involves identifying events received by the MARS Appliance that represent normal or planned network activity. You define drop rules to prevent MARS from processing such events as part of potential security incidents. When defining such drop rules, you should be as precise in the definition as possible, for example, identify the source of expected ping sweeps by an IP address within an expected time period, which is much more difficult to spoof as it requires explicit knowledge of your network and administrative practices. You can further qualify the rules using a combination of seven conditions: source, destination, service type, event type, time range, reporting device, and event severity. You must choose whether to drop the event entirely or to drop it and log it to the database, where it can be used by queries and reports.

**Note**

Drop rules do not prevent MARS from storing the event data; they simply prevent the appliance from processing the events. Events affected by drop rules can still appear a query as they are being stored on the appliance. You are still storing them; just not processing them for inspection rules. Therefore, if appliance storage considerations are an issue, we recommend using device-side tuning.

**Note**

For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

Tuning is an ongoing task to improve the identification of attacks, report quality surrounding truly suspicious activities, and the overall performance and accuracy of your STM solution. It involves a detailed study of traffic, which can be conducted and refined by evaluating the events that are coming into the appliance on a device-by-device basis.

**Tip**

In a lab network environment, use a MARS Appliance to study generated events and tuning options on an individual device type basis. By documenting your requirements in a controlled environment, you can eliminate much of the production network tuning by establishing valuable device-side tuning standards for each monitoring device type.

Result at Step Completion: The events being processed by the MARS Appliance are restricted to those that provide value to the STM system.

For more information, see the following references:

1. [Appliance-side Tuning Guidelines, page 2-15](#)
2. *Configuring Logging Policies on Firewall Devices* in the [Managing Firewall Devices](#) chapter of the *User Guide for Cisco Security Manager 3.2.1*

Checklist for Monitoring Phase

After you complete the provisioning phase, you must configure MARS to help you realize your broader security goals and requirements. During the monitoring phase, your primary goal is to effectively realize your monitoring, mitigation, and remediation policies. This phase involves defining the strategies, rules, reports, and other settings required to achieve this goal.

**Note**

You must prepare MARS to closely adhere to your corporate security policy before you begin monitoring traffic flows, as you must be prepared to react to detected attacks.

The following checklist describes the tasks required to understand the decision-making process and the basic flow required to operate MARS in the most productive manner. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1

Develop monitoring, notification, mitigation, remediation, and audit strategies.

These strategies are concerned less with desired traffic flows and generated events and focus more on what to do after MARS Appliance processes that data. These strategies are at the heart of how you will use MARS to protect your network, taking into account the short- and long-term requirements of monitoring and forensic analysis, as well as how to stop ongoing attacks and clean infected hosts. These strategies encompass not only your expected interaction with MARS, but the expectations of your reporting devices as well. Essentially, they identify the roles, tasks, and data requirements that you anticipate so that you can map events, rules, queries, and reports to those roles that provide the data required by the identified tasks.

As with any security system, we recommend that users be assigned the lowest-level privilege required to perform their job. Admin-level privileges should be reserved for administrators of the MARS Appliance.

Result at Step Completion: You have identified the users and roles required to effectively respond to detected attacks and device issues. You have defined clear guidance for responding to notifications and understand the information requirements of those such notifications and the expected format and delivery methods to be used.

For more information, see the following references:

1. [Strategies for Monitoring, Notification, Mitigation, Remediation, and Audit, page 2-14](#)
2. [Chapter 10, “Case Management”s](#)
3. [User Management, page 6-11](#)
4. [Promoting Global User Roles on Local Controller, page 6-16](#)
5. [User Role Worksheet, page 2-18](#)

Step 2 Define the notification services.

This task prepares the notification services of MARS to notify your mitigation and remediation personnel and take other required actions. In MARS, notification services have three building blocks:

- **User accounts**—Represent users who will receive reports or notifications or who will access the web interface for the purpose of monitoring or mitigation. Users can receive notifications in the form of e-mail, pager messages, or Short Message Service (SMS) messages. Users are assigned to one of four roles, admin, security analyst, operator, notification only, which determines their access privileges in the web interface.
- **Devices**—Represent those devices that will receive notifications in the form of an SNMP message, a syslog message, or in the case of an IOS IPS device, a DAM message (equivalent to a shun). For more on defining devices, refer to [Checklist for Provisioning Phase, page 2-3](#).
- **Actions**—Actions are defined within inspection rules, and they represent the notifying action. Depending on the target of the notification, a user or a device, your action can provide guidance to your staff or instruct your devices to log or block an attack.

Within MARS, any person or device that is expected to receive a notification must be identified in the system. Therefore, the first step is to define user accounts that map to the users or groups who must be notified based on specific event settings (see [User Role Worksheet, page 2-18](#)). You must also identify the devices that need to be notified or that need to take some action (see [Device Inventory Worksheet, page 2-16](#)).

The next step is to define the notification service settings (actions), which can be one or more of e-mail, page, SMS, SNMP, Syslog, or Dynamic Attack Mitigation. Each of these settings includes the contact information and a message that you can define for each type of notification.

There is not a separate interface for defining these settings. To define the notification service settings, you must edit an existing inspection rule and add new Action definitions. After you define these settings, they are available to all inspection rules.

Result at Step Completion: All required personnel have been identified in MARS so that rules and reports can be customized to notify the correct personnel.

For more information, see the following references:

1. [User Management, page 6-11](#)
2. [Adding or Removing a User from a Custom User Group, page 6-15](#)
3. [IP Management, page 6-3](#)
4. “Adding Reporting and Mitigation Devices” found in the [Configuring Reporting and Mitigation Devices in MARS](#) chapter of *Device Configuration Guide for Cisco Security MARS, Release 6.x*
5. [Forwarding Alert Data to 3rd -Party Syslog and SNMP Servers, page 3-41](#)
6. [MARS MIB Format, page 3-44](#)
7. [Inspection Rules, page 4-4](#)
8. [Working with System and User Inspection Rules, page 4-14](#)
9. [Setting Alerts, page 4-21](#)
10. [Chapter 5, “Alerts and Incident Notifications”](#)

Step 3 Define custom inspection rules and refine system inspection rules.

Inspection rules correlate events from disparate devices into meaningful sessions that reflect the end-to-end activities of an attack or other network session. By identifying the end-to-end view of attacks, MARS is better able to identify mitigation points in your network. However, you can define inspection rules to accomplish different goals: identification of an attack is just one possible goal. Other example goals might include identifying use of priority assets, assessing network health, or refining your network configuration based on usage analysis.

MARS ships with over 100 system inspection rules; however, you may find that you cannot identify those sessions that are important to your corporate policies. For example, if you want to monitor the use of a custom or unsupported application, you can either define a new inspection rule that monitors traffic between a selected source and destination using a known protocol and port pair, or define a custom log parser that uniquely processes the events generated by that application to expose the data within the event that you want to track. Monitoring a known protocol port pair can provide summary data, such as number of sessions, where a custom log parser can enable detailed inspection of aspects of the traffic, such as resource utilization or failed logging attempts. To define a custom parser, you must know the message format used by that appliance, and it must be published to MARS in clear text.

Organizing the rules that you create into meaningful groups helps clarify your purpose and improve the learnability of the system. As you consider your specific goals, you should define a rule group (and a corresponding report group) to help you refine the strategies you identified in [Step 1](#), above. Because rules can be members of multiple groups, you do not have to worry about creating multiple rules to address the same issue. The groups are merely available to help you organize your work and allow you to focus on one strategy at a time.

Result at Step Completion: Any custom inspection rules are developed and existing inspection rules are configured to provide proper notification in compliance with your corporate policies. Any custom log parser and inspection rules are defined that enable the audit of the traffic flows of home-grown or unsupported applications or protocols.

For more information, see the following references:

1. [Rule and Report Groups, page 4-22](#)
2. [Event Management, page 6-2](#)
3. [IP Management, page 6-3](#)

4. [Service Management, page 6-8](#)
5. [User Management, page 6-11](#)
6. [Inspection Rules, page 4-4](#)
7. [Working with System and User Inspection Rules, page 4-14](#)
8. [Setting Alerts, page 4-21](#)
9. [Chapter 5, “Alerts and Incident Notifications”](#)

Step 4 Define custom queries and reports.

Queries and reports are forensic analysis tools. They help you analyze historical data and enable you to identify trends over longer periods of time than the real-time monitoring features of MARS. The relationship between queries and reports is essentially that queries are on-demand, refined inspections of data as defined by a report template. Reports are scheduled to run periodically, enabling you to define the periods and frequencies that you want to inspect on an ongoing basis. Queries allow you to narrow or broaden your search based on a report template by filtering the search criteria. While MARS provides many predefined report templates, you can define new report templates that focus on the incidents and events important to fulfilling your policies. This feature can be especially useful for adhering to compliance reporting requirements, as you can define a report, schedule it to be generated, and store the results as part of your audit records.

As with overall access, you can restrict the ability to run or view reports and queries based on user role. Such safeguards can reduce accidental tampering with schedule reports by other users of the system. In addition, you can configure your report templates so that users are notified of the report. Typically, e-mail is the primary method used for report notification, but all notification methods are supported.

Result at Step Completion: The report templates required to realize your forensic analysis and audit goals are defined and assigned to user roles according to your least privilege policies. Any report groups that facilitate access or division of reports and queries among your staff are defined.

For more information, see the following references:

1. [Chapter 8, “Queries and Reports”](#)
2. [Select Query Criteria, page 8-7](#)
3. [Batch Query Operations, page 8-14](#)
4. [Reports, page 8-26](#)
5. [Report Creation, page 8-29](#)

Step 5 Monitor network and security activity.

This task encompasses monitoring your network for attacks or issues and responding to them. How users interact with MARS depends on their role and your organization’s operational guidelines. For users who are expected to use the web interface to monitor traffic in near real-time, this task requires an in-depth understanding of the data that is correlated and displayed, as well as when and how to respond to suspicious or anomalous behavior.

MARS provides two interfaces to network and security activity: the Summary tab and the Query/Reports tab. Each interface provides different views and tools to help you understand what is happening on your network.

The Summary tab focuses on near real-time events, whereas the Query/Reports tab focuses on historical, forensic analysis as described in the next task of this checklist. The Summary tab organizes priority views of your network activity, displaying hot spot diagrams, recent events, charts of incidents, and a topology diagram, identifying recent activities.

When you identify an incident that requires further investigation or mitigation, you can investigate the incident to determine whether it is a false positive or block attack using MARS. If you have choke points operating at layer 2, primarily switches, MARS will identify the appropriate device, provide recommended CLI changes, and allow you to push these changes to the device. If the choke point is a layer 3 device, MARS recommends CLI changes that you can copy and paste into an administrative session with the identified choke point.

In this manner, you can monitor your network for suspicious behavior and respond to any detections.

Result at Step Completion: Users understand the views and tools required to monitor, verify, and mitigate attacks on the network.

For more information, see the following references:

1. [Chapter 7, “Network Summary”](#)
2. [Chapter 9, “Incident Investigation and Mitigation”](#)
3. [False Positive Confirmation, page 9-7](#)
4. [Rule and Report Groups, page 4-22](#)
5. [Using Event Groups, page 6-2](#)
6. [Chapter 10, “Case Management”](#)
7. [The False Positive Page, page 9-9](#)
8. [Retrieving Raw Messages, page 13-3](#)

Step 6 Monitor system and network health.

The STM system is more than your MARS Appliance; it includes all reporting devices and mitigation devices and any MARS Appliances. When assessing the health of the system, you should monitor the health of each of these devices. You can monitor your system health by using inspection rules that generate notifications for anomalous behavior, by generating system health queries and reports, and by manually reviewing the system logs of MARS.

MARS provides reports about use of common resources, including CPU, bandwidth, and memory. To simplify the monitoring of system health, you can define a report group that organizes these reports into a meaningful collection. You can also restrict the presentation of those reports and queries to specific user roles.

Because reports can be scheduled, you can notify the appropriate users each time the report is updated.



Tip

If you cannot view the resource usage of a reporting device, verify that you have enabled the Monitor Resource Usage option as part of that device definition in Admin > System Configuration > Security and Monitored Devices. For the list of devices that can be configured to provide this data, see [Configuring Resource Usage Data, page 3-34](#).

MARS also includes detailed logs about the status of the appliance itself, as well as several command-line utilities that present status on the health of the appliance.

Result at Step Completion: The users responsible for monitoring the system and network health understand the tools and reports provided by MARS to perform these functions.

For more information, see the following references:

1. [Rule and Report Groups, page 4-22](#)
2. [Rule and Report Group Overview, page 4-22](#)
3. [Configuring Resource Usage Data, page 3-34](#)

4. `pnstatus` command in [Cisco Security MARS Command Reference, 6.X](#)
5. `pnlog` command in [Cisco Security MARS Command Reference, 6.X](#)
6. [Setting Runtime Logging Levels, page 13-1](#)
7. [Viewing the MARS Backend Log Files, page 13-2](#)
8. [Viewing the Audit Trail, page 13-2](#)
9. [Retrieving Raw Messages, page 13-3](#)

Step 7 Tune MARS processing.

Tuning, which is an ongoing activity for any monitoring application, involves refining the sensitivity and accuracy of event processing. In MARS, you can do any of the following to effect such changes:

- Use drop rules to enable or disable the processing of events by MARS.



Note

For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

- Turn on or off event generation at the device.
- Identify selected incidents as false positives.
- Tune inspection rules to include or exclude specific networks, hosts, services, reporting devices, or traffic flows.
- Tune the inspection of traffic by device type, such as IPS and IDS, refining the rule set they use to generate events.
- Add or remove reporting devices to alter the reported event set or to provide supporting data that can be used to improve the self-tuning features of MARS, such as false positives, OS fingerprinting, and vulnerability assessment.
- Describe the expected behavior on your network by describing the assets, services, and vulnerability assessment information. The more details MARS knows about your network, the better it can assess the incoming events.

Result at Step Completion: The events being processed by the MARS Appliance are restricted or expanded to encompass those that provide the most value to the STM system.

For more information, see the following references:

1. [Appliance-side Tuning Guidelines, page 2-15](#)
2. [Working with Drop Rules, page 4-18](#)
3. [False Positive Confirmation, page 9-7](#)
4. [Selection of the Devices to Monitor, page 3-2](#)

Strategies for Monitoring, Notification, Mitigation, Remediation, and Audit

STM requires the close coordination of multiple strategies in support of your corporate security policies:

- Monitoring involves the study of network activities and device status to identify anomalous activities or behavior.
- Notification involves alerting those parties responsible for responding to detected anomalies with the information necessary to respond.
- Mitigation involves responding to suspicious activity to prevent the spread of anomalies across your network.
- Remediation involves responding to successful exploits to clean infected hosts on your network.
- Audit involves logging and reporting activities that have taken place during other tasks. The goal of audit is to provide an account the activities and responses to support compliance audits and trend analysis.

The first decision you must make is who will be responsible for mitigation at the selected choke points. Often, organizations separate specialized security devices from the core network infrastructure devices along organizational divisions. As an example, two separate teams, security operations and network operations, may be responsible for different network components or different policies on shared devices. Before you roll MARS out on your network, ownership of a strategies for mitigation must be clearly defined in according with your corporate policies.

When it comes to a mitigation strategy, two options exist:

- You can rely on MARS to identify the choke point and accept the recommended CLI changes to block the detected attack.
- You can issue notifications and incident details to a responsible party who can evaluate the MARS recommendations, but ultimately that party will make the final decision about where and how to stop the detected attack.

Regardless of the option you choose, you should develop guidelines on how long an attack should be blocked, how to investigate an internal attack so that you can clean them, who is responsible for updating the policies after the required quarantine period, and how records of such events should be maintained for audit compliance (for example, is the case management feature of MARS tied to your ticket integration system?).

Next, you should make a distinction in the type of monitoring that you should perform: system monitoring versus security monitoring. *System monitoring* involves monitoring not only the status of the MARS Appliance but also the health and status of the reporting devices and mitigation devices that MARS manages. *Security monitoring* focuses on network and security activity.

For both types of monitoring, you must decide what predefined and custom queries and reports are required, the processes for evaluating and responding to the data they reveal, and guidelines on using the case management features of MARS to manage the responses and track changes.

The last phase involves determining who should be notified when specific incidents are detected. For example, who is notified of device status incidents versus security-related incidents. You must identify your mitigation and remediation personnel, identify those responsible for monitoring (across organizations if necessary), and determine how notifications are to be generated and what they should look like. This involves selecting among methods, including SMS, pager alert, and e-mail, as well as whether the notifications are based on incidents, queries, or reports.

Appliance-side Tuning Guidelines

Tuning on the MARS Appliance focuses on not inspecting traffic that is received from the reporting devices. Two primary techniques exist for appliance-side tuning:

- **Drop rules**—This technique involves dropping all events that match specific criteria received from a reporting device. This technique is the fastest and the least refined. As part of defining a drop rule, you can also specify whether to retain the event log in or simply discard it. The advantage of drop rules is that they events are not processed by any inspection rules, which speeds up the processing of the appliance by reducing the potential workload.



Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

- **Removing devices from inspection**—This technique involves removing a device from inspection rules. This technique is specific to the events that trigger a specific type of alarm. The advantage of this technique is that it does not drop all events that match specific criteria received from a reporting device. In other words, your focus is on reducing a specific false positive rather than all incidents that are fired based on the events. In addition, the events are retained so that you can review them using queries and reports.

When using either of these techniques, remember that when you add or modify a rule, you must click Activate before the changes take effect.

Device Inventory Worksheet

The device inventory worksheet will help you collect the required information about the devices on your network. It includes the following information:

- **Device name**—Identifies the well-known name of the device. Typically, this name is the DNS name of the device. MARS uses this name in the topology graph, reports, and events.
- **Reporting IP address**—Identifies the IP address assigned to the network interface from which MARS will be receiving events. This address is used by MARS to map back to the device name and to uniquely identify messages and events originating from the device.
- **Management IP address**—Identifies the IP address assigned to the network interface to which MARS connects to discover the configuration settings for the device.
- **Username/password**—Identifies the account that has the correct authorization to connect to the management IP address and read or write information based on the role in the network. For reporting devices, this account must have privileges sufficient for MARS to read the existing configuration. For mitigation devices, specifically layer 2 switches, this account can enable MARS to publish actual CLI changes to the device to block detected attacks.
- **Role in system/segment**—Identifies whether this device is a reporting device or a mitigation device. It can also identify supporting devices, such as DNS and e-mail servers. In addition, the role should take into account this device's expected importance relative to the network segment, specifically relative to the other devices on the same segment. You can qualify this segment-level role using terms that fit your overall monitoring strategy, such as primary source, second opinion, attack identification, false positive assessment, session data, and endpoint/MAC address identification. Understanding the role that a device can or should play at a network segment level helps prioritize the required and tunable log settings.
- **Required protocols**—Identifies the protocols that this device uses to operate. The primary focus is on the management protocols, notification protocols, and protocols used to publish audit events.

User Role Worksheet

The user role worksheet will help you collect required information about administrators of your network. It includes the following information:

- **User Name**—Identifies the user by name.
- **User Role**—Identifies the role this user has with respect to your corporate security policies.
- **MARS Account**—Identifies the MARS user account and role—admin, security analyst, operator, or notification only—which determines access privileges in the web interface. For accountability and security, each user typically has a unique account. However, you can define group-based accounts.
- **Notification Settings**—Identifies the information required to contact this user when incident rules are fired. For users, notification settings include e-mail, pager messages, or SMS messages. For response teams, you may use group aliases. Users should be notified when inspection rules fire and scheduled reports are generated.
- **Device Ownership**—Identifies the reporting devices and mitigation devices on your network for which the user is responsible. This list is especially important when the user is a member of your mitigation or remediation team.
- **Inspection Rules**—Identifies any inspection rules required to meet the needs of this user role. These rules must to be defined or configured to notify the user when they fire.
- **Reports/Queries**—Identifies any reports and queries required to meet the needs of this user role. You must ensure that the user can access these reports and queries. Optionally, you may want to notify the user when scheduled reports are generated.

Table 2-2 *User Role Worksheet*

User Name	User Role	MARS Account/Role	Notification Settings	Device Ownership	Inspection Rules	Reports/Queries



CHAPTER 3

Reports and Mitigation Devices Overview

After you complete the initial configuration of Local Controller as described in the document [Cisco Security MARS Initial Configuration and Upgrade Guide 6X](#), you must determine a monitoring strategy to use for your network. You must also determine a mitigation strategy, if you chose to take advantage of the MARS mitigation features. For guidance on how to determine the monitoring and mitigation strategies, see [Chapter 2, “Security Threat Mitigation \(STM\) Task Flow Overview”](#).

This chapters assumes that you have made corporate-level policy decisions and that you are executing against the [Checklist for Provisioning Phase, page 2-3](#). This chapter provides the following:

- Guidance on selecting and configuring reporting devices and mitigation devices
- Discussion of the levels of operation that MARS supports
- Guidance on selecting a method for adding devices to Local Controller
- Discussion of those features that enable rich data collection

This chapter contains the following topics:

- [Levels of Operation, page 3-1](#)
- [Selection of the Devices to Monitor, page 3-2](#)
- [Understanding Access IP, Reporting IP, and Interface Settings, page 3-7](#)
- [Selection of the Access Type, page 3-9](#)
- [Operating Upon Reporting and Mitigating Devices, page 3-13](#)
- [Data Enabling Features, page 3-17](#)
- [Integrating MARS with 3rd-Party Applications, page 3-41](#)

Levels of Operation

Before configuring the MARS Appliance to recognize reporting devices, you should understand the three levels of operation that MARS can achieve.

MARS operates at three discernible levels based on the type of data collected from reporting devices and the features such data enables for the system. These levels focus on the ability to identify attacks from end-to-end, and they are separate from the features enabled by specific types of reporting devices.

- **Basic**—At this level, MARS behaves like a smart syslog server. It collects reporting device logs and support basic queries and reports. To enable basic operation, you must complete the initial configuration of the MARS Appliance as described in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*. In addition, you must specify the device name and

reporting IP addresses of the reporting devices as described in "Adding Reporting and Mitigation Devices" found in the [Configuring Reporting and Mitigation Devices in MARS](#) chapter of *Device Configuration Guide for Cisco Security MARS, Release 6.x*.

- **Intermediate**—At this level, MARS processes events and performs session-based correlation, including resolving NAT and PAT translations at the IP address layer. To enable intermediate operation, you must provide more details about the devices you want to monitor, including access IP addresses, management access passwords, OS platforms and versions, and running services and applications, see [IP Management, page 6-3](#) for more information.
- **Advanced**—This level is a fully enabled MARS Appliance. When advanced operation is enabled, MARS Appliance discovers and displays the full topology, draws attack paths, and enables MAC address lookups of the hosts involved in an attack. To enable advanced operation, you must provide the SNMP community string information for your network. You must also enable topology discovery, as defined in [Scheduling Topology Updates, page 3-31](#).

[Table 3-1](#) summarizes the levels, their configuration requirements, and the features enabled at that level.

Table 3-1 **Levels of Operation**

Level Of Operation	Configuration Requirements	Functionality Enabled
Level 1	MARS configured Reporting device names and reporting IP addresses added NetFlow enabled	Basic syslog functionality Event correlation Query, reports, and chart support NetFlow anomaly detection
Level 2	Access IP addresses and information added	Starts performing event and session-based correlation NAT and PAT resolution IP address lookup of attackers and targets
Level 3	Community strings and networks added	MAC address lookup of attackers and targets Topologies enabled

Selection of the Devices to Monitor

All monitoring strategies involve selecting the types of devices to monitor and how much data to provide the MARS Appliance. All devices on your network, be they hosts, gateways, security devices, or servers, provide some level of data that MARS can use to improve the accuracy of security incident identification. However, careful consideration of what data to provide can improve the attack identification response time by ensuring that MARS does not perform necessary or redundant event correlation and analysis. Unnecessary logging and reporting by reporting devices can also reduce the effectiveness of your network.

We recommend analyzing each network segment to identify the most data rich combination that you can achieve, while identifying and refining your configurations to reduce redundant data.

When determining a monitoring strategy, you must also determine the goals behind the monitoring. Is it just for attack detection? Attack detection and mitigation? Regulatory compliance? Your goals affect which devices you must monitor and what features you must configure on those devices.

Consider distinct goals:

- Attack detection

- Attack detection and mitigation
- Regulatory compliance
- Full NAC awareness
- Identify the devices/feature pairs that overlap on the same network segment, where a choice between device can reduce duplicity or prioritize device performance

Last, you must consider an event tuning method for your monitoring strategy. How you tune your MARS affects your overall operational costs proportionally to the number of device of a give type that are monitored. Essentially, if you have the bandwidth available, we recommend that you tune the events at the MARS Appliance, which reduces your operational costs by tuning at a single point in the network. However, if bandwidth is a precious commodity, you may chose to tune the event propagation at the reporting device level, preventing the events from going onto the network.

Table 3-2 identifies the device types, describes what information they can provide, and recommends how to configure these devices within your network.

Table 3-2 **Device Types and Data Available**

Device Type	Data Available	Recommended Configurations
Router	For routers and switches, administrative access is not required; MARS can obtained the information using an SNMP read-only community string. If SNMP read-only access is enabled and you want to perform mitigation, you are prompted to provide a SNMP read-write administrative password as a one-time password. The device discovery protocol is the one used for administrative access/mitigation. For example, if SSH is used to discover the device, then SSH is the protocol that used to pushed the mitigation command. The following data is pulled from routers: • hostname • static routes • ACL rules • static NAT rules • traffic flows • SNMP RO Community strings • NetFlow data • device status and resource utilization, such as memory, CPU, and interface/port statistics. • ARP cache table. Used to map IP address to MAC address.	Enable the following: • SNMP RO community strings • Syslog traffic • Device discovery via SSH or Telnet access

Table 3-2 **Device Types and Data Available (Continued)**

Switch	During investigation and mitigation, the ARP cache tables are reviewed to resolve the MAC addresses involved in the incident. This data is cached for 6 hours. SNMP RO Community strings Forwarding tables, used to map IP address to MAC address. Device status and resource utilization, such as memory, CPU, and interface/port statistics. NetFlow data 802.1x logs generated during NAC sessions	Enable the following: • SNMP RO community strings • Syslog traffic • Device discovery via SSH or Telnet access • Enable NetFlow data • Administrative access for mitigation push
Firewall	Interface configurations. Used to populate topology view and determine expected routes, which helps refine correlation of traffic traversing the firewall. NAT and PAT mappings. Used to identify the point of origin attackers and targets and trace attacks as they spread. Firewall policies. When discovering ASA, PIX, and FWSM, MARS parses ACLs and conduits (PIX only). For Check Point firewalls, it collects the firewall policy from policy table. MARS using this information only for path computation and mitigation recommendations. It is not used by any other components, such as rules, reports, and sessionization. Firewall logs. Accepted and denied sessions logs are used to identify false positives and determine if potential attacks were blocked before reaching their targets. Audit logs. Associates users with authentication sessions and assists in identifying exploited accounts and administrative sessions. ARP cache tables. Used to map IP address to MAC address. Device status and resource utilization information. Used to identify anomalous network activities based on memory, CPU, and interface and port statistics.	Enable the following: • SNMP RO community strings • Syslog messages • Device discovery

Table 3-2 **Device Types and Data Available (Continued)**

VPN	Remote user information. Provides username to IP address mapping. VPN client helps determine the person who logged in and performed specific actions. Clarifies the true point of origin by identifying the host, not the VPN concentrator. Login/logout records. Helps identifies worms by tracing outbreaks back to a specific user and provides network access periods. Device status information. Identifies whether the device is operational, which allows prediction of possible spread of potential attacks and worms. • SNMP RO Community strings	
Network IDS/IPS	Fired signature alerts. Identifies attacks and threats, which helps determine mitigation response, identify potential false positive information, and target vulnerability assessment probes conducted by MARS. Trigger packet information. Provides the payload of the packet that caused the signature to fire. Determine whether an attack was blocked at a specific device. Device status information	Enable the following: • Device discovery via SSH access • SDEE access
Host IDSes	Provides host-level validation of exploits and blocked attacks, which improves the accuracy of false positive identification, which in turn improves the ability of the administrator to accurately prioritize the work required to contain attacks.	
Anti-Virus	Central anti-virus management servers provide information on which hosts are infected, which hosts have reported attempted infections, etc. The servers also provide the dat or signature file information for managed hosts, which improves the ability to determine whether an attack was likely to have succeeded.	
Vulnerability Assessment	Host OS and Patch Level. When a signature fires on an IDS and it is reported to MARS, MARS can either launch a targeted scan using Nessus, or query a vulnerability assessment system that helps determine whether the target was vulnerable.	Enable any vulnerability assessment solutions supported by MARS.

Table 3-2 **Device Types and Data Available (Continued)**

Host OSes	Microsoft Windows Hosts Events found in the security event log as well application event and system event log.	Install and configure SNARE, which pushes events to MARS in near real time, and scales more efficiently than pulling events from hosts.
	Solaris and Linux Hosts Incoming network session logs, via inted, and FTP transfer logs, via xferlog. In addition, any events that are written to the system log by applications and services running on host.	• Enable logging for the xferlog and inetd applications. • Enable syslog daemon. • Identify the MARS Appliance as syslog target.
	Generic Hosts (All OSes) Includes system-level information, such as privilege escalation and buffer overflow. Helps determine what attacks make it to the host layer. If MARS learns of activity at the host level, then it understands that the attack or exploit has successfully traversed the network. MARS correlates this data with the network level data to discover the whole incident and analyze the exploit method so the administrator can build a better defense. In some cases, MARS recommends actions for mitigating the attack. We recommend that you maintain these recommended blocks as long as similar attacks are expected. Typical blocking techniques, such as IPS shunning, often fail to identify the best chokepoint for containment. As part of the recommended action, MARS does identify the optimal chokepoint where the recommended action should be effected.	
Web Server	Same as hosts (SNARE and Perl script agents) need this when the hosts cannot send us the logs via syslog. agent is basically a transport.	
Web Proxy	Mapping from user to site, translations for the IP address mapping, tells us the real address of the host who is likely infected. URLs and also filtering...regulatory compliance.	
Database	Login/logout to determine the actual user (query report tab on the data). Privilege escalation, brute force crack type stuff, or maybe we want to do regulatory compliance.	

Table 3-2 **Device Types and Data Available (Continued)**

AAA Server	Login/logout and NAC functionality (deny a person due to privileges, it triggers NAC message) • passed authentication log • failed attempts log • RADIUS accounting log, including those events specific to NAC.	System Events related to Authentication and Login Attempts, page 14-4
Generic Syslog	Same as host, provides support for additional customer devices.	
Generic SNMP	Same as host, provides support for additional customer devices.	
Cisco Security Manager	Mapping to any committed policy rules defined in Security Manager that match any ACL rules that could cause the generation of a specific syslog event by a reporting device. This policy lookup feature allows you to debug network issues and understand the cause/effect relationships between event messages and the device policies and traffic that resulted in the generation of the event.	Enable HTTPS on the Security Manager server. Define an administrative level account on the Security Manager server that CS-MARS can use for policy lookups.

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 3-8](#)
- [Reporting IP, page 3-8](#)
- [Interface Settings, page 3-9](#)

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 3-9](#).

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



Note

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

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

Reporting IP

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

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

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

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

Interface Settings

Interface settings are exclusive to hosts and software applications running on hosts. While MARS can discover the settings of a reporting device that is a software application running on a host, it cannot discover settings about the host itself. The role of interface settings in MARS is different from that 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 can use either SNMP v1 or SNMPv3 to perform device discovery. If you are using SNMPv1 and 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 3-10](#)
- [Configure Telnet Access for Devices in MARS, page 3-11](#)
- [Configure SSH Access for Devices in MARS, page 3-12](#)
- [Configure FTP Access for Devices in MARS, page 3-12](#)

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 SMPOv1 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** Select **SNMP** in the Access Type list, and specify the following values:
- **Login**—Enter the username of the administrative account to use when accessing the reporting device.
 - **Password**—Enter the password associated with the username specified in the Login field.
 - **Enable Password**—If this device supports an enable mode, enter that password.
- Step 2** Select either the **SNMP Version 1** or the **SNMP Version 3** radio button, and specify the appropriate values:

**Note**

MARS uses SNMPv1 or SNMPv3 to perform device discovery. If MARS cannot 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.

SNMP Version 1

- **SNMP RO Community**—The shared string used to identify which MIB the agent should use to report activities to the MARS Appliance.

SNMP Version 3**Note**

SNMPv3 is only supported for Cisco devices.

- **Security Name**—Identifies the user (principal) on whose behalf the message is being exchanged. If "no authentication" is selected, this name is used to authenticate MARS Appliance to the device's SNMP agent. The expected value is a string between 1 and 255 characters.
- **Security Level**—Identifies the level of security to perform on each SNMP packet. The options are "authentication and privacy", "authentication only no privacy," or "no authentication no privacy." No "no authentication no privacy" authenticates using the security name over cleartext.
- **Authentication Protocol**—Required when Security Level is either "authentication and privacy" or "authentication only no privacy." Provides authentication based on the HMAC-MD5 (128-bit encryption) or HMAC-SHA (160-bit encryption) algorithms. Select between MD5 and SHA.
- **Auth. Password**—The expected value is a string between 8 and 64 characters.
- **Privacy Protocol**—Required when Security Level is "authentication and privacy." Identifies the cipher to use when encrypting traffic between the management console and agent. Select between DES (64-bit encryption based on CBC-DES) and AES (128-bit encryption).
- **Priv. Password**—Required when Security Level is "authentication and privacy." The expected value is a string between 8 and 64 characters.
- **Context Name**—(Optional) Refers to a named subset of the MIB objects at an agent. Using a name subset can restrict Cisco Security Monitoring, Analysis, and Response System (MARS)'s access to the MIB. The expected value is a string between 1 and 255 characters.

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.

Operating Upon Reporting and Mitigating Devices

This section details operations you can perform on reporting and mitigating devices that have been added to the system.

**Note**

For detailed information on adding and configuring devices to MARS, see the [Configuring Reporting and Mitigation Devices in MARS](#) section of the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.

This section contains the following topics:

- [Edit a Device, page 3-13](#)
- [Upgrade the Device Type to a Newer Version, page 3-13](#)
- [Delete a Device, page 3-14](#)
- [Delete All Displayed Reporting Devices, page 3-15](#)
- [Verifying Connectivity with the Reporting and Mitigation Devices, page 3-15](#)
- [Activate the Reporting and Mitigation Devices, page 3-17](#)

Edit a Device

-
- Step 1** Select one of the following pages:
- Admin > Security and Monitoring Devices
 - Management > IP Management
- Step 2** Check the box next to the device.
- Step 3** Edit the device's settings.
- Step 4** Click **Submit**.
-

Upgrade the Device Type to a Newer Version

You can change the Device Type version setting of a hardware-based security device. You cannot upgrade the version for software applications running on a host. To upgrade the software appliance version, you must remove the application from the host and add the newer one.

This version change feature applies only to device types with the same vendor and model but different versions. Specifically, you can change the version for the following device types:

- Cisco IPS

- Cisco PIX
- Cisco VPN Concentrator
- NetScreen ScreenOS

For example, you could change the settings for the device type Cisco PIX 6.1 to Cisco PIX 7.0 without having to delete the device and add it again. The benefit of matching the version setting to the deployed device is that it allows MARS to correlate any event types introduced in the more recent version. It also allows you to incrementally upgrade your reporting devices without having to worry about when to add that reporting device to MARS. The events that are correlated under one device type will be associated with the newer device type version when you make the change in MARS.

To change the version of a device, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices**.
- Step 2** Select the check box to the left of the device for which you want to change the version, and click **Change Version**.
- The Change the Device Type Version page appears, displaying the device name, vendor, model, and old version type information.
- Step 3** Select the new version in the New Device Type Version list.
- Step 4** To change the version of the device to the new version, click **Submit**.
- If any additional changes are available due to the version change, the Edit page appears.
- Step 5** If the Edit page appears, make any desired changes and click **Submit**.
- Step 6** Once you change the version setting for 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 3-17](#).
-

Delete a Device

When you define a reporting device in MARS, this device is added in two separate pages of the web interface. It appears where you have defined it, on the Admin > Security and Monitoring Devices page, as well as under the general device identification page under Management > IP Management. This duplication of content is based on the different functions that each of these pages serves.

The Security and Monitoring Devices page configures the contact and device type information, whereas the IP Management page is used by the parser module to correlate known devices versus unknown devices. Typically when you delete a device from the Security and Monitoring Device page, you still want to retain the knowledge of that device in MARS so that historical incidents and events and cases can resolve to a known device; therefore, the device is not deleted from the IP Management page.



Note

Deleting a device does disassociate any historical incidents and events from the IP address. In other words, once you delete the device, you will not be able to find historical events for that device even if you re-add the device at a later date.

However, if you need to delete and re-add a device to MARS, you must delete the device from both pages before you attempt to re-add the device.

In addition, as devices are discovered on your network, they are added to the list of devices in the IP Management page. If you want to add a reporting device and find that you cannot, review the list of devices in the IP Management page to ensure that the device has not been auto-populated. If it has, you must first delete that device, then you can add it as a reporting device on the Security and Monitoring Devices page.

To delete a device, follow these steps:

-
- Step 1** Select one of the following pages:
- Admin > Security and Monitoring Devices
 - Management > IP Management
- Step 2** Check the box next to each device you want to delete.
- Step 3** Click **Delete**.
- Step 4** On the confirmation page, click **Submit**.
- The device is deleted from the selected page.
-

Delete All Displayed Reporting Devices

You can perform this procedure from the Admin > Security and Monitoring Devices page.

To delete all devices displayed on a page, follow these steps:

-
- Step 1** On the Admin > Security and Monitoring Devices, select the checkbox to the left of the Device Name column heading at the top left of the table.
- All displayed devices are selected.
- Step 2** Click **Delete**.
- A page appears prompting you to confirm that you want to delete the list of devices.
- Step 3** Click **Submit** to delete all the selected devices.
-

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 3-16](#), contains a list of devices that can be checked or discovered.

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

Run a Reporting Device Query

Another method to see the added devices, is to run a query with the display format: **Reporting Device Ranking**.



Note

You might not see all of the devices that you loaded using the seed file right away because of lag, network size and traffic. If you do not see a device after waiting, it could be due to input error.

To run a reporting device ranking query, follow these steps:

- Step 1** Click the **Queries / Reports** tab.
- Step 2** On the Queries page, in the Query Event Data table, click **Event Type** in the Display Format column.
- Step 3** Select **Reporting Device Ranking**.
- Step 4** Click **Apply**.
- Step 5** Click **Submit** to run the query.

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.

Data Enabling Features

Adding the reporting devices and mitigation devices is the primary method of providing MARS with the data required to study the activities on your network. However, other features, both within the web interface and as part of configuring the devices, can provide MARS with additional data, which is used to refine the views it provides and to assist in the improving the overall effectiveness of the system. We think of these features as data enabling features.

This section contains the following topics:

- [Layer 2 Discovery and Mitigation, page 3-18](#)

Enable SNMP community strings to support the discovery the network topology. Allows for mapping to the port level for switches. Combined with 802.1x support required by NAC, this setting can resolve MAC address level settings for attached and wireless nodes on the network.

- [Networks for Dynamic Vulnerability Scanning, page 3-19](#)

Enables a Nessus-based scan of the targeted hosts. Nessus also uses nmap for OS fingerprinting and port scanning during a vulnerability assessment scan. These scans are conducted in response to suspicious activity to determine whether the attempted attack is successful or likely to succeed based on information such as target operating system type, patch level, and open ports on the host.

- [Understanding NetFlow Anomaly Detection, page 3-20](#)

By enabling NetFlow, MARS can detect anomalies in traffic and network usage by comparing new events with summary data. When anomalies are detected, MARS begins to store full NetFlow data. By default, full NetFlow data is not stored by MARS unless an incident is identified.

- [Host and Device Identification and Detail Strategies, page 3-27](#)

Details about reporting devices and the hosts that are on your network aids in the elimination of false positives, as well as improves the performance of MARS in assessing events.

- [Discovering Your Network: Layer 3 Topology Discovery, page 3-27](#)

Layer 3 topology discovery aids in attack path analysis, as well as the population of the topology graph in the web interface.

- [Scheduling Topology Updates, page 3-31](#)

Topology update schedules are a critical part of many of the data enabling features, including discovery of Layer 2 and Layer 3 devices, as well as pulling information from specific reporting devices.

- [Configuring Resource Usage Data, page 3-34](#)

MARS can collect additional data from a select set of reporting devices, which is used to provide reports about CPU utilization, memory utilization, and device saturation. This data can be helpful in detecting anomalies as well in network capacity planning.

- [Configuring Network Admission Control Features, page 3-39](#)

Describes how to accomplish full NAC awareness, what it provides, and what products are required.

- [MARS MIB Format, page 3-44](#)

Describes the format of the MARS MIB, which helps integrate with other SNMP-based management applications on your network.

Layer 2 Discovery and Mitigation

Make sure that all the L2 devices have the SNMP RO (read only) community strings specified in the web interface for L2 mitigation, even if the access type is not SNMP. (See [False Positive Confirmation, page 9-7](#) for more information on mitigating an attack.)

The SNMP RO community string is *always* required on Layer 2 devices for L2 mitigation. L2 devices must be added manually—there is no automatic discovery for these device.



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).

MARS does not discover L2 devices automatically as it does with L3 devices.

**Note**

L2 devices must be added manually; there is no automatic discovery for these devices. Make sure all the L2 devices (switches) have the SNMP RO community strings specified in the web interface, even if the access type is not SNMP. The SNMP RO community string is always required on L2 devices for L2 mitigation.

You can specify which L3 devices to discover by specifying networks and SNMP RO community values, as defined in [Discovering Your Network: Layer 3 Topology Discovery](#), page 3-27.

The reason is MARS does not scan the network for devices. Therefore, you must manually add L2 devices using the web interface or a CSV file. Assuming that device discovery permission has been provided, L3 devices are discovered automatically using the route information provided by monitored gateways. Once devices are loaded/added in the web interface, user can use the topology scheduler feature to update the configuration of both L2 and L3.

For L2 devices SNMP access type is sufficient with RO community. But for mitigation, MARS requires SNMP RW community access. If SNMP RW community is not possible, select TELNET/SSH access type with SNMP RO Community.

Networks for Dynamic Vulnerability Scanning

With dynamic vulnerability scanning, the MARS probes the networks that you have specified for weaknesses. These automatic scans commence after a rule has fired that indicates an attack is in progress. Once an attack is underway, these scans accomplish the following:

- return information that determines if the attack failed
- return information that determines if the attack likely succeeded
- return false positive information
- assign severity to firing events and incidents

Select a Network for Scanning

To select a network for scanning, follow these steps:

-
Step 1	Click the Select radio button.
Step 2	Click a network to scan.
Step 3	Click Add.
Step 4	Repeat Step 1 through Step 3 .
Step 5	Click Submit when ready.
-

Create a Network IP Address for Scanning

To create a network address that you can use to define the scan settings, follow these steps:

-
Step 1	Click the Network IP radio button.
Step 2	Enter the Network IP address and Mask.

Step 3 Click **Add**.

Create a Network IP Range for Scanning

To create a range of network addresses that you can use to define the scan settings, follow these steps:

Step 1 Click the **IP Range** radio button.

Step 2 Enter the range of IP addresses.

Step 3 Click **Add**.

Understanding NetFlow Anomaly Detection

NetFlow is a Cisco technology that supports monitoring network traffic and is supported on all basic IOS images. NetFlow uses an UDP-based protocol to periodically report on flows seen by the Cisco IOS device. A *flow* is a Layer 7 concept that consists of a session set up, data transfer, and session teardown. For every flow, a NetFlow-enabled device record several flow parameters including

- Flow identifiers, specifically source and destination addresses, ports, and protocol
- Ingress and egress interfaces
- Packets exchanged
- Number of bytes transferred

Periodically, a collection of flows and its associated parameters are packaged in an UDP packet according to the NetFlow protocol and sent to any identified collection points. Because data about multiple flows is recorded in a single UDP packet, NetFlow is an efficient method of monitoring high volumes of traffic compared to traditional methods, including SYSLOG and SNMP.

The data provided by NetFlow packets is similar to that provided by SYSLOG, SNMP, or Checkpoint LEA as reported by enterprise-level firewalls, such as Cisco PIX, NetScreen ScreenOS, and Checkpoint Firewall-1. The difference being that NetFlow is much more efficient. To receive comparable syslog data from a firewall device, the syslog logging level on the firewall must be set to DEBUG, which degrades firewall throughput at moderate to high traffic loads.

If NetFlow-enabled reporting devices are positioned correctly within your network, you can use NetFlow to improve the performance of the MARS Appliance and your network devices, without sacrificing MARS's ability to detect attacks and anomalies. In fact, NetFlow data and firewall traffic logs are treated uniformly as they both represent traffic in the network.

This section contains the following topics:

- [How MARS Uses NetFlow Data, page 3-21](#)
- [Guidelines for Configuring NetFlow on Your Network, page 3-21](#)
- [Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 3-22](#)
- [Configuring Cisco CatIOS Switch, page 3-23](#)
- [Enable NetFlow Processing in MARS, page 3-23](#)

How MARS Uses NetFlow Data

When MARS is configured to work with NetFlow, you can take advantage of NetFlow's anomaly detection using statistical profiling, which can pinpoint day zero attacks like worm outbreaks. MARS uses NetFlow data to accomplish the following:

- Profile the network usage to determine a usage baseline
- Detect statistically significant anomalous behavior in comparison to the baseline
- Correlate anomalous behavior to attacks and other events reported by network IDS/IPS systems

After being inserted into a network, MARS studies the network usage for a full week, including the weekend, to determine the usage baseline. Once the baseline is determined, MARS switches to detection mode where it looks for statistically significant behavior, such as the current value exceeds the mean by 2 to 3 times the standard deviation.

By default, MARS does not store the NetFlow records in its database because of the high data volume. However, when anomalous behavior is detected, MARS does store the full NetFlow records for the anomalous entity (host or port). These records ensure that the full context of the security incident, such as the infected source and destination port, is available to the administrator. This approach to data collection provides the intelligence required by an administrator without affecting the performance of the MARS Appliance. Storing all NetFlow records consumes unnecessary CPU and disk resources.

MARS supports NetFlow versions 1, 5, 7 and 9, for MARS-supported routers and switches.

MARS supports a variant of NetFlow version 9, called NSEL (NetFlow Security Event Logging) for the ASA 8.1. NSEL uses NetFlow version 9 templates to customize the scope of the security information captured.

Guidelines for Configuring NetFlow on Your Network

NetFlow is most effective when collected from the core and distribution switches in your network. These switches, together with the NetFlow from Internet-facing routers or SYSLOG from firewalls, typically represent the entire network. With this in mind, review the following guidelines before deploying NetFlow in your network:

- MARS normalizes NetFlow and SYSLOG events to prevent duplicate event reporting from the same reporting device.
- Review VLANS in switches and pick several VLANs for which the traffic volume is low. This approach allows you to slowly integrate NetFlow and become comfortable with using it in your environment.
- Be aware of existing CPU utilization on NetFlow capable devices. For more information on understanding how NetFlow affects the performance of routers and network throughput, see the following link white paper: [NetFlow Performance Analysis](#).
- Consider using a sampling of NetFlow data 10:1 100:1 ratio's in highly utilized VLANs.
- Be selective in using NetFlow, you do not need to enable it on all NetFlow-capable devices. In fact, such usage can create duplicate reporting of events, further burdening the MARS Appliance.
- Ensure that the version of Cisco IOS software or Cisco CatOS running on your reporting devices supports at least one of these NetFlow versions.

The taskflow for configuring NetFlow to work with MARS is as follows:

1. Identify the reporting devices on which to enable NetFlow.
2. Enable NetFlow on each identified reporting device and direct the NetFlow data to the MARS Appliance responsible for that network segment.

3. Verify that all reporting devices are defined in the MARS web interface.
4. Enable NetFlow processing in the MARS web interface.
5. Allow MARS to study traffic for a week to develop a usage baseline before it begins to generate incidents based on detected anomalies.

The following tasks provide guidance on the required device configuration:

- [Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 3-22](#)
- [Enable NetFlow Processing in MARS, page 3-23](#)
- [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#)

Enable Cisco IOS Routers and Switches to Send NetFlow to MARS

For more information on NetFlow and configuring the settings in Cisco IOS, refer to:

[NetflowConfiguration Guides](#)

Before you configure NetFlow from MARS, you must first configure it on the router or switch.

To enable NetFlow on a Cisco IOS router or switch and to push those events to the MARS Appliance, follow these steps:

Step 1 Log in to the Cisco IOS router or switch with administrator's privileges.

Step 2 Enter the following commands:

Command	Purpose
enable	Turn on enable mode.
configure terminal	Enter global configuration mode. Note Commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).
ip flow-export destination <MARS_IP_address> <UDP_port>	Enables the data export to the MARS Appliance on UDP port 2055 (assuming the default port is used). <i>MARS_IP_address</i> is the IP address of the MARS Appliance that is responsible for processing the NetFlow events for this reporting device. <i>UDP_port</i> is the default UDP port to send NetFlow (the default port is 2055).
ip flow-export source <syslog_interface_name>	Set the source IP for the interface to send the NetFlow. The <i>syslog_interface_name</i> value should be the interface attached to the network through which the MARS Appliance is reachable, and it must equal the syslog source interface name.
ip flow-export version <version_number>	Identifies which version of NetFlow, 5 or 7, to use when generating events.
ip flow-cache timeout active 5	Configures the flow timeout. This timeout value breaks up long-lived flows into 5-minute segments. You can choose any number of minutes between 1 and 60; however, selecting the default of 30 minutes will result in spikes appearing in utilization reports.
ip flow-cache timeout inactive 15	Ensures that those flows that have finished are exported in a timely manner.

Step 3 For each interface in the device, enter the following commands:

Command	Purpose
interface <interface_name>	Specifies the interface for which you want to enable NetFlow and it enters the interface configuration mode. <i>interface_name</i> is the name of the interface to which the MARS is connected. This command varies based on the device type. For example, interface type slot/port-adapter/port (Cisco 7500 series routers) interface type slot/port (Cisco 7200 series routers)
ip route-cache flow	Enables NetFlow for the selected interface.

Step 4 To verify that NetFlow is enabled correctly, enter the following commands:

show ip flow export show ip cache flow

Step 5 To exit enable mode, enter the following command:

exit

Configuring Cisco CatIOS Switch

Some Cisco Catalyst switches support a different implementation of NetFlow that is performed on the supervisor. With the cache-based forwarding model, which is implemented in the Catalyst 55xx running the Route Switch Module (RSM) and NetFlow Feature Card (NFFC), the RSM processes the first flow and the remaining packets in the flow are forwarded by the Supervisor. This support is also implemented in the early versions of the 65xx with MSFC. The deterministic forwarding model used in the 65xx with MSFC2 do not use NetFlow to determine the forwarding path, the flow cache is only used for statistics as in the current IOS implementations. In all of these configurations, flow exports arrive from both the RSM/MSFC and the Supervisor engines as distinct streams.

The router-side running IOS is configured as specified in [Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 3-22](#). However, to configure the he CatIOS NetFlow Data Export, use the following commands:

set mls flow full

set mls nde version 5

set mls nde <MARS_IP_address> 2055

set mls nde enable

From a user's perspective, the switch is only running IOS when the 65xx is running in Native mode.

Enable NetFlow Processing in MARS

Once you have enabled NetFlow on your routers, switches, or Cisco ASAs, and you have directed those devices to publish NetFlow data to the MARS Appliance, you must configure the appliance to process that data. This configuration involves determining how to store data, as well as identifying which networks you want to process for anomalous behavior. Both of these options can affect the rate at which MARS can process events: storing the full event data rather than summary data burdens the system with writing large volumes of data rather than processing new incoming events. Also, by not specifying a select set of networks, MARS studies all networks.

- Step 1** Navigate to Admin > System Setup > NetFlow Config Info. The NetFlow configuration page appears, as shown in the following figure.

Figure 3-1 NetFlow Configuration Page (Admin > System Setup > NetFlow Config Info)

The screenshot shows the NetFlow Configuration page. At the top, there is a navigation bar with tabs: System Setup, System Maintenance, User Management, System Parameters, and Custom Setup. Below the navigation bar is a header with the Cisco logo and a 'SUMMARY' button. The main content area is titled 'NetFlow Configuration' and contains a form with the following fields:

- Global NetFlow UDP Port: 2055
- Enable NetFlow Processing: Yes (selected)
- Always Store IOS NetFlow Records: No (selected)
- Always Store ASA Netflow Security Event Logs: No (selected)
- Turn on IOS Netflow Verbose Raw Messages: No (selected)

- Step 2** Under **NetFlow Configuration**, enter the NetFlow **Global NetFlow UDP Port**. This is the default port for MARS to listen for NetFlow; the default value is 2055.



Note This value must match the value you entered in the “ip flow-export destination” command when configuring the router (see [Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 3-22](#)). Also, verify you have enabled this traffic to flow between the router or switch and the MARS Appliance on any intermediate gateways, such as routers and firewalls.

- Step 3** Choose whether to **Enable NetFlow Processing**.
- **Yes** tells MARS to process the NetFlow logs.
 - **No** disables the processing of NetFlow data into the MARS.
- Step 4** Choose whether to **Always Store IOS NetFlow Records (Routers and Switches only)**.
- **Yes** tells MARS to store all of the IOS NetFlow events in the database. Selecting this option can slow down the system by greatly decreasing the number of events per second that MARS is able to process.
 - **No** tells MARS to store only anomalies. The 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

Step 5 Configure Always Store ASA Netflow Security Event Logs (Cisco ASA only).

- **Yes**—MARS will 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
 - Retrieval 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. The 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.

Selecting 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 6 Configure **Turn on IOS NetFlow Verbose Raw Messages**.

- **Yes**—IOS NetFlow raw messages contain the full five tuple information in addition to their own fields in the MARS database.
- **No**(default)—IOS NetFlow raw messages contain only byte and packet count for the flow. The five tuple info is present in its own DB fields and can be queried.



Note

Prior to MARS Release 6.0.1, the default was Yes. All IOS NetFlow (v5/v7) raw messages contained the full five tuple in addition to being in their own database fields.



Note

This setting does not affect Cisco ASA NSEL logs.

Step 7 Click **Submit** to save your changes.

Step 8 Navigate to Admin > System Setup > Networks for Traffic Anomaly Detection.

Figure 3-2 *Networks for Traffic Anomaly Detection Page (Admin > System Setup > Networks for Traffic Anomaly Detection)*



Configure Networks for Diagnosing Traffic Anomalies

- Step 9** In the Configure Networks for Diagnosing Traffic Anomalies window, you can enter one or more of the addresses for networks you want to monitor and use the Add button to add them.



Tip

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 10** Click **Submit** to save your changes.
- Step 11** To enable NetFlow processing by the MARS Appliance, click **Activate**.



Tip

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 12** Verify NetFlow configuration by observing raw messages with the MARS real-time event viewer. (For more information see [Viewing Events in Real-time, page 8-22.](#))

Host and Device Identification and Detail Strategies

MARS studies many events at the network layer, relying on firewalls, routers, and IPS devices to identify anomalies and suspected incidents at a layer above the endpoint hosts that are the source or destination of network sessions. If operating exclusively at this network layer, MARS can generate a number of false positive incidents that must be manually investigated. However, several features exist that allow you to provide host-level details to MARS:

- Enable event reporting from the hosts on your network. MARS can receive, and in some cases, pull event data directly from the hosts on your network. This additional data allows MARS to verify the success of some attacks, as well as to report issues with the operation of the host, such as including them in “device down” reports if they are inaccessible.
- Manually identify the operating system type and network services running on discovered hosts.
- Manually identify common hosts and nodes in your network by adding other devices via Management > IP Management. This additional data allows you to identify those hosts that are likely to be involved in network sessions without having to configure the hosts to provide event data directly to MARS. This open allows you to provide vulnerability assessment information to assist in the reduction of false positives. For more information on adding hosts manually, see [Add a Host to a Local Controller, page 6-5](#).

Discovering Your Network: Layer 3 Topology Discovery

For MARS to reach full operability, you must specify the Simple Network Management Protocol (SNMP) discovery settings and identify which networks to discover. There are many advantages to discovering your network, including identifying Cisco routers and gateways that can act as mitigation devices and providing a more complete topology graph on the Dashboard page that enables a more accurate attack path analysis. Once the appliance discovers these networks, MARS offers 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, page 3-1](#) for more information.

SNMP is a network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. Beginning in 6.0.6, MARS supports SNMP version 3.0 (SNMPv3) for Cisco devices, which enables authentication of the manager node (MARS Appliance) by the agent (monitored device) as well as encryption between the two nodes. SNMPv1, available in releases before 6.0.6, is only valid in read-only environments—reading MIB data maintained by the agent. Even in a read-only environment, the data is passed in cleartext. However, SNMPv3 can exist in a network control environment because it supports authenticating the manager before writing to the MIB. SNMPv3 includes three key services: authentication, privacy, and access control.

In MARS, SNMPv3 support enables the following features:

- Per-device SNMPv3 credentials are used for manual discovery and layer 2 mitigation.

**Note**

For those devices that support SNMPv3, you can now configure SNMP credentials in either the version 1 or version 3 format. For older devices, you do not see the new configuration options.

- Support for SNMPv3 credentials for an entire network or range of IP addresses. The MARS autodiscovery feature clones the credentials for an autodiscovered device on that network.

- Monitor the health of supported devices via SNMPv3 using the resource utilization charts that you can add to the **Summary > My Reports** subtab.

**Note**

SNMPv3 is only supported for Cisco devices.

To view the topologies, select the **Summary > Dashboard** page in the web interface.

**Note**

Remember to activate additions and changes to your SNMP configuration settings 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 access to layer 3 devices is required. You can choose between SNMPv1 read only access via an SNMP RO community string or various SNMPv3 access options. You can also refine the discovery parameters to ensure that you do not discover your ISP's network (**Admin > System Setup > Valid Networks**).

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

- A device, such as a firewall, that blocks SNMP access to itself or a network segment.
- You have listed the networks to discover (under **Admin > System Setup > Community Strings and Networks**) and a network segment is identified but it does not appear in the network discovery list (under **Admin > System Setup > Topology/Monitored Device Update Scheduler**).

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 Cisco works format.

Define SNMP Discovery Settings for a Network or IP Range

Once you have identified networks and their associated SNMP community string or authentication information, MARS can discover networks, devices, and interfaces within those networks and IP ranges. This type of discovery improves the topology population and helps identify new mitigation points on your network.

To define the SNMP discovery settings for a network address or IP range, follow these steps:

-
- Step 1** Click **Admin > Community Strings and Networks** in the Topology Discovery Information box.

Community Strings and Networks

Step 2 Do one of the following:

- Click the **Network** radio button, and specify the IP and Mask values.
- Click the **IP Range** radio button, and specify the start and end IP addresses of the range.

Step 3 Click either the **SNMP Version 1** or the **SNMP Version 3** radio button, and specify the appropriate values:

SNMP Version 1

- **SNMP RO Community**—The shared string used to identify which MIB the agent should use to report activities to the MARS Appliance.

SNMP Version 3



Note SNMPv3 is only supported for Cisco devices.

- **Security Name**—Identifies the user (principal) on whose behalf the message is being exchanged. If "no authentication" is selected, this name is used to authenticate MARS Appliance to the device's SNMP agent. The expected value is a string between 1 and 255 characters.
- **Security Level**—Identifies the level of security to perform on each SNMP packet. The options are "authentication and privacy", "authentication only no privacy," or "no authentication no privacy." No "no authentication no privacy" authenticates using the security name over cleartext.
- **Authentication Protocol**—Required when Security Level is either "authentication and privacy" or "authentication only no privacy." Provides authentication based on the HMAC-MD5 (128-bit encryption) or HMAC-SHA (160-bit encryption) algorithms. Select between MD5 and SHA.
- **Auth. Password**—The expected value is a string between 8 and 64 characters.
- **Privacy Protocol**—Required when Security Level is "authentication and privacy." Identifies the cipher to use when encrypting traffic between the management console and agent. Select between DES (64-bit encryption based on CBC-DES) and AES (128-bit encryption).
- **Priv. Password**—Required when Security Level is "authentication and privacy." The expected value is a string between 8 and 64 characters.

- **Context Name**—(Optional) Refers to a named subset of the MIB objects at an agent. Using a name subset can restrict MARS's access to the MIB. The expected value is a string between 1 and 255 characters.

Step 4 Click **Add**.



Note To edit an entry, select that entry on the left. The fields at the right will populate. Make your changes and click **Update**.

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 Valid Networks to Discovery List

MARS uses SNMP to discover your layer 3 network devices. Beginning with a provided SNMP target, MARS discovers that target's layer 3 neighbors and then uses each neighbor as a new starting point to discover its neighboring devices and so on. Only SNMP read access (RO) is required. 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 > System Setup > Valid Networks** to open the Valid Networks page.

Step 2 Specify values for the following field:

- **SNMP Target**—The IP address of the SNMP target, which is the entry-point where the MARS starts discovering devices on a network. The target typically identifies an address of a default gateway, such as a Cisco Router or a firewall, on the network.

Step 3 (Optional) To restrict the scope of the scan for the given target, do one of the following:

- Click the **Network** radio button, and specify the IP address and Mask values of the network. MARS restricts its scan to Layer 3 neighbors belonging to the specified network.
- Click the **IP Range** radio button, and specify the start and end IP addresses of the range. MARS restricts its scan to Layer 3 neighbors with IP addresses within specified range.

Step 4 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 3-31](#). 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

Scheduled topology updates inform MARS about the hosts on the network, providing details such as IP addresses, operating systems, open ports, and applications running on the hosts. MARS uses this information to populate the cloud segments of its topology with host addresses and determine probable vulnerabilities relative to detected attacks. The scheduled updates also pull event information from reporting devices and via its built-in NMAP process.

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, SSH or SNMP, 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 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 modules or virtualization, 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 of devices that require such polling are the following:

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

Figure 3-3 Example Scheduled Update for eEye REM

Name:

10.1.1.86/255.255.255.255

☐ Select:
☐ Network IP:
Mask:
☐ IP Range:

Schedule	Time of Day	Days
☒ Run On Demand Only		
☐ Daily	12:00 Midnight	
☐ Weekly	12:00 Midnight	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
☐ Monthly	12:00 Midnight	☐ 1st ☐ 2nd ☐ 3rd ☐ 4th ☐ 5th ☐ 6th ☐ 7th ☐ 8th ☐ 9th ☐ 10th ☐ 11th ☐ 12th ☐ 13th ☐ 14th ☐ 15th ☐ 16th ☐ 17th ☐ 18th ☐ 19th ☐ 20th ☐ 21st

143360

Depending on the device being discovered, MARS selects from the following management information bases (MIBs) to discover the device's settings:

- mib-2(1) .System
- mib-2(1) .Interface.iftable
- mib-2(1) .ip.iproutetable
- mib-2(1) .ip.ipaddrTable
- mib-2(1) .ip.forwarding
- mib-2(1) .At.attable (for ARP info)
- mib-2(1) .dot1dBridge(17)
- vtpVlanState EMIB

Schedule a Network Discovery

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

- Step 1** Click **Admin > System Setup > 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** To select or enter your networks, do one of the following:
 - 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.

**Tip**

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

Step 6 In the schedule table, click 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 3-3 *Troubleshooting Discovery Issues*

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

Configuring Resource Usage Data

By monitoring and reporting on available device usage parameters, MARS can inform you of device health status and any abnormal conditions a device may be encountering.

Although the Monitor Resource Usage box appears on every host and reporting device, only some device types actually provide resource usage data to MARS. The nature and extent of the data provided is shown in [Table 3-4 on page 3-34](#).

Table 3-4 *Device Anomaly Resource Monitoring*

Vendor, Model, Description	CPU	Memory	Connection	Interface
Cisco IOS routers running 12.2, 12.3, 12.4	Yes	Yes	No	Yes
Cisco IOS switches running 12.2	Yes	Yes	No	Yes
Cisco PIX 6.0, 6.1, 6.2, 6.3, 7.0, 8.x	Yes	Yes	Yes	Yes ¹
Cisco ASA 7.0, 7.2, 8.0, 8.1, 8.2	Yes	Yes	Yes	Yes ¹
Cisco FWSM 2.2, 2.3, 3.1, 3.2	Yes	Yes	Yes	Yes ¹
Check Point OPSEC NG FP3, NG AI, NGX	No	No	Yes	No

¹For FWSM, ASA, and PIX 7.X and onwards, 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.

For these 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 Object Identifiers (OIDs):

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

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

The following resource usage data reports are available:

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

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

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

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

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

Enabling the Required SNMP OIDs for Resource Monitoring

Table 3-5 on page 3-36 lists the OIDs to enable, on a per device basis, for the supported model and versions.

Table 3-5 *SNMP OIDs Required for Resource Monitoring*

Vendor, Model, and Version	OID Descriptor	OID ¹
Cisco IOS 12.2, Cisco IOS 12.3, Cisco IOS 12.4	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 3-5 *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
PIX 6.2, 6.3, 7.0, 7.2, 8.0, , 8.1, 8.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.3.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_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 3-5 *SNMP OIDs Required for Resource Monitoring (Continued)*

ASA 7.0, 7.2, 8.0	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_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 3-5 *SNMP OIDs Required for Resource Monitoring (Continued)*

FWSM 2.2, 2.3, 3.1, 3.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.3.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_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
CheckPoint OpSec NG FP3, NG AI, NGX	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

¹For OIDs ending with '.i', the 'i' represents a variable interface number. Based on the total number of interfaces for that device, device_monitor replaces the 'i' with each interface number and queries the device separately for that interface.

Configuring Network Admission Control Features

Network Admission Control (NAC) is a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

MARS supports the NAC initiative by storing and reporting about the NAC-based events generated by the various reporting devices on your network. The devices include:

- Cisco Trust Agent. While CTA does not report to MARS, it does report discovered settings to the Cisco network devices, from which MARS collects events.
- 3rd-party 802.1x Supplicants.

- Cisco IOS routers running Cisco IOS Software, Release 12.3(8)T with security.
- Cisco VPN 3000 Concentrators
- Cisco Secure ACS
- Cisco Security Agent

To enable NAC reporting on your network, you must ensure that the NAC-specific events are logged by the reporting devices, 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.

The following reports are available to support NAC:

- Activity: AAA Failed Auth - All Events (Total View)
- Activity: AAA Failed Auth - Top NADs (Total View)
- Activity: AAA Failed Auth - Top Users (Total View)
- Activity: Security Posture: Healthy - Top Users (Total View)
- Activity: Security Posture: NAC - Top NADs (Total View)
- Activity: Security Posture: NAC - Top NADs and Tokens (Total View)
- Activity: Security Posture: NAC - Top Tokens (Total View)
- Activity: Security Posture: NAC Agentless - Top Hosts (Total View)
- Activity: Security Posture: NAC Agentless - Top NADs (Total View)
- Activity: Security Posture: NAC Agentless - Top Tokens (Total View)
- Activity: Security Posture: NAC Audit Server Issues - All Events (Total View)
- Activity: Security Posture: NAC End Host Details - All Events (Total View)
- Activity: Security Posture: NAC Infected/Quarantine - All Events (Total View)
- Activity: Security Posture: NAC Infected/Quarantine - Top Hosts (Total View)
- Activity: Security Posture: NAC L2 802.1x - Top Tokens (Total View)
- Activity: Security Posture: NAC L2IP - Top Tokens (Total View)
- Activity: Security Posture: NAC Static Auth - Top Hosts (Total View)
- Activity: Security Posture: NAC Static Auth - Top NADs (Total View)
- Activity: Security Posture: NAC Static Query Failure - Top Hosts (Total View)
- Activity: Security Posture: Not Healthy - All Events (Total View)
- Activity: Vulnerable Host Found (Total View)
- Activity: Vulnerable Host Found via VA Scanner (Total View)

The following system rules are available to support NAC:

- System Rule: Security Posture: Audit Server Issue - Network Wide
- System Rule: Security Posture: Audit Server Issue - Single Host
- System Rule: Security Posture: Excessive NAC Status Query Failures - Network Wide
- System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host
- System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD
- System Rule: Security Posture: Infected - Network Wide
- System Rule: Security Posture: Infected - Single Host

- System Rule: Security Posture: Quarantine - Network Wide
- System Rule: Security Posture: Quarantine - Single Host
- System Rule: Security Posture: Vulnerable Host Found

Integrating MARS with 3rd-Party Applications

MARS provides multiple integration methods with 3rd -party applications. The following topics describe how to integrate using these methods:

This section contains the following topics:

- [Forwarding Alert Data to 3rd -Party Syslog and SNMP Servers, page 3-41](#)
- [Syslog Relay Support, page 3-41](#)
- [MARS MIB Format, page 3-44](#)
- [Relaying Syslog Messages from 3rd-Party Syslog Servers, page 3-45](#)

Forwarding Alert Data to 3rd -Party Syslog and SNMP Servers

You can forward alert data from MARS to third-party syslog and SNMP servers. The data is forwarded on a per rule basis. In other words, you must configure those rules for which you want to forward alert data to include either SNMP, syslog, or both as notification methods. When a rule fires, the notifications will be sent in the selected formats to the specified recipients, which should be the desired servers in the case of SNMP and syslog.

For more information on configuring notification methods for a rule, see [Setting Alerts, page 4-21](#). To learn more about the SNMP MIB format sent by MARS, see [MARS MIB Format, page 3-44](#).

Syslog Relay Support

MARS can act as a relay for the syslog messages received from reporting devices to a single collector.

- A *reporting device* is a source host that generates a syslog message and sends that message to a Local Controller.
- A *relay* is a Local Controller that receives a syslog message from a reporting device and forwards it to a collector.
- A *collector* is a host that receives a syslog message, but the collector does not relay it to another host.



Note

This feature is not supported on Global Controller models.

The Local Controller can now act as a relay; it processes the incoming syslog messages locally before it forwards them to the designated collector. The destination port number is 514 for incoming and relayed syslog messages. MARS adheres to *RFC 3164: The BSD syslog Protocol* while relaying the syslog messages with the following exceptions:

- MARS can only forward to a single collector IP address.

- Because MARS supports exactly one collector, you cannot specify that events originating from one device address be forwarded to one collector while those originating from a different device address are forwarded to a different collector. All events are forwarded to the same collector.
- Forwarded syslog can be up to 1024 bytes in length. Logs longer than 1024 bytes are truncated.

**Note**

Using this feature, you can daisy chain Local Controllers. Configure the first Local Controller to forward to the second. In the web interface of the second Local Controller, identify the first Local Controller as **Generic Syslog Relay Any** in the Security and Monitoring Devices list. This configuration mirrors the data on both appliances.

The Local Controller generates internal events for the dropped packets, and it does not relay internal system and operating system event logs. Dropped packets result when one of the following condition exist:

- the forward queue is full
- a reporting device is down
- the collector is down.

You configure the syslog relay feature using the MARS CLI interface; no web interface exists to configure these settings. The configuration process is summarized as follows:

1. Access the MARS console.
2. Define the collector.
3. Define the list of devices for which events should be forward.
4. If you chose to select the ANY option, define the list of devices you want to exclude.

**Note**

Syslog forwarding is disabled until you specify the collector and at least one source host.

To configure and use this feature, see the following topics:

- [Enable the Syslog Relay Feature, page 3-42](#)
- [Disable the Syslog Relay Feature, page 3-43](#)
- [MARS Events, System Rule, and Report Details for the Syslog Relay Feature, page 3-43](#)
- [Troubleshooting the Syslog Forwarding Feature, page 3-44](#)

For more information on using the syslog relay feature, see the following commands in the [Cisco Security MARS Command Reference, 6.X](#):

- `syslogrelay setcollector`
- `syslogrelay src`
- `syslogrelay list`

Enable the Syslog Relay Feature

To enable the relay forward, follow these steps:

- Step 1** Log in to the Local Controller that will act as the relay. For more information, see "Log In to the Appliance via the Console" in the [Administering the MARS Appliance](#) chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*.

- Step 2** At the [pnadmin]\$ prompt, enter **syslogrelay setcollector *ip_address*** , where *ip_address* is the IP address value for the host to which you want to forward the syslog messages that this MARS Appliance receives from reporting devices.
- The the [pnadmin]\$ prompt returns. To verify the address, enter **syslogrelay list collector**.
- Step 3** At the [pnadmin]\$ prompt, enter one of the following commands:
- **syslogrelay src include *ip_address*** , where *ip_address* is one or more IP addresses that represent the reporting devices for which syslog messages should be forwarded to the collector.
 - **syslogrelay src include ANY** to specify that MARS should forward the syslog messages for all reporting devices that do not appear in the exclude list.
- If you use ANY, then you may define an exclude list using **syslogrelay src exclude *ip_address***, where *ip_address* is one or more IP addresses that represent the reporting devices for which syslog messages should not be forwarded.
- Step 4** To verify your settings, enter **syslogrelay list all**.
-

Disable the Syslog Relay Feature

You can disable the syslog relay feature using either of two approaches:

- Clear the list of syslog relay sources
- Clear the syslog collector address

To disable the relay forward feature, follow these steps:

- Step 1** Log in to the Local Controller that will act as the relay. For more information, see "Log In to the Appliance via the Console" in the [Administering the MARS Appliance](#) chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*.
- Step 2** At the [pnadmin]\$ prompt, enter one of the following commands:
- **syslogrelay src reset**
This the list of syslog relay sources so that messages are forwarded.
 - **syslogrelay unsetcollector *ip_address***, where *ip_address* is the IP address value for the collector to which syslog messages are currently forwarded.
- Step 3** To verify your settings, enter **syslogrelay list all**.
-

MARS Events, System Rule, and Report Details for the Syslog Relay Feature

Two internal events are defined in the Info/HighUsage/CS-MARS event group in support or this feature:

- MARS-2-100026: MARS Dropped Syslog Relay Event Since Capacity is Reached - First Event in the Hour
- MARS-2-100027: MARS Dropped Syslog to be Relayed Event Since Capacity is Reached - Drop Count in the Hour

The System Rule: Resource Issue: CS-MARS rule includes the MARS-2-100026 event. The Resource Issues: CS-MARS - All Events system report, which includes the Info/HighUsage/CS-MARS event group, summarizes data for the new event types.

Troubleshooting the Syslog Forwarding Feature

The following techniques can assist you in troubleshooting the syslog forwarding feature:

- If incoming syslog messages that should be forwarded are not being forwarded, verify the `pnparser` service is running on the Local Controller.
- If `pnparser` is having problems, you can use the `pnstop` and then `pnstart` command to restart the processes.

```
[pnadmin]$ pnstatus
Module State                Uptime
...
pnesloader RUNNING 3-16:18:29
pnmac RUNNING 3-16:18:29
pnparser RUNNING 3-16:18:23
process_event_srv RUNNING 3-16:18:28
process_inlinerep_srv RUNNING 3-16:18:28
process_postfire_srv RUNNING 3-16:18:28
process_query_srv RUNNING 3-16:18:29
superV RUNNING 3-16:18:30
```

- At least one source and one destination must be configured to enable syslog forwarding. Use the `syslogrelay list` command to verify the configuration.
- Source devices must send syslog message to destination port 514 on the Local Controller. Use the `tcpdump` command on the Local Controller to verify the configuration:

```
[pnadmin]$ tcpdump src host 192.168.3.2 and dst host 192.168.3.4 and udp dst port 514
```

where 192.168.3.4 is the IP address of the Local Controller and 192.168.3.2 is configured as a syslog source.

- MARS forwards syslog message to destination port 514 only. Use `tcpdump` command on the syslog collector (192.168.1.1) to verify the configuration

```
tcpdump src host 192.168.3.4 and dst host 192.168.1.1 and udp dst port 514
```

where 192.168.3.4 is the Local Controller and 192.168.1.1 is configured as the syslog collector.

MARS MIB Format

The MARS management information base (MIB) is defined for all MARS releases. The SNMP notification contains the same content as the syslog generated by MARS. The MARS private enterprise number is 16686. All “Top 3” categories display x of y occurrences. where x can be 1 to 3, and y can be 1 to n. The “Count” is the always the count of the firing events that match the rule criteria. The Rule ID number is for internal use only, it has no correspondence to any rule attribute viewable from the MARS GUI or CLI.

The MARS MIB definitions are as follows:

```
enterprises.16686.1.0 string "MARS-1-101"
enterprises.16686.2.0 string "<alert_content>"
enterprises.16686.3.0 string "<optional_port_list_for_sudden_traffic_increase_incident>"
enterprises.16686.4.0 string "<Top 3 src-dest address pairs>"
enterprises.16686.5.0 string "<Top 3 dest TCP/UDP ports>"
enterprises.16686.6.0 string "<Top 3 event types>"
enterprises.16686.7.0 string "<Top 3 reporting devices>"
```

alert_content: <<priorityInfo>> current_time %MARS-1-101: Rule ruleid (<rulename>) fired and caused color Incident incidentId , starting from start_time to end_time

Optional_port_list_for_sudden_traffic_increase_incident: TBD

Top 3 src-dest address pairs:

Top 3 src-dest address pairs sorted by severity and count showing x of y, src_IP -> dest_IP Severity: color Count: count

Top 3 dest TCP/UDP ports:

Top 3 TCP/UDP Ports sorted by severity and count showing x of y, dest_port Severity: color Count: count

Top 3 event types:

Top 3 event types sorted by severity and count showing x of y, Severity: severity Count: count

Top 3 reporting devices:

Top 3 reporting devices sorted by count showing x of y, reporting_device_name Count: count.

In the following two examples of the SNMP notification output, 10.1.1.1 is the IP address of the MARS Appliance:

```
SNMPv2-SMI::enterprises.16686 10.1.1.1 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
SNMPv2-SMI::enterprises.16686.2.0 "<34>Mon Apr 28 20:11:43 2003 %MARS-1-101: Rule 45513
(Nimda Attack) fired and caused red Incident 12265001, starting from Mon Apr 28 19:58:47
2003 to Mon Apr 28 20:11:21 2003"

SNMPv2-SMI::enterprises.16686 10.1.1.1 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
SNMPv2-SMI::enterprises.16686.2.0 "<34>Wed Feb 4 14:44:09 2009 %MARS-1-101: Rule 306498
(any) fired and caused green Incident 287020054, starting from Wed Feb 4 14:43:15 2009 to
Wed Feb 4 14:43:19 2009 on gVaAdGOCE"
SNMPv2-SMI::enterprises.16686.4.0 "Top 3 src-dest
address pairs sorted by severity and count showing 3 of 6, N/A -> N/A Severity: green
Count: 4, 10.4.11.10 -> 10.1.1.16 Severity: green Count: 1, 10.4.11.10 -> 10.1.1.17
Severity: green Count: 1"
SNMPv2-SMI::enterprises.16686.5.0 "Top 3 dest TCP/UDP Ports
sorted by severity and count showing 3 of 4, 21 Severity: green Count: 1, 22 Severity:
green Count: 1, 23 Severity: green Count: 1"
SNMPv2-SMI::enterprises.16686.6.0 "Top 3
event types sorted by severity and count showing 3 of 3, Built/teardown/permitted IP
connection Severity: green Count: 4, Unknown Device Event Type Severity: green Count: 4,
CS-MARS Miscellaneous authentication message Severity: green Count: 1"
SNMPv2-SMI::enterprises.16686.7.0 "Top 3 reporting devices sorted by count showing 3 of
6, gq_2 Count: 4, d1_1 Count: 1, d1_3 Count: 1"
```



Note

Notifications are sent only from the Local Controller.

Relaying Syslog Messages from 3rd-Party Syslog Servers

You can rapidly deploy MARS by forwarding messages from existing syslog-ng or Kiwi syslog servers. This feature eliminates the network and device changes required to insert MARS into an operational network. You are no longer required to configure each network device to publish its syslog messages directly to MARS, which saves time, avoids device change approval processes, preserves packet processing performance of the network devices, and ensures daily network operations proceed without interruption. This relay feature also allows the correlation and inspection of syslog messages from reporting devices, such as those on the DMZ, for which corporate policies might prohibit the existence of or connection to configuration information.

If your network devices already publish syslog messages to syslog-ng or Kiwi syslog servers, you can configure those servers to forward messages to the MARS Appliance and identify the syslog servers in MARS. Currently, the devices for which MARS parses the generated syslog messages include following: Cisco PIX, Cisco IOS, Cisco CatOS, Cisco ICS, Cisco ASA, Cisco FWSM, Cisco VPN 3000, Cisco

Secure ACS, Snort IDS, Juniper/Netscreen firewalls, Solaris, Linux, and Microsoft Internet Information Server (IIS), Microsoft Windows running the SNARE agent. For other devices, you can define custom log parsers.

The MARS Appliance can begin processing and storing the events while you define the reporting devices using the MARS user interface. You are still required to define the reporting device by IP address and device type in MARS to ensure proper event correlation; however, you are not required to configure device to publish syslog messages directly to MARS.

To configure MARS to work with a syslog relay server, perform the following tasks:

1. Configure the syslog relay server to forward correctly formatted messages to MARS. See [Configuring Syslog-ng Server to Forward Events to MARS, page 3-46](#) or [Configure Kiwi Syslog Server to Forward Events to MARS, page 3-46](#).
2. Identify the MARS Appliance as a forward target.
3. Add the syslog relay server to the MARS user interface. See [Add Syslog Relay Server to MARS, page 3-47](#).
4. Add the reporting devices monitored by the syslog relay server to the MARS user interface. See [Adding Devices Monitored by Syslog Relay Server, page 3-48](#).

Configuring Syslog-ng Server to Forward Events to MARS

We recommend the following settings in the configuration options of the syslog-ng.conf file to ensure good integration of syslog-ng with MARS:

```
options { long_hostnames(off); use_dns(0); keep_hostname(yes); };
```

where

- The long_hostnames(off) setting conforms to RFC 3164, which recommends that the HOSTNAME does not contain domain name.
- The use_dns(0) setting ensures that the IP address is used in HOSTNAME rather than the hostnames.
- The keep_hostname(yes) setting preserves the original sending device's HOSTNAME even when it is relayed more than once.

In addition to configuring the message format, you must specify that the MARS Appliance is a destination loghost on UDP port 514. The following lines must appear in the syslog-ng.conf file:

```
destination loghost { udp("IP address of MARS Appliance" port(514)); };
log { source(src); destination(loghost); };
log { source(net); destination(loghost); };
```

Configure Kiwi Syslog Server to Forward Events to MARS

We recommend the following settings in the configuration options of the Kiwi Syslog Daemon to ensure good integration of Kiwi with MARS:

-
- Step 1** Expand the **File > Setup > Rules > Actions tree**.
 - Step 2** Right click on **Actions** and click **Add an Action**.
 - Step 3** Enter a name for the action, such as "Forward to pncop".
 - Step 4** For the following fields, enter the following values:
 - **Destination IP address or hostname**—Enter the IP address of the MARS Appliance.

- **Protocol**—UDP
- **New Facility**—No Change
- **New Level**—No Change
- **Port**—514
- **Send with RFC 3164 header information**—Selected if the syslog server receives syslog messages directly from the source devices only. Clear if the syslog server also receives syslog messages from relays. Do not configure mixed relays.

This additional header is necessary for the supported device types that do *not* have HOSTNAME in the syslog messages; thereby allowing MARS to correctly identify the original sending device. However, this option cannot be used on a Kiwi relay of relay. To support a Kiwi relay of relay in MARS, the first relay must have this option selected and must receive syslog messages only from the source devices, and all other relays must have this option cleared and must only receive syslog messages from other Kiwi relays, not directly from devices.

- **Retain the original source address of the message**—Cleared.

Step 5 If you are using SNARE agents, click **Setup > Modifiers** and clear “Replace non printable characters with <ASCII value>”

If this value is selected, tabs appear as <009> in the Windows event logs, which prevents MARS from parsing the events correctly.

Step 6 Save your changes.

Add Syslog Relay Server to MARS

In addition to representing each of the potential reporting devices, you must define the syslog relay server so that MARS knows for which messages it should attempt to discover the true reporting device. To add a syslog relay server, you must add it as a security software application running on a host.

To add a syslog relay server, follow these steps:

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 6](#).

Step 3 Specify values for the following fields:

- **Device Name**—Enter the hostname of the syslog relay 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.
- **Reporting IP**—Enter the IP address of the interface in the syslog relay server from which MARS will receive syslog messages.

This address represents the physical IP address of the syslog relay server. To learn more about the reporting IP address, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 3-7](#).

Step 4 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in the syslog relay server from which syslog messages will be received.

This address represents the physical IP address of the syslog relay server. To learn more about the interface settings, its role, and dependencies, see [Understanding Access IP, Reporting IP, and Interface Settings, page 3-7](#).

- Step 5** Click **Apply** to save these settings.
 - Step 6** Click **Next** to access the Reporting Applications tab.
 - Step 7** Select **Generic Syslog Relay ANY** from the Select Application list, and click **Add**.
 - Step 8** Click **Submit** to add this application to the host.
Generic Syslog Relay ANY appears in the Device Type list.
 - Step 9** 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.
 - Step 10** Click **Done** to save the changes.
The host appears in the Security and Monitoring Information list.
 - Step 11** To activate the device, click **Activate**.
-

Adding Devices Monitored by Syslog Relay Server

While you do not have to configure each reporting device to forward syslog messages to the MARS Appliance, you must define the device to MARS so that when it parses the syslog messages forwarded by the relay server, then it is able to match the true reporting IP address to that of a known reporting device type. By knowing the reporting device type, MARS can correctly parse the events.

The process for adding these reporting devices is the same as if there were no syslog relay server except that you do not configure the reporting device to forward events to the MARS Appliance. In the MARS web interface, you should still configure the reporting devices so that MARS can discover their settings and to perform any mitigation operations.



CHAPTER 4

Rules

This chapter discusses MARS Inspection and Drop rules, how to construct and employ them, as well as how to set alerts and use rule and report groups.

This chapter contains the following topics:

- [Rules Overview, page 4-1](#)
- [Constructing a Rule, page 4-5](#)
- [Working with System and User Inspection Rules, page 4-14](#)
- [Working with Drop Rules, page 4-18](#)
- [Setting Alerts, page 4-21](#)
- [Rule and Report Groups, page 4-22](#)

Rules Overview

An inspection rule is a real-time filter that detects interesting patterns of network activity. These patterns can signify attacks or false positives, and they inform you of network configuration errors and other anomalous network behavior. Rules on the Global Controller are propagated down to Local Controllers. When these rules are triggered, incidents are sent to the Global Controller.

An attack might be straightforward, or it could be a probe, an attack, and then a follow-up to the attack. Whatever the method of attack, attacks share common traits, and you use rules to define these traits to identify and mitigate attacks.

Rules create incidents. Rules connect the information you receive from your networks' reporting devices, linking them together to form a chain of events that describes an unfolding intrusion. They classify incoming events as firing events by matching them against the rule criteria. They also determine when a false positive is either dropped completely or kept as information in the database.

A rule is either active or inactive. Active means the rule is operating and is being applied to incoming events. Inactive indicates that the rule is inoperative and not consuming CS-MARS resources. For a list of all system inspection rules, see [Appendix E, "System Rules and Reports"](#).

[Figure 4-1](#) shows a portion of the Inspection Rules page of the Rules tab.

Figure 4-1 Top Portion of Inspections Rules Page on a Local Controller

Rule Name	Action	Provider	Description	Status	Time Range
Global Rule: Cisco IDS rule	None	Cisco	Global Rule: Cisco IDS rule	Active	On: On
System Rule: Backdoor Active	None	None	System Rule: Backdoor Active	Active	On: On

Prioritizing and Identifying

Your first order of business is to prioritize your network's assets; in other words, figure out what is going to be the most damaging if it goes down. Next, identify your networks' most exploitable weaknesses. Choose which ones you are willing and able to close, and rank the remaining weaknesses by risk and exploitability.

Use this ranked list to guide your time and energy expenditures when customizing the CS-MARS rule set.

Thinking Like a Black Hat

Ignore for a moment the benign users who do legitimate business on your networks.

Get inside the mind of the black hat that wants to take your network down. The person who should concern you is the one with a plan.

Good plans have a sequence of steps, contingencies, and metrics to determine success or failure. The more fully you can anticipate these plans, the fewer attacks will be able to execute unhindered and unobserved. The black hat is looking for wide-open doors and easy access. Failing that, the black hat is going to look for specific and obvious exploitable weaknesses.

Planning an Attack

Start to detail the plan for how you would attack your network. You want to penetrate a network. You'd like to avoid detection and identification if possible. You want root access on a host.

How do you get root access? You do not have a preexisting account, and physical access isn't feasible. The first few options that come to mind are password guessing, password brute force, or exploiting a known weakness on the host.

You decide to exploit services running on the host, so you need to find out what it is running. To do this, you have a number of techniques: port scans, OS fingerprinting, banner probing, etc.

Once you've identified a vulnerable service or software, you can attack it with a catalogue of exploit software. Depending on what you find and your available exploits, there are a number of different effects, usually allowing you to execute arbitrary code.

You now own the host. What happens next is up to you. You have many options: you can install a root kit, you can crash the machine, etc. You have full access—you can do just about anything to/from/on that host.

Back to Being the Admin

You must now express the plan in terms of information that is reported to you. This attack plan contains an attack with a follow up of some kind. You might write your plan like:

- Probe
- Attacker to target, buffer overflow
- Attacker to target, root login (compromised host)

At this point, the black hat has compromised the host. What happens next is up to the attacker. This makes the next few steps especially hard to predict. They want to be able to manipulate the world, they want to make change. Your newly compromised host is the instrument for change. You can specify additional potential steps in the plan that make it even more urgent to take care of the situation immediately. Such as:

- Target to FTP server, code download
- Target to secondary target, buffer overflow

The attacker is now using your compromised host as a launching point for further attacks.

One you've mapped out the anticipated attack to watch for, you can define a monitoring plan. The following task flow outlines the tasks involved in implementing a monitoring plan:

-
Step 1	Ensure your reporting devices are providing all the data you need. This step involves ensuring that each device is generating logs about the events that you expect to occur as the result of the probes and attacks. Depending on the device type, this can involve several substeps, such as to specify a logging level, to enable logging for the specific event, and to ensure that the reporting device publishes events to the Local Controller appliance. It can also involve enabling administrative access to the reporting device from the Local Controller appliance.
Step 2	Configure CS-MARS to pull events from the reporting devices on your network. This step involves adding each reporting device to a Local Controller. If the reporting device type is not directly supported, you must define a custom device type for the reporting device. To add a supported reporting device, see the Configuring Reporting and Mitigation Devices in MARS section of the <i>Device Configuration Guide for Cisco Security MARS, Release 6.x</i> . To define a custom device type, see Create a Device Type , page 15-7.
Step 3	Ensure that the event types that you need to study are accepted and processed by Local Controller. If they are not, you must define a custom log parser template for each event and a custom device template to which the custom log parser templates are associated. For device types supported by CS-MARS, this should not be necessary. To define a new device event type (previously called a parser template), see Create Device Event Types for a Custom Device Type , page 15-8.

**Note**

You cannot define a custom log parser template for a reporting device that is supported out of the box. In this case, to define a log parser for an unsupported event type, you must still define a custom device type before you can define the log parser.

- Step 4** Check to see if a system rule will capture the information that you want, otherwise write your own user inspection rule. Define user inspection rules that monitor for the event types and correlate those events into a structure that will help you identify the incident. You can also specify who should be notified and how if the rule fires.

Types of Rules

This section details the following types of rules:

- [Inspection Rules, page 4-4](#)
- [Global User Inspection Rules, page 4-4](#)
- [Drop Rules, page 4-5](#)

Inspection Rules

An inspection rule states the logic by which the CS-MARS tests whether or not a single network event or series of events is a noteworthy incident. An event or series of events with attributes that match the attributes specified in an inspection rule causes the rule to trigger (or “fire”) to create an incident. Incidents may be attacks, network configuration errors, false positives, or just anomalous network activity. The over 100 inspection rules that ship with MARS are called System Inspection Rules. The number and structure of system rules are updated in signature upgrades and with more recent software releases. Both types of upgrades are performed from the Admin > System Maintenance > Upgrade page.

You can create custom inspection rules by editing or duplicating system inspection rules, by adding your own from the Inspection Rules page, or by using the Query interface. Customized inspection rules are called User Inspection Rules and are displayed on the Inspection Rules page.

Inspection rules can be created on both the Global Controller and the Local Controllers. Rules on the Global Controller are propagated down to Local Controllers. When these rules are triggered, incidents are sent to the Global Controller.

Global User Inspection Rules

Global Inspection Rules are inspection rules you create on a Global Controller and then push to the Local Controller. From the Local Controller, you can edit only the Source IP Address, Destination IP Address, and Action fields of a Global Inspection Rule. To change the arguments of the other fields, you must edit the rule on the Global Controller. When you edit a global inspection rule on the Local Controller then edit it again on the Global Controller, the Global Controller version overwrites the Local Controller version. Global Inspection Rule names are displayed with the prefix “Global Rule.”

Drop Rules

Drop rules enable false-positive tuning on a MARS, and are defined only on the Local Controller Drop Rules page. They allow you to refine the inspected event stream by specifying: 1) events and streams to be ignored and 2) whether those data should be stored in the database or discarded entirely. Drop rules are applied to events as they come in from a reporting device, after they have been parsed and before they have been sessionized. Events that match active drop rules are not used to construct incidents. Because the Global Controller does not receive events from reporting devices, rather it receives them from Local Controllers, you cannot define drop rules for the Global Controller.

Constructing a Rule

Each step of your plan corresponds to a line of a rule. Each line identifies a set of conditions. A rule can have a single line, two lines, or multiple lines. You link these lines together using the logical operators, “AND, OR, FOLLOWED-BY (in time).”

For more information on the conditions and operators found in a rule, see [Table 4-1](#).

The first step of the example plan, identified in [Back to Being the Admin, page 4-3](#), involved probing the target host. You can express a probe by selecting the appropriate event type groups as the line’s event type criteria. Also, you want to use dollar variables (\$TARGET) to constrain your host to ensure that the probe and attacks that are reported have happened to the same host. Then you need to figure out the logical step for the next line. In this case, the probe could be optional depending on the time frame in which the probe was sent and its subtlety.



Note

For more information on the conditions and operators found in a rule, see [Table 4-1](#).

- **Variables**—Variables names begin with a dollar sign (such as \$TARGET and \$DEVICE01) or contain the word SAME and DISTINCT (such as, SAME, DISTINCT, and DISTINCT_ANY_DEST_PORT).

A variable, such as (\$TARGET), serves two purposes in the rule: 1.) It captures the number of times the same cell value is matched upon—the count for that cell, e.g., ten login failures from the same source address. 2.) It correlates the same value of a cell across rule lines, for example, a probe from a source address AND an attack from that same source address.

Identical variables used in different fields mean that the values represented by the variable are the same. For instance, if \$TARGET01 were the only argument in the Source IP Address and Destination IP Address fields of an offset, the rule can only fire when the two address of the event are the same. Such a rule may never fire.

- **Rule Logic**—Rule logic is simple. You have a row. Every row has cells. The logical expressions connecting different cells are “and,” while the expressions connecting items inside a cell are either “or” or “and not”, depending which clause is chosen—the equal to or not equal to.
- **Structure**—By studying the system inspection rules, you can identify three commonly used rules: attempts, success likely, and failures. The most common rule structure is the basic three-line rule that identifies an attempted attack. It is expressed as:

```
(Probe AND
Attack) OR
Attack)
```



Note

Success likely rules extend the attempt rules by identifying suspicious activities originating from the attacked host. The general structure of these rules is:

```
((Probe AND
Attack) OR
Attack)) FOLLOWED BY
(Suspicious Activity[1]..Suspicious Activity[n])
```

Failures identify an event from a reporting device that the device classifies as a failure. Often, these rules simply match to known syslog or SNMP messages indicating some failure on the device. You can define alerts to keep you abreast of device failures. These rules follow one of two general structures: a one line failure—

Failure

—or multi-line failures separated by the *OR* operator—

```
1.. N Failure OR
Failure
```

In the HTML interface, system rules are displayed in rows and columns. The row number is called the Offset. A rule can have more than one row (or offset), as shown in [Figure 4-2](#).

Figure 4-2 **Rule with Multiple Offsets**

[illegible]

The flexibility in rule construction is a factor of the rule’s fields and arguments; these are detailed in [Table 4-1](#)

Table 4-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Offset	The row number.	
Open (	Identifies the opening of a clause. Clauses are used to compare one or more compound conditions in a rule.	Displays the open braces you create a clauses.
Source IP	IP address of the packet originator.	
	Variables	<i>ANY</i> —(Default). Signifies that the IP address for each count is any IP address. <i>SAME</i>— Signifies that the IP address for each count is the same IP address. This variable is local to its offset. <i>DISTINCT</i>— Signifies that the IP address for each count is a unique IP address. This variable is local to its offset. <i>\$Target01 to \$Target20</i>— The same variable in another field or offset signifies that the IP address for each count is the same IP address.
	Network Groups	<i>Defined network groups</i> —Topologically valid network groups as defined under Management > IP Management.
	Networks	Topologically valid network groups as defined under Management > IP Management.
	Devices	The hosts and reporting devices present in the system.
	IP addresses	IP addresses present on devices in the system or user entered dotted quads.
	IP ranges	The range of addresses between two dotted quads.
Destination IP	IP address of the packet destination. Often referred to as the target.	
	Variables	
	Network Groups—	<i>Defined network groups</i> —Topologically valid network groups as defined under Management > IP Management.
	Networks —	Topologically valid network groups as defined under Management > IP Management.
	Devices— The hosts and reporting devices present in the system.	The hosts and reporting devices present in the system.
	IP addresses—	IP addresses present on devices in the system or user entered dotted quads.
	IP ranges— The range of addresses between two dotted quads.	The range of addresses between two dotted quads.

Table 4-1 Rule Fields and Arguments (Continued)

Service Name	A TCP/IP-based network service, identified by protocol and port, defined within the packet.	
	Variables	ANY—(Default) No constraint is placed on the source or destination ports or protocol or port. SAME type variables signify that the specified destination port, source port and protocol are the same for each count. These variables are local to the offset. - SAME_ANY_DEST_PORT - SAME_TCP_DEST_PORT - SAME_UDP_DEST_PORT - SAME_ANY_SRC_PORT - SAME_TCP_SRC_PORT - SAME_UDP_SRC_PORT DISTINCT type variables signify that the specified destination port, source port and protocol are unique for each count. These variables are local to the offset. - DISTINCT_ANY_DEST_PORT - DISTINCT_TCP_DEST_PORT - DISTINCT_UDP_DEST_PORT Identical variables in different fields or offsets signify that the specified port and protocol for each count are identical to each other. \$ANY_BOTH_PORT5 \$ANY_DEST_PORT1 to ANY_DEST_PORT5 \$ANY_SRC_PORT1 \$TCP_BOTH_PORT1, \$TCP_BOTH_PORT2 \$TCP_DEST_PORT1 to \$TCP_DEST_PORT5 \$TCP_SRC_PORT1, \$TCP_SRC_PORT2 \$UDP_BOTH_PORT1, \$UDP_BOTH_PORT2 \$UDP_DEST_PORT1 to \$UDP_DEST_PORT5 \$UDP_SRC_PORT1, \$UDP_SRC_PORT2
	Defined services —One or more services defined under Management > Service Management.	
	Service groups —One or more service groups defined under Management > Service Management.	- Backdoor - Instant Messaging - Mail Retrieval - Online Game - P2P - Recent Backdoor - TCP-highport - UDP-highport - vulnerable-protocols

Table 4-1 Rule Fields and Arguments (Continued)

Event	Identifies one or more event types. An event type indicates some type of network activity or condition. Sometimes, events reported from different devices and different device types identify the same activity or condition, and therefore, they map to the same event type within MARS. Event types are sorted into event groups, such as “Probe/PortSweep/Stealth”, to catch any of the network conditions identified by the group.	
	Variables —Signify any single event type defined under Management > Event Management, only useful for lines in tandem with the same variable.	• ANY —Any of the active event types can match this rule. • SAME • DISTINCT • \$EVENT_TYPE01, \$EVENT_TYPE10
	Event types —Events that have been merged into types.	• ANY • SAME • DISTINCT • All events
	Event type groups —Groups of event types.	• ANY • SAME • DISTINCT
	Red Severity Event Types—Displays all severe event types	
	Yellow Severity Event Types—Displays all yellow event types	
	Green Severity Event Types—Displays all green event types	
Device	The value of this condition can be one of the following:	
	Variables —Signify any single device defined under Admin > System Management > Security and Monitor Devices, only useful for lines in tandem with the same variable.	• ANY —(Default) Specifies that this rule is applied to events generated by any of the reporting devices defined in MARS. • SAME • DISTINCT • Unknown Reporting Device —Specifies that this rule is applied to events generated by any reporting device that is not defined in MARS. • \$DEVICE01 to \$DEVICE10

Table 4-1 Rule Fields and Arguments (Continued)

	• Reporting Devices —Identifies one or more hosts or reporting devices for which events are inspected. Valid values are one or more devices as defined under Admin > System Setup > Security and Monitor Devices.	
	Defined Device Types—	
Reported User	Identifies the active user on the host when this event was recorded. Not all events include this data. The value of this condition can be one of the following:	• ANY —No constraint is placed on the reported user. • NONE —(Default) Specifies that this condition should not be used to match this rule. • Variables —Signify any single user, only useful for lines in tandem with the same variable. • Invalid User Name —Specifies that this condition is met when the user name reported is invalid.
IPS Risk Rating	Identifies, on a scale of 0 to 100, the Risk Rating (RR) value assigned by an IPS device version 6.0 or greater. The higher the RR the greater the security risk	You can use the IPS RR to filter events in a report. For additional information see, Cisco IPS Risk Rating Explained.
IPS Threat Rating	IPS Threat Rating (TR) provides a single view of the threat environment of the network.	You can use the IPS TR to minimize alarms and events by customizing the viewer to show only events with a high TR.
IPS Global Correlation Score	Identifies, on a scale of -10 to 10, the Global Correlation Score assigned to a device, if one has been assigned. It indicates the probability that a particular attacker IP address will initiate malicious behavior based on its known past activity.	You can use the IPS Global Correlation Score to filter events in a report. For additional information see, Configuring Global Correlation.

Table 4-1 **Rule Fields and Arguments (Continued)**

Severity	The value of this condition can be one of the following:	• ANY —(Default) Specifies that this rule is applied to events of all severity levels. • Green —Restricts this rule to firing against low-severity events. • Yellow —Restricts this rule to firing against medium-severity events. • Red —Restricts this rule to firing against high-severity events.
Count	Identifies the number of items the event must occur before the condition is met. The value for this condition is a whole number ranging between 1 and 100. The default value is 1. Note Events of the same event type occurring in the same session in a three-second period increment the active count by one. This inherent threshold ensures that a event floods of the same type does not increase the active count arbitrarily and incorrectly fire the rule.	<i>Example usage:</i> When a backdoor rootkit install is detected, the count should be 1 as it is only going to be reported once and it is not something you expect to ever see on your network. However, if you are using deny messages to detect infected hosts, you may want the count value to be higher. For example, you may want to allow for several common mistakes, such as password failures, before firing a rule for the event. People accidentally mistype passwords, they don't accidentally install a rootkit.
Close	Identifies the close of a clause.	
Operation	The value of this field can be one of the following:	• None —(Default) Defines a single-line rule or a simple condition. • AND —A boolean “and” used to construct a compound condition (two or more lines). This line and the next line must both be satisfied before the compound condition is met. • OR —A boolean “or” used to construct a compound condition (two or more lines). Either this line or the next line can be satisfied to meet the compound condition. • FOLLOWED-BY —Identifies a compound condition (two or more lines). specifically a sequential order of occurrence. Also referred to as a time conditional rule (e.g., Y must happen after X).The condition of this line must be met, and then the condition of the next line must be met before the compound condition is met.

Table 4-1 **Rule Fields and Arguments (Continued)**

Time Range	Identifies the period of time over which the count value is augmented. For rules that have a Count value greater than one, the Time Range value determines how long the period should be before the count value is reset. For example, you can assume that if no more than three login attempts have occurred over a 10-minute period that counter can be reset.	Usage Guideline: The Time Range value combined with the Count value can affect the operation of your MARS. Each time an event is captured that satisfied a unique instance of an inspection rule, a monitoring session is constructed to track possible future occurrences until either the Count value is reached or the time period expires.
Action	Identifies the action that MARS will take when the rule is fired. Actions are user-defined alerts that include an action name and description, which also doubles at the message text provided in the alert. Each action can combine alert techniques, such as email and syslog. Each alert technique can have multiple values. For example, an action can generate two emails, a page, and a SNMP trap. Each rule can have multiple such actions. Alerts can be constructed using one or more of the following techniques: Note You will see the column Action/Operation. In this case, you can select either one of the following actions or one of the operators.	• NONE—(Default) This action states that no further action will be taken. When NONE value is selected, the firing of the rule causes an event record to be created and stored in MARS. Regardless of the selected action, this record is always created. • Email—Identifies the list of administrators to whom an alert should be sent. An e-mail address must be defined for the selected administrators. • Syslog—Identifies the list of hosts to whom an alert should be sent. You can select any number of devices to which you want a syslog message sent. • Page—Identifies the list of administrators to whom an alert should be sent. The message format is text. A pager number must be defined for the selected administrators. • SNMP—Lists the hosts to which a Simple Network Management Protocol (SNMP) alert can be sent. • SMS—List of users to receive notification by Short Message Service (SMS). The message can be up to 160 characters. An SMS number must be ten numbers and a domain name, for example, 1234567890@provider.com.

Working Examples

The examples in this section demonstrate the use of variables, in particular, how to use variables to detect Deny patterns.



Note

We recommend that you study the system inspection rules for more complex examples. For a list of system rule names and descriptions, see [Appendix E, “System Rules and Reports”](#).

**Note**

For a single offset rule, the variables SAME and SAME_ANY_DEST_PORT can be substituted in any of the examples for \$TARGET01 and \$ANY_DEST_PORT1, respectively. The “ANY” in \$ANY_DEST_PORT1 means either UDP or TCP protocol.

Example A: Excessive Denies to a Particular Port on the Same Host

Figure 4-3 Rule for Excessive Denies to a Particular Port on the Same Host

The screenshot shows the Cisco Security MARS Local Controller interface for rule configuration. The rule is named 'Example A' and is currently inactive. The description is 'Excessive denies to particular port on the same host.' The rule is configured with the following parameters:

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Severity	Count	Close	Operation
1	ANY	\$TARGET01	\$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	100		

In this example, the rule fires when 100 of the specified events occur from any source IP address to the same destination IP address, and the destination port numbers are identical.

Example B: Same Source Causing Excessive Denies on a Particular Port

Figure 4-4 Rule for Same Source Doing Excessive Denies on a Particular Port

The screenshot shows the Cisco Security MARS Local Controller interface for rule configuration. The rule is named 'Example B' and is currently inactive. The description is 'Same source doing excessive denies on a particular port.' The rule is configured with the following parameters:

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Severity	Count	Close	Operation
1	\$TARGET01	ANY	\$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	ANY	ANY	ANY	ANY	ANY	YELLOW	100		

In this example, the rule fires when 100 of the specified events occur that have the source IP address, any Destination IP address, and identical destination port numbers.

Example C: Same Host, Same Destination, Same Port Denied

Figure 4-5 Rule for Same Host, Destination, Same Port Denied

The screenshot shows the Cisco Security MARS Local Controller interface for rule configuration. The rule is named 'Example C' and is currently inactive. The description is 'Same host, destination, same port getting denied.' The rule is configured with the following parameters:

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Severity	Count	Close	Operation
1	\$TARGET01	\$TARGET02	\$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	ANY	ANY	ANY	ANY	ANY	YELLOW	20		

In this example, the rule fires when 20 of the specified events occur that have the same source and destination addresses, and identical destination port numbers.

Working with System and User Inspection Rules

Navigate to the **Inspection Rules** page by clicking the **Rules** tab.

You can perform the following actions with inspection rules:

- Change the Source IP, Destination IP and Device fields of a System Inspection rule.
- Duplicate any inspection rule, then edit the fields to make a new User Inspection Rule.
- Build a new User Inspection Rule with the Rule wizard.
- Edit any field in a User Inspection Rule.
- Make any rule active or inactive.
- Edit, delete, or add a Rule Group.

**Note**

When you add or edit a rule, you must click **Activate** to enable the changes.

**Note**

Upgrade the MARS software regularly to obtain new and updated System Inspection Rules. For more information, see the [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#). For a list of System Inspection Rules, see [Appendix E, “System Rules and Reports”](#).

This section contains the following topics:

- [Change Rule Status—Active and Inactive, page 4-14](#)
- [Duplicate a Rule, page 4-15](#)
- [Editing a Rule, page 4-15](#)
- [Add an Inspection Rule, page 4-16](#)

Change Rule Status—Active and Inactive

The MARS correlation engine continuously tests only active rule criteria against incoming events to identify incidents. Inactive rules do not consume resources used for realtime operations.

To change the status of a rule, follow these steps:

-
Step 1	Navigate to the Rules > Inspection Rules page.
Step 2	Select the check box of the rule (or rules) to change.
Step 3	Click Change Status .
	The selected rules are made inactive if active, and active if inactive, and are displayed on a different page.
Step 4	To display inactive rules, select Inactive from the View dropdown list. To display active rules, select Active .
-

Duplicate a Rule

Duplicating a rule creates a new rule that is a copy of an existing system or user inspection rule. You can edit all of the fields of a duplicate rule, but only the Source IP, Destination IP, and Device fields of a system inspection rule. The original rule is left unchanged after duplication.

To duplicate a rule, follow these steps:

Step 1 Select the check box of the rule to duplicate.

Step 2 Click **Duplicate**.

The name of duplicated rule is the name of the original rule extended with a timestamp of when the original was duplicated (for example, System Rule: Client Exploit - Sasser Worm Copied: 05.10.05/16:54:21). The name can be changed by editing the duplicate rule.

Editing a Rule

You can edit rules with inline editing, or with the rule wizard. To edit inline, you click the argument to edit. The rule wizard is invoked by selecting a rule to edit then clicking **Edit**. The rule wizard begins with the Rule Name field and progresses through each subsequent field.

**Note**

You only edit the Source IP, Destination IP, and Device fields of a system inspection rule. See [Duplicate a Rule, page 4-15](#) for further information on modifying system inspection rules.

This section contains the following topics:

- [Edit a Rule with Inline Editing, page 4-15](#)
- [Edit a Rule with the Rule Wizard, page 4-16](#)

Edit a Rule with Inline Editing

You can perform inline editing to rules from the Incidents Detail page, or from the Inspections Rules page.

To edit a rule with the Inline Editing, follow these steps:

Step 1 Click the Rule argument that you want to edit.

The edit page for the selected field appears.

Step 2 Change the argument, then click **Apply**.

Step 3 Repeat [Step 1](#) as required.

Step 4 Add Open and Close parentheses as required then click **Submit**.
If no parentheses are required, just click **Submit**.

Step 5 Click **Activate** to include the rule in event correlation processing.

Edit a Rule with the Rule Wizard

The Rule Wizard can only be invoked from the Inspections Rule page.

To edit a rule with the Rule Wizard, follow these steps:

-
- Step 1** Select the check box of the rule to edit.
- Step 2** Click **Edit**. The rule wizard page appears for the Rule Name field.
- Step 3** Do one of the following actions:
- Change the argument of the field, then click **Apply**. Proceed to [Step 6](#).
 - Change the argument, then click **Next** to proceed to the next field.
 - Click **Next** to proceed to the next field without changing the argument.
 - Click **Previous** to go back to the previous field. Previous does not appear for the Rule Name page.
- Step 4** Repeat [Step 3](#) as required.
- Step 5** Click **Apply** after making all edits.



Tip To skip to the end, click the Count argument, after which, only the **Action**, and **Time Range** fields must be reviewed.

- Step 6** Add Open and Close parentheses as required then click **Submit**. If no parentheses are required, just click **Submit**.
- Step 7** Click **Activate** to include the rule in event correlation processing.



Note When you edit a rule on the Global Controller, the Local Controller receives only information pertinent to that Local Controller from the Global Controller. For example, if an edited Global Inspection rule is triggered only by a device that does not report to a specific Local Controller, the rule changes are not propagated to that Local Controller.

Add an Inspection Rule



Note Rules that you add are called User Inspection Rules.

To add a user inspection rule, follow these steps:

-
- Step 1** Navigate to the Inspection Rules page.
- Step 2** Click **Add**.
- Step 3** Enter a name and description for the rule, then click **Next**.
- Step 4** Select Source IP address.

Figure 4-6 User Inspection Rule Wizard Form

The following numbers correspond to the numbers shown in [Figure 4-6](#).

1. Check the boxes next to the items in the **Sources Selected** field to select them, and click the **Toggle Equal** button to change them between equal and not equal.
2. Click the **Select All** button to select all items in the **Sources Selected** field. Items selected in the Sources Selected field are deselected when you click **Select All**.
3. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field into the **Sources Selected** field.
4. Filter sources from this drop-down list.
5. Enter search text, and click **Enter** to move items that match the search criteria from the **Sources Available** field to the **Sources Selected** field.
6. To add a new item to the sources, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button.
7. Click an item or items in the Sources Selected field, and use the **Remove** button.
8. To move IP values up into the Sources Selected field, click the **Equal**  up icon, or the **Not Equal**  up icon.
9. Check the radio button next to **IP** or **Range**, and enter an IP address or a range of IP addresses into their respective fields.
10. Select items in the Sources Selected field by clicking them. Enter a group name, and click the **Grouped As** button to group them.

Step 5 Follow the wizard, and select the values for the rule, clicking the **Next** button to progress to the next step.

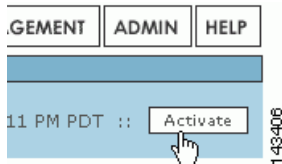
Step 6 When you are asked, “Are you done defining the rule conditions,” you can:

- Click the **Yes** button for a single line rule. Continue to add repetition requirements (counts), alert information, and valid time ranges for each line.

- Click the **No** button, to create a multi-line rule that uses an operator (OR, AND, or FOLLOWED BY). Return to [Step 4](#) and continue to make your selections. Continue to add rule information, and click **Submit** when finished.
- Click the **Submit** button when finished.

Step 7 When the rule is complete, you need to activate it by clicking the **Activate** button.

Figure 4-7 Clicking the **Activate** button



Note

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

Working with Drop Rules

Navigate to the Drop Rules page by clicking the **Rules > Drop Rules** tabs.

Drop rules instruct the MARS to either drop a false positive completely from the appliance, or to keep it in the database. On the Drop Rules page, you add, edit, duplicate, activate an inactive rule, or inactivate an active rule. Inactive rules do not fire.



Note

Drop Rules can be defined only on the Local Controller Drop Rules page.

While working with drop rules is similar to working with inspection rules, it is not identical.

This section contains the following topics:

- [Change Drop Rule Status— Active and Inactive, page 4-18](#)
- [Duplicate a Drop Rule, page 4-19](#)
- [Edit a Drop Rule, page 4-19](#)
- [Add a Drop Rule, page 4-19](#)

Change Drop Rule Status— Active and Inactive



Note

Drop Rules can be changed only on the Local Controller Drop Rules page.

Step 1 Check the box next to the rule.

Step 2 Click **Change Status**.

When you change the status to inactive, the rule displays only on the inactive rules page.

Step 3 To display inactive drop rules, select **Inactive** from the **View** dropdown list.

Duplicate a Drop Rule

**Note**

Drop rules can be duplicated only on the Local Controller Drop Rules page.

Step 1 Check the box next to the rule.

Step 2 Click the **Duplicate**.

After duplicating a rule, you can edit the duplicate without altering the original.

Edit a Drop Rule

**Note**

Drop rules can be edited only on the Local Controller Drop Rules page.

Step 1 Check the box next to the rule.

Step 2 Click **Edit** on the field that you want to change.

Step 3 Follow the rule's wizard and complete any other changes to the rule.

Step 4 Click **Submit**.

**Note**

When the rule or rules are complete, click **Activate**.

Add a Drop Rule

**Note**

Drop Rules can be added only on the Local Controller Drop Rules page.

Step 1 Click **Add**.

Step 2 Enter a name and description for the rule, and click **Next**.

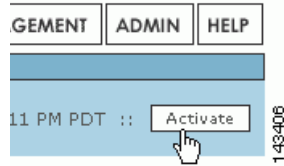
Step 3 Select your sources.

Figure 4-8 Drop Rule Creation Form

The following numbers correspond to the numbers as shown in [Figure 4-8](#):

1. Check the boxes next to the items in the **Sources Selected** field to select them, and click the **Toggle Equal** button to change them between equal and not equal.
2. Click the **Select All** button to select all items in the **Sources Selected** field. (Note: if you have items highlighted in the Sources Selected field, clicking **Select All** will de-select them.)
3. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field into the **Sources Selected** field.
4. Filter sources from this drop-down list.
5. Enter search text, and click **Enter** to move items that match the search criteria from the **Sources Available** field to the **Sources Selected** field.
6. To add a new item to the sources, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button. See [IP Management, page 6-3](#) for more information.
7. Click an item or items in the Sources Selected field, and use the **Remove** button.
8. To move IP values up into the Sources Selected field, click the **Equal**  (Up) icon, or the **Not Equal**  (Up) icon.
9. Check the radio button next to **IP** or **Range**, and enter an IP address or a range of IP addresses into their respective fields.
10. Select items in the Sources Selected field by clicking them. Enter a group name, and click the **Grouped As** button to group them.

- Step 4** Follow the wizard, and select the values for the rule, clicking the **Next** button to progress to the next step.
- Step 5** When you are asked, “Are you done defining the rule conditions,” click the **Submit** button.
- Step 6** When the rule is complete, you need to activate it by clicking the **Activate** button.

Figure 4-9 Clicking the **Activate** button**Note**

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

Setting Alerts

You have two options for learning about rules that have fired:

- You can log in and view the appropriate pages in the HTML interface, or
- You can have MARS send alerts to external devices and users.

You use *actions* to provide instructions to MARS on the second method.

Using alerts associated to rules, you can alert a particular person, group, or system that a particular rule has fired. The roles and groups you can choose are determined by the information you have entered in User Management. See [Green-field, Multi-box Deployment, page 1-6](#) for more information.

Configure an Alert for an Existing Rule

- Step 1** Click on a rule argument.
- Step 2** Click **Next** until the Action/Operation column is selected.
- Step 3** Click the **Add** button to add users for an alert.
- Step 4** Enter a **Name** and **Description** for the notification.
- Step 5** Check the box next to the type of notification that you want to send. Your choices are:
 - **Email**—select the roles or groups that you want to receive an email.
 - **Syslog**—select the systems that you want to receive the syslogs.
 - **Page**—select the roles or groups that you want to receive an electronic page on their pagers or cellular telephones.

**Note**

For information on setting up pager alerts, see [Adding a Service Provider \(Cell phone/Pager\), page 6-14](#).

- **SNMP**—select the systems that you want to receive the SNMP trap information.

**Note**

For SNMP and Syslog, you need to configure the receiving systems for this feature to work.

- Step 6** Click the **Change Recipient** button to add or edit recipients for alerts for that notification type (email, syslog, page, or SNMP).
- Step 7** Check the box next to the role, group, or system that you want to receive alerts.
- Click the **Add** button to select recipients (to move them into the left field.)
 - To remove recipients, click their names to highlight them (in the left field) and click the **Remove** button.
- Step 8** Repeat [Step 5](#) through [Step 7](#) for all the alert selections that you want to include.
- Step 9** Click the **Submit** button.
- Step 10** Click the **Apply** button.

**Note**

If a user adds an alert to a rule created on the Global Controller, and the rule is pushed down and fired on the Local Controller, the designated user receives the alert from the Local Controller and not the Global Controller.

Rule and Report Groups

This section contains the following topics:

- [Rule and Report Group Overview, page 4-22](#)
- [Global Controller and Local Controller Restrictions for Rule and Report Groups, page 4-24](#)
- [Adding, Modifying, or Deleting a Rule Group, page 4-24](#)
- [Adding, Modifying, or Deleting a Report Group, page 4-27](#)
- [Display Incidents Related to a Rule Group, page 4-30](#)
- [Create Query Criteria with Report Groups, page 4-30](#)
- [Use Rule Groups in Query Criteria, page 4-31](#)

Rule and Report Group Overview

**Note**

For a list of all System Inspection rules and reports, see [Appendix E, “System Rules and Reports”](#).

Grouping rules and reports helps you by speeding access to those particular rules and reports relevant to your immediate task. You can create groups, or use the groups provided with CS-MARS (System groups). Groups act as filters to limit the display of rules, reports, and incidents in the CS-MARS HTML interface. All groups can be modified or deleted.

CS-MARS provides more than 100 system rules and 150 system reports. You can add more by creating custom rules and reports and by performing periodic software updates. A rule or report group contains, as members, a particular subset of all rules or reports. Usually, rules or reports within the same group have related functions (such as, reconnaissance activities, server attack, etc.). When you select a group from a dropdown filter, only those rules and reports that are members of that group are displayed on the page. When you select a rule group on the Incidents page, only those incidents related to the rules of the selected group display. You can also use report and rule groups when constructing queries.

For instance, there are at least 16 system rules that detect suspicious network access events and incidents, and 15 system reports to report this information. CS-MARS provides a system rule group and a system report group named “Access” that can filter the Inspection Rules, Incidents, and Report pages to display only those rules and reports related to monitoring access events (such as password attacks), thereby eliminating the need to search for the pertinent rules and reports within the complete rule and report pages or dropdown lists. CS-MARS provides system rule and report groups as listed in [Table 4-2](#).

Table 4-2 *Predefined Rule and Report Groups*

System Report Groups	Corresponding System Rule Groups
System: Access	System: Access
System: All Events - Aggregate View	—
System: All Exploits - Aggregate View	—
System: COBIT DS3.3 - Monitoring and Reporting	—
System: COBIT DS5.10: Security Violations	—
System: COBIT DS5.19: Malicious software	—
System: COBIT DS5.20: Firewall control	—
System: COBIT DS5.2: Authentication and Access	—
System: COBIT DS5.4: User Account Changes	—
System: COBIT DS5.7: Security Surveillance	—
System: COBIT DS9.4: Configuration Control	—
System: COBIT DS9.5: Unauthorized Software	—
System: CS-MARS Incident Response	System: CS-MARS Incident Response
System: CS-MARS Issue	
System: Client Exploits, Virus, Worm and Malware	System: Client Exploits, Virus, Worm and Malware
System: Configuration Changes	—
System: Configuration Issue	System: Configuration Issue
System: Database Server Activity	System: Database Server Activity
System: Host Activity	System: Host Activity
System: Network Attacks and DoS	System: Network Attacks and DoS
System: New Malware Outbreak (Cisco ICS)	System: New Malware Outbreak (Cisco ICS)
System: Operational Issue	System: Operational Issue
System: Reconnaissance	System: Reconnaissance

Table 4-2 **Predefined Rule and Report Groups (Continued)**

System: Resource Issue	System: Resource Issue
System: Resource Usage	—
System: Restricted Network Traffic	System: Restricted Network Traffic
System: SOX 302(a)(4)(A)	—
System: SOX 302(a)(4)(D)	—
System: Security Posture Compliance (Cisco NAC)	System: Security Posture Compliance (Cisco NAC)
System: Server Exploits	System: Server Exploits

Global Controller and Local Controller Restrictions for Rule and Report Groups

Global Controller and Local Controller rule and report groups have the following restrictions:

- Rule and report groups created on the Global Controller are pushed to all the Local Controllers.
- Rule groups created on a Local Controller are confined to the Local Controller. They are not copied to the Global Controller or to other Local Controllers.
- Local Controller account holders can edit only the Source IP, Destination IP, and Device fields of a rule group created on a Global Controller.
- Local Controller account holders cannot edit Global Controller report groups.
- Local Controller account holders cannot delete Global Controller rule and report groups.



Note

The procedures described in this section are valid for both the Local and Global Controllers, except for the Case Bar, which does not appear on the Global Controller HTML interface.

The following behaviors should also be noted:

- If an object (network group, network, or device) specific to LC1 is passed to LC2, the object is removed from the source or destination list of the rule or report on LC2. It is removed because LC2 has no knowledge of the object.
- For *user* rules if the entire source or destination field is empty after the removal of devices unknown to that Local Controller, the rule status changes to INACTIVE and the empty field of the rule shows as *none*.
- For *system* rules if the entire source or destination field is empty after the removal of devices not known to that Local Controller, the rule status changes to INACTIVE and the empty field of the rule shows as *ANY*.
- For reports, if the entire source or destination field is empty after the removal of devices not known to that Local Controller, the report status changes to INACTIVE. Therefore, the report does not appear in the web interface of the Local Controller.

Adding, Modifying, or Deleting a Rule Group

This section details how to operate upon rule groups.

This section contains the following topics:

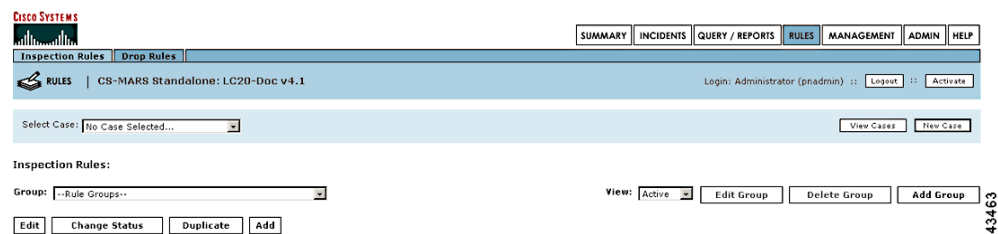
- [Add a Rule Group, page 4-25](#)
- [Modify a Rule Group, page 4-26](#)
- [Delete a Rule Group, page 4-27](#)

Add a Rule Group

To add a rule group, follow these steps:

- Step 1** Navigate to the Inspection Rules page, as shown in [Figure 4-10](#).

Figure 4-10 Inspection Rules Page



- Step 2** Click **Add Group**.

The Add Group dialog box appears, as shown in [Figure 4-11](#).

Figure 4-11 Add Group Dialog Box



- Step 3** Enter the new group name in the **Name** field.

- Step 4** Click the check boxes of the rules to be added to the new rule group.

**Tip**

The dropdown list above the list of rules can limit the display of rules to active system rules, active user rules, or inactive rules. The search function displays only those rules that match a search string (for example, “New Malware Traffic Match.”). The asterisk wildcard character (*) is supported.

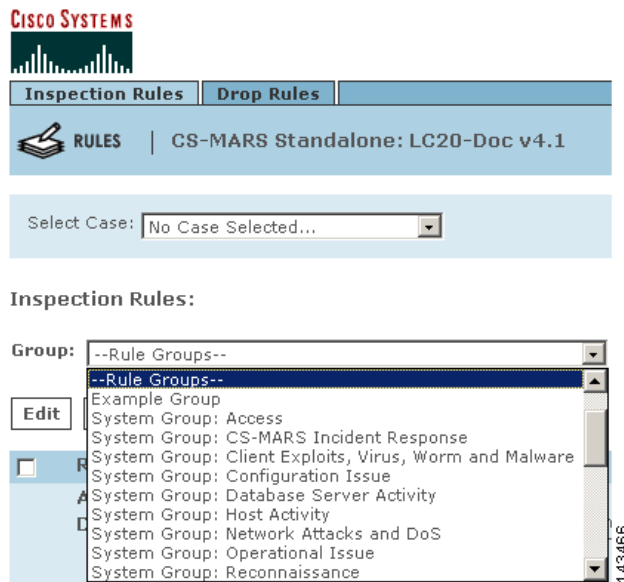
Step 5 Click **Add**.

The selected rules appear in the lefthand pane of the dialog box. To remove a rule from the group, highlight the item in the lefthand pane and click **Remove**.

Step 6 Click **Submit**.

The new rule group name appears in the **Group** dropdown filter on the Inspection Rules page, as shown in [Figure 4-12](#). In this example, the new rule group name is “Example Group.” Because it is a user-created rule group, the rule group name appears without the prefix “System.” You can also click **Cancel** to return to the Inspection Rules page without creating a new rule group.

Figure 4-12 New Rule Group Appears on the Dropdown List of the Inspections Rules Page



Modify a Rule Group

To edit a rule group, follow these steps:

Step 1 Navigate to the Inspection Rules page, as shown in [Figure 4-10](#).**Step 2** Select the rule group to edit in the **Group** pull-down filter.**Step 3** Click **Edit Group**.

The Add Group dialog box appears, as shown in [Figure 4-11](#). The rule group name appears in the **Name** field, and the included rules appear as selected rules in the lefthand pane of the dialog box.

- Step 4** To add additional rules, click the checkbox of all the rules to be added to the group, then click **Add**. To remove rules, highlight the items in the lefthand pane to remove, then click **Remove**.
- Step 5** Click **Submit**.
-

Delete a Rule Group

To delete a rule group, follow these steps:

-
- Step 1** Navigate to the Inspection Rules page, as shown in [Figure 4-10](#).
- Step 2** Select the rule group to delete in the **Group** pull-down filter.
- Step 3** Click **Delete Group**.
- The Delete Group dialog box appears listing the rules in the group to be deleted. You are prompted to confirm deletion.
- Step 4** Click **Yes**.
- The rule group no longer appears in the **Group** drop-down filters on the Incident and Inspection Rules pages.
-

Adding, Modifying, or Deleting a Report Group

This section details how to operate upon report groups.

This section contains the following topics:

- [Add a New Report Group, page 4-27](#)
- [Modify a Report Group, page 4-29](#)
- [Delete a Report Group, page 4-29](#)

Add a New Report Group

To add a report group, follow these steps:

-
- Step 1** Navigate to the Report page, as shown in [Figure 4-13](#).

Figure 4-13 Reports Page
Step 2 Click **Add Group**.

The Add Group dialog box appears, as shown in [Figure 4-14](#).

Figure 4-14 Add Report Group Dialog Box
Step 3 Enter the new report group name in the **Name** field.**Step 4** Select the checkboxes of the reports to be added to the new report group.**Tip**

The dropdown filter above the list of reports can filter the display of reports to display system reports, user reports, or all reports. The search function displays only those reports that match a search string (for example, “Spy” for Spyware). The asterisk wildcard character (*) is supported.

Step 5 Click **Add**.

The selected reports appear in the lefthand pane of the dialog box. To remove a report from the group, highlight the item in the lefthand pane and click **Remove**.

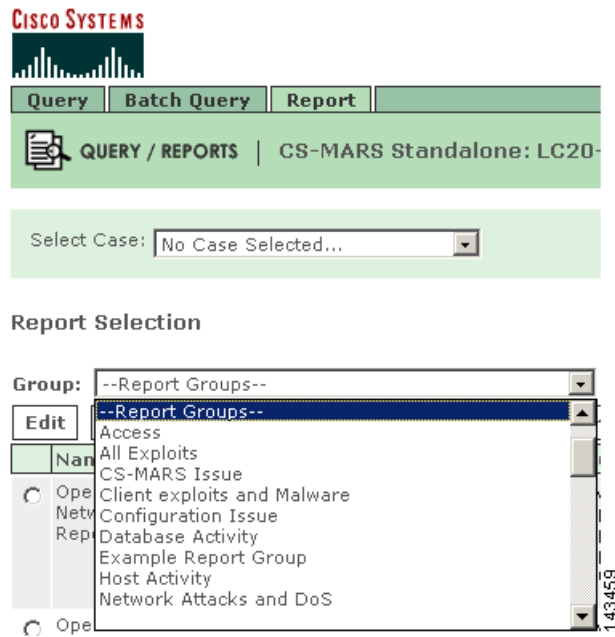
Step 6 Click **Submit**.

The new report group name appears in the **Group** dropdown list display filter on the Report page, as shown in [Figure 4-15](#), and on the Query Page. Because it is a user-created report group, the report group name appears without the prefix “system.”

**Tip**

You may also click **Cancel** to return to the Report page without creating a new report group.

Figure 4-15 The New Report Group Appears on the Dropdown Filter of the Report Page



Modify a Report Group

To modify a report group, follow these steps:

- Step 1** Navigate to the Reports page, as shown in [Figure 4-13](#).
- Step 2** Select the report group to edit from the **Group** pull-down list.
- Step 3** Click **Edit Group**.
The Add Report Group dialog box appears, as shown in [Figure 4-14](#). The report group name appears in the **Name** field, and the reports that are in the report group appear in the lefthand pane of the dialog box.
- Step 4** To add additional reports, click the checkboxes of the reports to be added to the group, then click **Add**.
To remove reports, highlight the items to remove in the lefthand pane, then click **Remove**.
- Step 5** Click **Submit**.

Delete a Report Group

To delete a report group, follow these steps:

- Step 1** Navigate to the Reports page, as shown in [Figure 4-13](#).
- Step 2** Select the report group to delete in the **Group** pull-down filter.
- Step 3** Click **Delete Group**.

The Delete Report Group dialog box appears listing the reports in the group to delete. You are prompted to verify deletion.

Step 4 Click **Yes**.

The report group no longer appears in the report group dropdown lists on the Report and Query pages.

Display Incidents Related to a Rule Group

To display incidents that occur from the firing of rules in a specific rule group, follow these steps:

Step 1 Navigate to the Incidents page.

Step 2 Select the rule group in the dropdown filter above the Matched Rules column, as shown in [Figure 4-16](#).

The Incidents page displays only those incidents that occurred from rules firing in the selected rule group.

Figure 4-16 Rule Group on Incidents Page

The screenshot shows the Cisco Systems Incidents page. At the top, there are tabs for 'Incidents', 'False Positives', and 'Cases'. Below these, there is a header for 'INCIDENTS | CS-MARS Standalone: LC20-Doc v4.1'. A 'Select Case:' dropdown menu is visible, currently showing 'No Case Selected...'. Below this, there is a 'Recent Incidents' section with a 'View' button. A table of incidents is displayed, with columns for Incident ID, Event Type, Action, and Time. A dropdown menu is open over the table, showing a list of rule groups including 'All Rules', 'Rule Groups--', 'Example Group', 'System Group: Access', 'System Group: CS-MARS Incident Response', 'System Group: Client Exploits, Virus, Worm and Malware', 'System Group: Configuration Issue', 'System Group: Database Server Activity', 'System Group: Host Activity', 'System Group: Network Attacks and DoS', and 'System Group: Operational Issue'.

Incident ID	Event Type	Action	Time
I:10985516	Inactive CS-MARS reporting device	Alert	14:34:67
I:10985515	Inactive CS-MARS reporting device	Alert	14:34:67
I:10985514	Inactive CS-MARS reporting device	Alert	14:34:67
I:10985513	Inactive CS-MARS reporting device	Alert	14:34:67
I:10985512	Inactive CS-MARS reporting device	Alert	14:34:67

Create Query Criteria with Report Groups

To create queries from report groups, follow these steps:

Step 1 Navigate to the Query page.

Step 2 Select a report group in the **Load Report as On-Demand Query with Filter** dropdown filter, as shown in [Figure 4-17](#).

Only the reports that belong to the report group are displayed in the Select Report dropdown list, as shown in Figure 4-18.

Figure 4-17 *Selecting A Report Group to Make a Query*

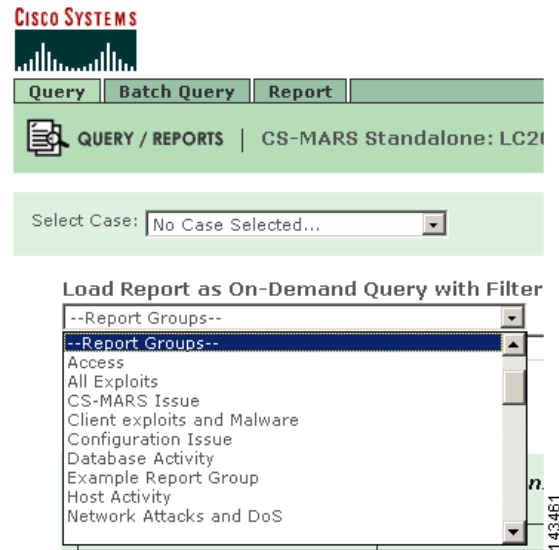
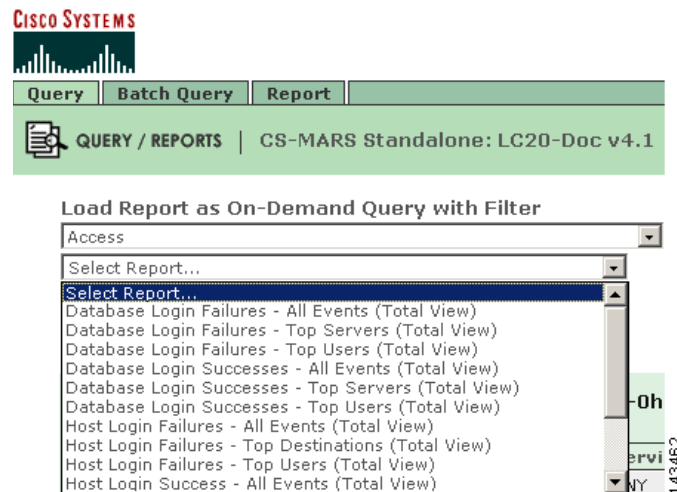


Figure 4-18 *Selecting a Report Within the Report Group to Make a Query*



Step 3 Select the report in the secondary dropdown list.

The **Query** criteria are automatically populated per the selected report.

Use Rule Groups in Query Criteria

To populate the Rule field of the **Query Event Data** bar using rule groups, follow these steps:

- Step 1** Navigate to the Query page.
- Step 2** Click **Any** in the **Rules** field of the **Query Event Data** bar.
The Filter by Rule dialog box appears as shown in Figure 4-19.
- Step 3** Select the rule group in the dropdown list above the list of rules, as shown in Figure 4-14.
The list of rules will display only those rules in the selected rule group.

Figure 4-19 Rule Group Used to Populate Rule Criterion in Query

Query type: Event Types ranked by Sessions, 0h:10m [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY

Filter by Rule

Group: Example Group [Search]

System Rule: Backdoor: Active
System Rule: Backdoor: Connect

143465

- Step 4** Click the checkboxes of the rules to include in the query.
- Step 5** Click **Add**.
The selected items appear in the lefthand pane of the Query dialog box.



Tip To remove rules, highlight the items to remove in the lefthand pane, then click **Remove**.

- Step 6** Click **Apply**.
The selected rules appear in the **Rules** field of the **Query Event Data** bar.



CHAPTER 5

Alerts and Incident Notifications

A Cisco Security Monitoring, Analysis, and Response System (MARS) alert action is a signal transmitted to people or devices, or both, as notification that a MARS rule has fired, and that an incident has been logged. Alert actions can only be configured through the Action parameter of a rule. An alert action determines which alert notification types are sent to which MARS user accounts or user groups.

This chapter contains the following topics:

- [Notification Methods, page 5-1](#)
- [Configure the E-mail Server Settings, page 5-7](#)
- [Configure a Rule to Send an Alert Action, page 5-8](#)
- [Create a User—Role, Identity, Password, and Notification Information, page 5-13](#)
- [Create a Custom User Group, page 5-15](#)
- [Add a User to a Custom User Group, page 5-16](#)

Notification Methods

The content of alert notifications is fixed and cannot be customized. The XML notification contains the most information of all the alert notification types.

MARS can transmit alerts by the methods listed in [Table 5-1](#).

Table 5-1 MARS Incident Notification Methods

Alert Notification Type	Description
Sent in Human-Readable Format	
- E-mail - XML Notification - Short Message Service (SMS) - Pager	E-mail notifications send the incident ID, matched rule, severity, incident time, Top 3 source-destination address pairs, Top 3 source IPs, Top 3 destination IPs, Top 3 destination TCP/UDP ports, Top 3 event types, and Top 3 reporting devices in the body of the email. For Botnet Traffic Filter rules, Botnet Site information is included in the email (when available). SMS, and pager alerts send the incident ID, matched rule name, severity, and incident time in SMS and pager formats respectively. You must login to the MARS to view all the incident details. XML notification sends an email notification of an incident with an attached XML data file (see Figure 5-1). The XML data file contains the same incident details that can be viewed from the GUI, except for path and mitigation information. The XML data file can be sent as a plain-text file or as a compressed gzip file. The XML data filename is constructed with the incident ID number, for example: CS-MARS-Incident-13725095.xml. You can parse and extract data from the XML file with a custom application. For example, you can integrate the XML data with trouble ticketing software. See Appendix D, “Cisco Security MARS XML API Reference” for further information on the MARS XML notification schema and usage guidelines. MARS SMS text message notifications can be up to 160 characters in length. Because the MARS SMS incident notification exceeds 160 characters, it is sent in three segments. Pager messages are sent through the MARS internal modem. MARS dials a carrier’s IXO/TAP number and uses SNPP to transmit the alpha-numeric page. Pager notifications are still possible when the network is down. Pagers can often receive messages in places where mobile phones are inoperative or forbidden (for instance, hospitals).

Table 5-1 MARS Incident Notification Methods (Continued)

Sent to a Device	
• SNMP trap • Syslog	These alerts send the incident ID, matched rule, severity, incident time, Top 3 source-destination address pairs, Top 3 destination TCP/UDP ports, Top 3 event types, and Top 3 reporting devices to MARS devices or applications, all of which must be properly configured within the MARS device administration pages. See the section, Chapter 2, “Security Threat Mitigation (STM) Task Flow Overview” for information on configuring individual devices to work with MARS.

Alert Notification Procedures [Table 5-2](#) provides links and descriptions of related Alert Action configuration procedures.

Table 5-2 Alert Notification Procedures

Alert Related Procedures	Description
Configure the E-mail Server Settings, page 5-7	To send Email, SMS, and XML notifications, MARS requires that you configure the E-mail Server settings.
Configure a Rule to Send an Alert Action, page 5-8	Complete this procedure to create or modify an alert action.
Create a User—Role, Identity, Password, and Notification Information, page 5-13	Alert notifications can be sent only to user accounts configured on MARS. A new user account can be configured from the User Management tab, or when creating an alert action for a rule. This is where you enter the service provider phone numbers and email addresses for E-mail, SMS, Pager, and XML notification.
Create a Custom User Group, page 5-15	Complete this procedure to create a MARS user group other than the default MARS user groups. Unlike default user groups, custom groups can be edited.
Add a User to a Custom User Group, page 5-16	Complete this procedure to include a newly created user account into a MARS user group.

MARS Incident Notification Examples

This section contains examples of the following notifications:

- [MARS Email Notification, page 5-4](#)
- [MARS Syslog Notification, page 5-5](#)
- [MARS SNMP Trap Notification, page 5-6](#)
- [MARS XML Notification Email Attachment, page 5-6](#)
- [MARS SMS Notification Example, page 5-7](#)

Incident notifications all report Rule ID, Rule Name, incident ID, incident start/end time and Incident Severity. Where applicable, notifications also report the following categories.

- Top 3 source IP and destination IP pairs
- Top 3 Source IP Addresses
- Top 3 Destination IP Addresses
- Top 3 TCP/UCP destination ports
- Top 3 reporting devices
- Top 3 event types
- Top 3 Botnet Sites (Botnet Traffic Filter incidents only)

The following considerations apply:

- Notifications are sent only from the Local Controller.
- Alert notifications cannot be customized.
- The Rule ID number is for internal use only, it has no correspondence to any rule attribute viewable from the MARS GUI or CLI.
- The Top 3 Source IP and Destination IP Pairs category is sorted first by session severity and then by count.
 - If the source or destination IP address is 0.0.0.0, it displays as “N/A.”
- The Top 3 Destination TCP/UCP ports category is sorted first by session severity and then by count.
 - If the source port and destination ports are “0” the destination port displays “N/A” otherwise it displays the actual port number or “0” for port number.
- Top 3 Reporting Devices category is sorted by session count.
- Top 3 Event Types category is sorted first by session severity and then by count.
- All “Top 3” categories display x of y occurrences. where x can be 1 to 3, and y can be 1 to n .
- The field “Count” is the always the count of the firing events that match the rule criteria.
- Because of space limitations, the syslog and SNMP incident notifications do not explicitly label botnet site information.

MARS Email Notification

[Example 5-1](#) shows a typical email alert notification triggered by a Botnet Traffic Filter incident.



Note

The Sudden Increase in Ports category is listed after the Top 3 Reporting Devices when applicable.

Example 5-1 Email Notification With Botnet Site Information

```
From: notifier.pnmars@cisco.com [mailto:notifier.pnmars@cisco.com]
Sent: Friday, June 19, 2009 2:49 PM
To: Lavim Busa (labusa)
Subject: CS-MARS Incident Notification (yellow, Rule Name: labusa-notif)
```

The following incident occurred on "pnmars"

```
Start time:      Fri Jun 19 14:46:22 2009
End time:        Fri Jun 19 14:46:29 2009
```



```

Fired Rule Id: 328056
Fired Rule: labusa-notif
Incident Id: 607632
Incident Severity:yellow

Top 3 src-dest address pairs sorted by severity and count (showing 3 of 9):
1. N/A -> N/A Severity: yellow Count: 54
2. 1.2.3.4 -> 4.5.6.7 Severity: yellow Count: 6
3. 11.22.33.44 -> 41.52.63.74 Severity: yellow Count: 3

Top 3 src ip's address sorted by severity and count (showing 3 of 6):
1. N/A -> Severity: yellow Count: 54
2. 1.2.3.4 -> Severity: yellow Count: 6
3. 11.22.33.44 -> Severity: yellow Count: 5

Top 3 dest ip's address sorted by severity and count (showing 3 of 9):
1. N/A -> Severity: yellow Count: 54
2. 4.5.6.7 -> Severity: yellow Count: 6
3. 41.52.63.74 -> Severity: yellow Count: 3

Top 3 dest TCP/UDP ports sorted by severity and count (showing 2 of 2):
1. 80 Severity: yellow Count: 11
2. 80 Severity: green Count: 8

Top 3 event types sorted by severity and count (showing 3 of 16):
1. Download failed for dynamic filter data file from updater server Severity: yellow Count:9
2. Authentication failure with dynamic filter updater server Severity: yellow Count:9
3. Decryption of downloaded dynamic filter data file failed Severity: yellow Count:9

Top 3 reporting devices sorted by count (showing 1 of 1):
1. asa82 Count: 100

Top 3 sites sorted by count (showing 3 of 3):
1. cisco.com (Type: black) Count: 6
2. whitecisco.com (Type: white) Count: 6
3. altavista.com (Type: grey) Count: 5

For more details about this incident please go to:
https://pnmars/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://pnmars.mars.cisco.com cisco.com/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://192.168.1.10/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://10.2.4.1/Incidents/IncidentDetails.jsp?Incident\_Id=607632

For all incidents occurred recently please go to:
https://pnmars/Incidents/
https://pnmars.mars.cisco.com cisco.com/Incidents/
https://192.168.1.10/Incidents/
https://10.2.4.1/Incidents/

```

MARS Syslog Notification

The rule name, reporting device name and event type is limited to 100, 50 and 50 characters respectively.

[Example 5-2](#) shows a MARS syslog notification.

Example 5-2 MARS Syslog Notification

```

10.2.3.196 Wed Feb 4 14:48:40 2009 <34>Wed Feb 4 14:44:09 2009 %MARS-1-101: Rule 306498
(any) fired and caused green Incident 287020054, starting from Wed Feb 4 14:43:15 2009 to
Wed Feb 4 14:43:19 2009 on gVaAdGOCEW, Top 3 src dest addrs pairsshowing 3 of 6 ;; N/A ->
N/A Severity: green Count: 4 ;; 10.4.11.10 -> 10.1.1.16 Severity: green Count: 1 ;;
10.4.11.10 -> 10.1.1.17 Severity: green Count: 1, Top 3 dest ports showing 3 of 4 ;; 21

```

```
Severity: green Count: 1 ;; 22 Severity: green Count: 1 ;; 23 Severity: green Count: 1, Top
3 event types showing 3 of 3 ;; Built/teardown/permitted IP connection Severity: green
Count: 4 ;; Unknown Device Event Type Severity: green Count: 4 ;; CS-MARS Miscellaneous
authentication message Severity: green Count: 1, Top 3 reporting devices showing 3 of 6 ;;
gq_2 Count: 4 ;; d1_1 Count: 1 ;; d1_3 Count: 1
```

MARS SNMP Trap Notification

All fields use the same enterprise OID, PROTEGO_ENTERPRISE_NUMBER:16686 but use different sub-OIDs, as follows:

```
enterprises.16686.1.0 string "MARS-1-101"
enterprises.16686.2.0 string "<alert_content>"
enterprises.16686.3.0 string "<optional_port_list_for_sudden_traffic_increase_incident>"
enterprises.16686.4.0 string "<Top 3 src-dest address pairs>"
enterprises.16686.5.0 string "<Top 3 dest TCP/UDP ports>"
enterprises.16686.6.0 string "<Top 3 event types>"
enterprises.16686.7.0 string "<Top 3 reporting devices>"
```

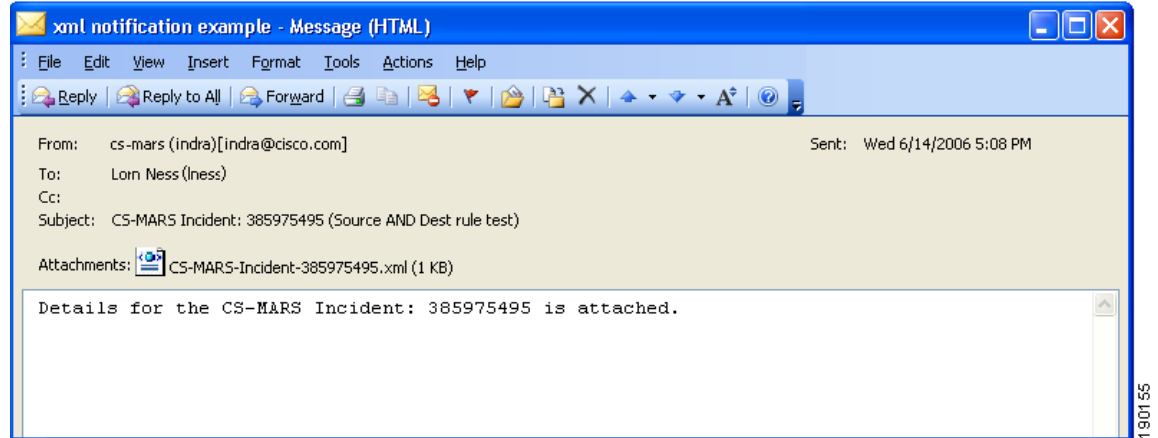
[Example 5-3](#) shows a MARS SNMP trap notification message.

Example 5-3 MARS SNMP Notification

```
SNMPv2-SMI::enterprises.16686.10.2.3.196 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
SNMPv2-SMI::enterprises.16686.2.0 "<34>Wed Feb 4 14:44:09 2009 %MARS-1-101: Rule 306498
(any) fired and caused green Incident 287020054, starting from Wed Feb 4 14:43:15 2009 to
Wed Feb 4 14:43:19 2009 on gVaAdGOCE-W" SNMPv2-SMI::enterprises.16686.4.0 "Top 3 src-dest
address pairs sorted by severity and count showing 3 of 6, N/A -> N/A Severity: green
Count: 4, 10.4.11.10 -> 10.1.1.16 Severity: green Count: 1, 10.4.11.10 -> 10.1.1.17
Severity: green Count: 1" SNMPv2-SMI::enterprises.16686.5.0 "Top 3 dest TCP/UDP Ports
sorted by severity and count showing 3 of 4, 21 Severity: green Count: 1, 22 Severity:
green Count: 1, 23 Severity: green Count: 1" SNMPv2-SMI::enterprises.16686.6.0 "Top 3
event types sorted by severity and count showing 3 of 3, Built/teardown/permitted IP
connection Severity: green Count: 4, Unknown Device Event Type Severity: green Count: 4,
CS-MARS Miscellaneous authentication message Severity: green Count: 1"
SNMPv2-SMI::enterprises.16686.7.0 "Top 3 reporting devices sorted by count showing 3 of
6, gq_2 Count: 4, d1_1 Count: 1, d1_3 Count: 1"
```

MARS XML Notification Email Attachment

[Figure 5-1](#) shows an XML notification with its attached XML data file. When compression is configured, the XML data file arrives as a GZIP compressed file.

Figure 5-1 MARS XML Notification Email Attachment

MARS SMS Notification Example

Example 5-4 shows a Simple Message Service notification.

Example 5-4 MARS SMS Notification

```
From: notifier.gVaAdGOCEW@cisco.com [mailto:notifier.gVaAdGOCEW@cisco.com]
Sent: Wednesday, February 04, 2009 2:05 PM
To: Yi Lin (yilin)
Subject: CS-MARS Incident Notification(yellow,Rule Name:System Rule: DoS: Network -
Attempt)
Incident Id:287020048
```

Configure the E-mail Server Settings

To send alert actions, MARS must be configured to communicate with an e-mail server.

To configure the e-mail server settings, follow these steps:

Step 1 Click **Admin > Configuration Information**.

The Device Configuration window appears, as shown in Figure 5-2.

Figure 5-2 MARS Device Configuration Window

CS-MARS Device Config

→ Name:

Interface Name	IP Address				Net Mask				Default Gateway			
eth0	10	89	149	151	255	255	255	128	10	89	149	254
eth1	192	168	1	100	255	255	255	0				

→ Mail Gateway:

IP:Port :

Email domain name: (ex: Enter 'domain1' for user@domain1)

- Step 2** In the **IP:Port** field of the Mail Gateway section, enter the IP address and **Email Domain Name** of your Mail Gateway server.
- Step 3** Click the **Update** button at the bottom of the page to update the MARS configuration. The e-mail server settings for sending alert actions are configured.

Configure a Rule to Send an Alert Action

To send alert notifications to individual users or groups of users, configure the Action parameters of a rule to create an alert action. This procedure configures alerts for pre-existing rules. When you create a rule, the Action parameters are configured after the count number parameter.

**Note**

Drop rules do not have Action parameters and cannot trigger alerts.

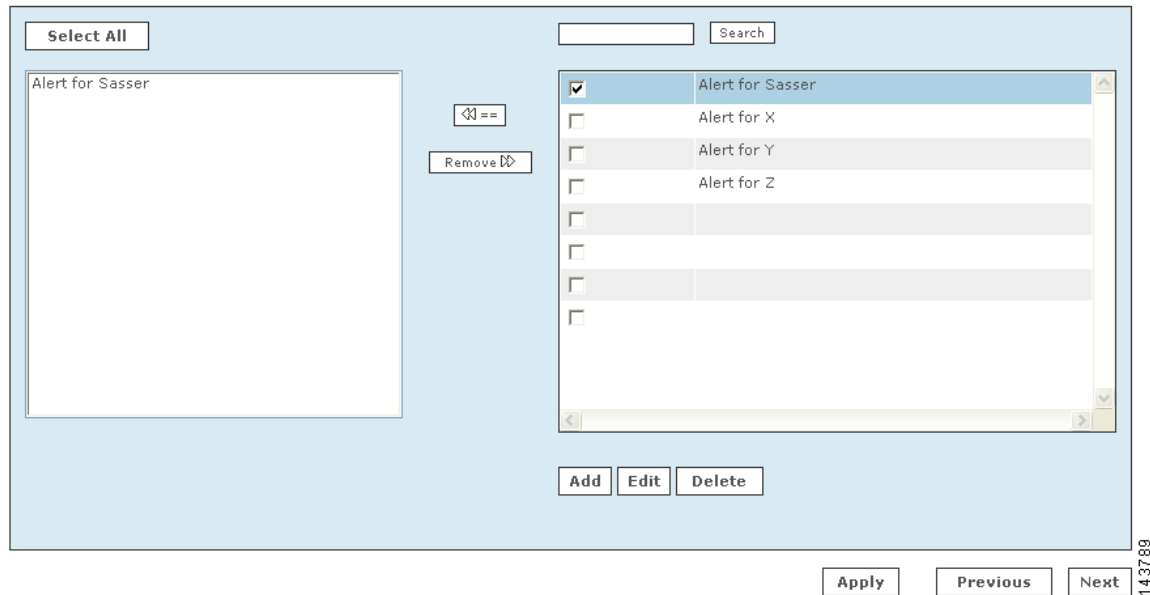
To modify or create an alert for an existing rule, follow these steps:

- Step 1** Click the **RULES** tab to navigate to the Inspection Rules page.
- Step 2** Identify the Rule to configure, and click the value displayed in the **Action** field.

The Action Selection dialog box, as shown in [Figure 5-3](#), appears below the rule description table. All defined alert actions are listed in the right-hand area of the Action dialog box. An alert action determines which alert notifications are sent to which users or user groups when the rule fires. You can edit or delete existing alert actions or create a new one.

Figure 5-3 Action Selection Dialog

Action

**Step 3** Perform one of the following sub-procedures:

- Remove an alert action that is applied to the rule.
 - a. In the left-hand area, pick the alert actions to remove with Ctrl+Click, then click **Remove >>**.
The alert action is deleted from the left-hand area.
 - b. Proceed to [Step 13](#) to complete the procedure.
- Apply an existing alert action to the rule.
 - a. In the right-hand area, click the check boxes of the alert actions you require, then click **<<==**.
The alert action appears in the left-hand area.
 - b. Proceed to [Step 13](#) to complete the procedure.
- Delete an existing alert action from MARS.
 - a. Click the check box of the alert action in the right-hand area, then click **Delete**.
A delete verification window appears.
 - b. Click **Yes**.
The alert action is deleted from the right-hand area.
 - c. Proceed to [Step 13](#) to complete the procedure.
- Edit an existing alert action.
 - a. Click the check box of the alert action in the right-hand area, then click **Edit**.
The Alert recipients page appears in a new window, as shown in [Figure 5-4](#).
 - b. Proceed to [Step 4](#) to complete the procedure.
- Create a new alert action.
 - a. Click **Add**.

The Alert recipients page appears in a new window, as shown in [Figure 5-4](#).

- b. Proceed to [Step 4](#) to complete the procedure.

Figure 5-4 Alert Recipients Window

Name:

Description:

☐ Email

☐ Syslog

☐ Page

☐ SNMP

☒ SMS

☒ XML Email

☐ Compress

251096

Step 4 For a new alert enter a name and description in the **Name** and **Description** fields. If editing an existing alert, you can modify the name or description.

Step 5 Click the check box of a notification type to select or deselect it.

Recipients for the notification types are as follows:

- **E-mail**—Users or user groups can receive an e-mail.
- **Page**—Users or user groups can receive an alpha-numeric electronic page on their pagers or pager-enabled mobile telephones.
- **SMS**—Users or groups can receive a text message on their SMS-enabled mobile telephones.

- **XML Email**—Users or groups can receive an email message with incident details appended in an XML data file. Click the **Compress** check box to send the XML data file as a compressed gzip file. For more information on this feature, see [Appendix D, “Cisco Security MARS XML API Reference”](#).
- **Syslog**—Specified devices can receive syslog messages. Non-reporting devices, such as as a syslog server, are added to MARS as a Software security application on a host, and viewed on the page, **Management > IP Management > Host**
- **SNMP**—Specified devices can receive SNMP trap information. See, Syslog above.



Note For SNMP and Syslog, you must configure the receiving systems to receive notifications.

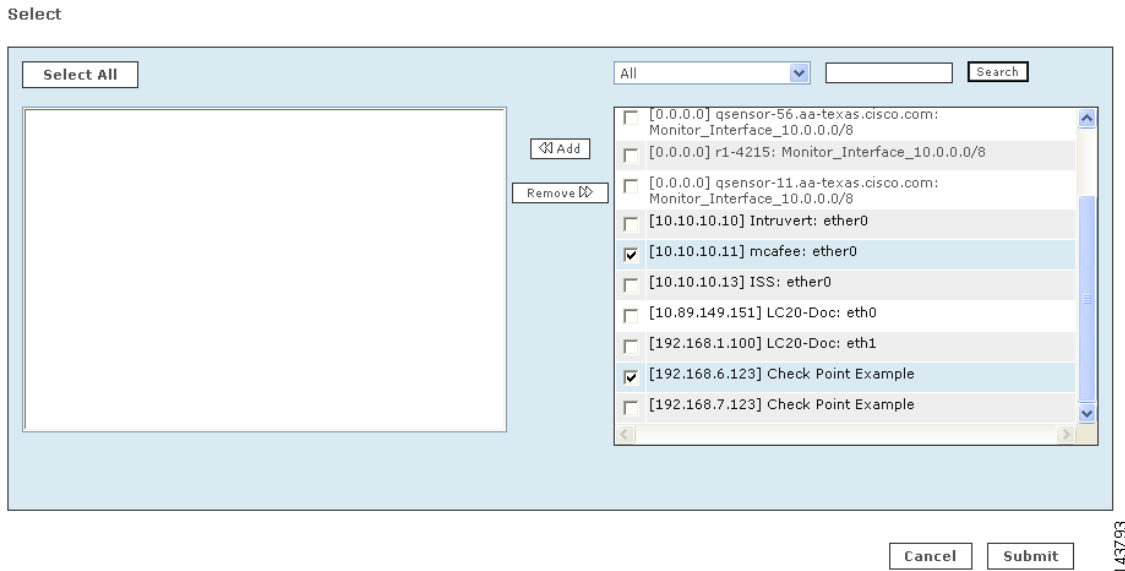
- Step 6** Click the **Change Recipient** button to add or remove a recipient for a notification type. For E-Mail, Page, SMS, and XML Email, the Select (recipient) dialog box appears, as shown in [Figure 5-5](#).

Figure 5-5 Select Recipient Dialog Box

Select

The dialog box is titled "Select". It features a header bar with a "Select All" button and a dropdown menu currently set to "All Users". Below the header is a search input field with a "Search" button. The main content area is divided into two panes. The left pane displays a list of selected recipients, currently containing "Lucre, Phremeus (slimy)". Above and below this list are "Add" and "Remove" buttons, respectively. The right pane displays a list of available users, each with a checkbox: "Administrator (pnadmin)", "Gallus, Cornelius (pnadmin2)", "Lucre, Phremeus", and "Test, GC (gcTest)". Below this list are "Add", "Edit", and "Delete" buttons. At the bottom right of the dialog are "Cancel" and "Submit" buttons.

For Syslog and SNMP, the Select (device) dialog box appears, as shown in [Figure 5-6](#).

Figure 5-6 **Device Selection Page**

For Distributed Threat Management notification, the Select (IOS-IPS Devices) dialog appears (not shown).



Tip If you do not know the group to which a user or device belongs, select **All** from the dropdown list to view all users or devices.

- Step 7** Click the check box next to the users or device you want to receive the notification, then click << **Add**. Your selections appear in the left-hand area. To remove items, Ctrl+click the items in the left-hand area, then click **Remove**. The items are then deleted from the left-hand area.
- Step 8** If you are not adding a user, skip to Step [Step 9](#). To add a new user, do the following substeps:
- Click **Add**.
 - The User Configuration page appears in a separate window, as shown in [Figure 5-7](#).
- Step 9** Click **Submit**.
You are returned to the [Figure 5-4](#).
- Step 10** Repeat Step [Step 6](#) through [Step 9](#) until you have assigned recipients to all the notification types you have selected.
- Step 11** Click **Submit**.
You are returned to the [Figure 5-3](#). Any newly created or edited action alert appears in the right-hand area.
- Step 12** Click the check boxes next to the action alerts to be sent when the rule fires. Click << **Add**.
Your selections appear in the left-hand area.
- Step 13** Click **Next**.
The Time Range dialog may or may not appear.

- Step 14** Click **Next** if the Time Range dialog appears.
The Rule Summary table appears.
- Step 15** Click **Submit** to save your changes to the rule.
- Step 16** Verify that the alert actions you selected appear in the Action field of the rule description.



Note An inactive rule is made active by applying an alert action. To inactivate a rule, select the rule and click **Change Status**.

Create a User—Role, Identity, Password, and Notification Information

New user accounts and user groups are created on the **Management > User Management** tab, or as a substep in creating an alert notification recipient (with the **Add** button on the Select [user] dialog).

To create a MARS user, follow these steps:

- Step 1** Navigate to the User Management page by either of the following methods:
- Click **Add** on the **Management > User Management** tab.
 - Click **Add** on the Select (user) dialog box when creating an alert notification. See [Configure a Rule to Send an Alert Action, page 5-8](#).

The User Configuration page appears, as shown in [Figure 5-7](#).

Figure 5-7 *User Configuration Page*

Role: Admin

Login: pndadmin

Password:

Re-enter password:

First Name:

Last Name:

Organization:

Email:

SMS:

Work Phone:

Home Phone:

Fax:

Pager: (Cell phone or pager number e.g: 4082345678)

Service Provider:

Step 2 From the **Role** field, select a role for the user.

- **Admin**—has full use of the MARS.
- **Notification Only**—for a non-user of the MARS appliance, use this to send alerts to people who are not administrators, security analysts, or operators.
- **Operator**—has read-only privileges.
- **Security Analyst**—has full use of the MARS, except read-only access to the Admin tab.

Step 3 Create or change the user's password if necessary.

Step 4 Enter the user's credentials and personal information, which may include any of the following:

- First name
- Last name
- Organization name
- Email address
- Short Message Service (SMS) number—for example, 8885551212@servprov.com
- Work telephone number
- Home telephone number
- FAX number
- Pager number or ID—may also be a mobile telephone number, for example, 5552345678

Step 5 If you are not creating a notification by pager, go to [Step 10](#).

Step 6 For notification by pager, you must specify a service provider (cell phone or pager company). From the Service Provider field, select **New Provider**.

This pull-down menu is populated as you add new providers.

Additional service provider information fields appear on the same page, as shown in [Figure 5-8](#).

Figure 5-8 Service Provider Fields to Add or Change a Service Provider

Step 7 In the **Provider Name** field, enter the name of the service provider.

Step 8 In the **Provider Phone No** field, enter the service provider's telephone number.

This is the number the service provider requires for accepting alpha-numeric messages using the IXO/TAP protocol. The format is like a regular phone number, such as: 18001234567. The format of 1-800-1234567 is also acceptable. If dialing "9" is required to access a number outside your private branch exchange, type a "9," before the full telephone number (for example, 9,1-800-1234567).

Step 9 In the **Provider Baudrate** field, enter the baud rate specified by the provider.

This is the baud rate the service provider requires for the specified phone number. Common values are 1200, 2400, 4800, and 9600.

Step 10 Click **Submit**.

The new user is created, the User Configuration page is closed, and you are returned to the **User Management** tab.

Create a Custom User Group

You can create a custom user group to help organize the user accounts on your system.

To create a custom user group in addition to the default groups created by MARS, follow these steps:

Step 1 Navigate to the **Management > User Management** tab.

Step 2 Click **Add Group**.

Step 3 In the **Name** field, enter a name for the group.

Step 4 To add users to the group, click the check box of users from the list on the right-hand area. Click **Add**. The checked names appear in the left-hand side of the dialog box.

To remove users from the group, pick the users from the left-hand side with Ctrl+click. Click **Remove**.

The selected names appear in the right-hand side of the dialog box.

Step 5 Click **Submit**.

You are returned to the User Management tab.

Add a User to a Custom User Group

Once you've defined a custom user group, you can add any users that are already defined to that group.

**Note**

The user is added to the user group that corresponds to their role. Admin, Operator, Notification, and Security Analyst are system user groups and cannot be edited.

To include a user in a custom user group, follow these steps:

- Step 1** Navigate to the **Management > User Management** tab.
 - Step 2** Select the User Group to edit from the **Select Group** dropdown list.
The members of the group are displayed.
 - Step 3** Click **Edit Group**. The User Group dialog box appears.
 - Step 4** Check the users to add to the group from the list on the right hand side. Click **Add**. The checked names move to the left-hand area of the dialog box.
 - Step 5** Click **Submit**.
You are returned to the User Management tab.
The user is added to the custom user group.
-



CHAPTER 6

Management Tab Overview

Use the management features in the Local Controller to assign: event, addressing, service, and user information. This information is used in rules, queries, and to determine false positives.

This chapter contains the following topics:

- [Understanding the Activate Button, page 6-1](#)
- [Event Management, page 6-2](#)
- [Using Event Groups, page 6-2](#)
- [IP Management, page 6-3](#)
- [Service Management, page 6-8](#)
- [User Management, page 6-11](#)

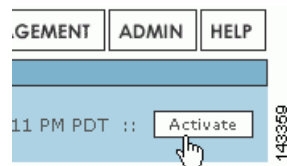
Understanding the Activate Button

In general, you need to activate changes in the Management tabs if the changes are part of a rule. If a change is made that requires activation, the color of the Activate button turns from gray to red. If you plan to make a series of changes, it may be more efficient to perform all of the changes and then click **Activate**. Activate instructs the MARS Appliance to pick up changes and apply them to the running system.

To activate a set of management additions or changes, follow these steps:

-
- Step 1** Make one or more changes.
- Step 2** When changes (or additions) are complete, activate them by clicking Activate.

Figure 6-1 Clicking the Activate Button



The MARS Appliance picks up the changes and applies them to the running system

Event Management

To open the Event Management sub-tab, click the **Management > Event Management** tabs.

On the Event Management page, you can search for and filter events and event groups, and work with groups of events.

Search for an Event Description or CVE Names

You can search for partial matches of event descriptions or Common Vulnerabilities and Exposures (CVE) names.

-
- Step 1** Enter the text that you want to search for in the **Search** field.
- Step 2** Click **Search** .
-

View a List of All Currently Supported CVEs

You can generate a list of all Common Vulnerabilities and Exposures (CVEs) currently supported.

-
- Step 1** Enter CVE into the **Search** field.
- Step 2** Click **Search**.
-

Using Event Groups

Using and creating event groups is one of the most powerful ways to employ rules. You can take any of the events presented here, group them, and then use them with rules to concentrate your searches for attacks.

Filtering by Event Groups or Severity

From the appropriate list, select the group or severity.

Edit a Group of Events

**Note**

You cannot edit system-defined groups.

-
- Step 1** Select the group in the Select Group list.
- Step 2** Click **Edit Group**.

- Step 3** Click each group in the Chosen and Available fields to select it. Click it again to deselect it.
- Step 4** Click **Add** or **Remove** to move highlighted items as needed.
- Step 5** Click **Submit**.
-

Add an Event Group

- Step 1** Click **Add**.
- Step 2** In the Name field, enter a name for the group.
- Step 3** In the Available field, click each group that you want to add to select it. Click it again to deselect it.
- Step 4** Click **Add**.
- Step 5** Click **Submit**.
-

IP Management

The IP Management page, accessed by clicking **Management > IP Management**, enables the definition of network assets that you use as building blocks for inspection rules, drop rules, reports and queries, topology discovery schedules, and in defining reporting devices and mitigation devices. You can define assets as networks, IP ranges, or hosts. You can also defined named variables for use within inspection rules.

The vulnerability assessment information that you define for a host—specifically the operating system type and patch level and the known services that run on the host—assists MARS in determining false positives.



Tip

You can filter the list of objects displayed by the View list box. This selection allows you to filter to hosts, networks, IP ranges, or variables.



Note

A Global Controller pushes any global IP Management Groups to the active Local Controllers that it manages.

This section contains the following topics:

- [Search for an Address, Network, Variable, or Host, page 6-4](#)
- [Filter IP Management List, page 6-4](#)
- [Edit an IP Group, page 6-4](#)
- [Add an IP Group, page 6-4](#)
- [Add a Network, IP Range, or Variable, page 6-5](#)
- [Add a Host to a Local Controller, page 6-5](#)
- [Edit Host Information on a Local Controller, page 6-7](#)

Search for an Address, Network, Variable, or Host

-
- Step 1** Select **Management > IP Management**
- Step 2** Enter the text that you want to search for in the **Search** field.
- Step 3** Click **Search**.
-

Filter IP Management List

The IP Management tab includes the filter options for view and group that you can use to display a shorter, filtered list.

Perform either of the following filter steps, as desired:

-
- Step 1** From the **View** dropdown list, select a view. Choices include the following:
- Variable
 - Network
 - IP Range
 - Host
 - All
- Step 2** From the **Select Group** dropdown list, select a group.
-

Edit an IP Group

-
- Step 1** Select **Management > IP Management**.
The IP Management page appears.
- Step 2** Select the group in the **Select Group** list.
- Step 3** Click **Edit Group**.
- Step 4** Click each group in the **Chosen** and **Available** fields to select it. Click it again to deselect it.
- Step 5** Click **Add** or **Remove** to move highlighted items as needed.
- Step 6** Click **Submit**.
-

Add an IP Group

-
- Step 1** Select **Management > IP Management**.
The IP Management page appears.

- Step 2** Click **Add Group**.
- Step 3** In the **Name** field, enter a name for the group.
- Step 4** In the **Available** field, click a group to select it. To deselect an item, click it again.
- Step 5** Click **Add** to move the selected Event Type Groups into the Chosen field.
- Step 6** Click **Submit**.

Add a Network, IP Range, or Variable

- Step 1** Select **Management > IP Management**.
The IP Management page appears.

Figure 6-2 Add a Network, IP Range, or Variable

Type: Network

 Network
 IP Range
 Variables

Network IP:

IP Mask:

143375

Cancel
Submit

- Step 2** Click **Add**.
- Step 3** In the **Type** list select network, IP range, or variable.
- Step 4** For each type, enter the appropriate information.
- **Network**—name, network IP, network mask
 - **IP range**—name and range
 - **Variable**—variable name
- Step 5** Click **Submit**.

Add a Host to a Local Controller

Within MARS, a host is manually or automatically defined as the result of one of the following options:

- A reporting device or mitigation device defined under the Admin > Security and Monitoring Devices tab.
- A host managed by a reporting device defined under the Admin > Security and Monitoring Devices tab, such as a host running Cisco Security Agent and discovered by MARS when processing the logs provided by the CSA Management Console.

- An asset that you want to identify for the purpose of actively interacting with that host from the MARS system, such as third-party syslog sever to which you want to forward syslog messages using alerts.
- A host that is discovered by the system as part of topology discovery. For example, when processing the ARP cache table on a Cisco Catalyst Switch.
- A host involved in a session that, at one time or another, was considered suspicious, such as a potential target of an attack. In this case, MARS will have performed a Nessus and nmap port sweep of the host to identify whether it was likely it had been breached.

Due to these various options, you can have a large number of hosts defined on the IP Management page in the web interface. If you do not have a vulnerability assessment package that is compatible with MARS, you should consider providing as much information as possible about these hosts. For information on configuring the QualysGuard API Server for vulnerability assessment, see the chapter [Qualys QualysGuard Devices](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.

**Note**

If you are attempting to add a host and you are detecting a conflict with a previously defined host, see [Delete a Device, page 3-14](#) for additional troubleshooting information.

To manually add a host, follow these steps:

Step 1 Select **Management > IP Management**.

The IP Management page appears.

Step 2 Click **Add**.

Step 3 In the Type list select **host**.

Figure 6-3 General Information for a Host

Type: Host

↓

General | Vulnerability Assessment Info

→ *Device Name:

→ Access IP:

→ Operating System: Windows

→ NetBIOS Name:

Enter interface information:

Name:	IP Address:	Network Mask:
☐ ether0		

143370

- Step 4** In the **Device Name** field, enter the host's name.
- Step 5** In the **Access IP** field, identify the address used to pull log events from this host, or is used to connect to when performing dynamic vulnerability assessments while investigating detected attacks.
- Step 6** If the host is running a variety of Windows, Solaris, or Linux, select the corresponding value in the **Operating System** field. Otherwise, verify that **Generic** is selected.
- Step 7** If you are running NetBIOS on your network, in the **NetBIOS Name** field enter the name associated with this host.
- NetBIOS provides name registration and resolution services. MARS uses this setting to provide attack path analysis and address resolution.
- Step 8** Under Enter Interface Information, enter the values for the interface Name, IP Address, and Network Mask.
- Step 9** Add additional IP addresses and masks to the interface, as necessary, by clicking **Add IP/ Network Mask**.
- Step 10** If you have a dual-homed host, you can add additional interfaces by clicking **Add Interface**.

Edit Host Information on a Local Controller

- Step 1** Select **Management > IP Management**.
- Step 2** From the View dropdown list, select **Host**.
- Step 3** Check the box to the left of the host that you want to edit.

- Step 4** Click **Edit**.
- Step 5** Make changes, as necessary, to the following fields:
- Device Name
 - Access IP
 - Operating System
 - NetBIOS Name
- Step 6** To enter or edit interface information for the selected host, you have the following choices:
- To add another interface, click **Add Interface**. Then, on the new line that appears, specify the Name, IP Address, and Network Mask.
 - To remove an interface or IP, check the box to the left of an interface and click **Remove Interface/IP**.
 - To add an IP or Network Mask to an interface, click **Add IP/Network Mask**. Then specify the IP Address, and Network Mask.
- Step 7** Click **Done** when you are finished editing.
- Step 8** After you have made all the changes desired for this administrative session, click **Activate**.

**Tip**

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

Service Management

To open the Service Management sub-tab, click the **Management > Service Management** tabs.

Service is a combination of source port, destination port, and protocol. The Service Management page displays services and their descriptions, ports, and protocols. On the Service Management page, you can work with the services on your networks.

This section contains the following topics:

- [Search for a Service, page 6-8](#)
- [Add a Group of Services, page 6-9](#)
- [Edit a Group of Services, page 6-9](#)
- [Add a Service, page 6-10](#)
- [Edit a Service, page 6-10](#)
- [Delete a Service, page 6-10](#)

Search for a Service

- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Enter the text that you want to search for in the Search field.
- Step 3** Click **Search**.

**Tip**

To filter by service groups, select the group you want from the Select Group list.

Add a Group of Services

-
- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Click Add Group.
- Step 3** In the Name field, enter a name for the group.
The Service Group page appears, with available services listed in the box on the right.
- Step 4** Check the box next to the services to select them (you can click them again to de-select them).
- Step 5** Click <<Add.
The services are listed in the box on the left.
- Step 6** Click **Submit**.
The new group is established and available in the Select Group list.
-

Edit a Group of Services

**Note**

You cannot edit system-defined groups.

To edit the services included in a group of services, follow these steps:

-
- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Select the group in the **Select Group** list.
- Step 3** Click **Edit Group**.
- Step 4** To add an item to the group, check the box next to the service to select it, then click <<Add.

**Tip**

Clicking again deselects the item.

The service(s) are listed in the box on the left.

- Step 5** To remove a service from the group, click on a service (or services) to select it, then click **Remove>>**.
The services are relisted in the box on the right.
- Step 6** When finished editing the list click **Submit**.
-

Add a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Click **Add**.

The Define Service page appears.

Step 3 Enter the service's details, including:

- Name
- Description (your own description)
- Protocol (select from list)
- Source Port (entered either as a value or as a range with high and low values specified)
- Destination Port Port (entered either as a *Value* or as a *Range* with high and low values specified)

Step 4 Click **Submit**.

The service is added.

Edit a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Select the checkbox to the left of the service you want to edit.

Step 3 Click **Edit**.

Step 4 Make changes as required and then click **Submit**.

Delete a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Select the checkbox to the left of the service you want to delete.

Step 3 Click **Delete**.

Step 4 On the confirmation page, click **Yes**.

User Management

This section contains the following topics:

- [Top Level Control, page 6-11](#)
- [Basic User Management, page 6-11](#)
- [Global and Local Controller User Management Functions, page 6-12](#)
- [User Credentials, page 6-12](#)
- [Adding a New User, page 6-12](#)
- [Adding a Service Provider \(Cell phone/Pager\), page 6-14](#)
- [Searching for a User, page 6-14](#)
- [Editing or Removing a User, page 6-15](#)
- [Creating a User Group, page 6-15](#)
- [Adding or Removing a User from a Custom User Group, page 6-15](#)
- [Filtering by Groups, page 6-16](#)
- [Promoting Global User Roles on Local Controller, page 6-16](#)

Top Level Control

MARS supports local authentication of MARS users. The user credentials are stored on the MARS Appliance in SHA-1 cryptographic hash format. Every MARS appliance has a single super administrator account named *pnadmin* by default. This top-level account is distinct from all other other "Admin"-role user accounts that are subsequently created. *Pnadmin* is the only account that can access the device via local console connection or remotely via SSH. The name "*pnadmin*" can not be changed. Despite its unique super-admin privileges to the CLI, the "*pnadmin*" user displays the role "Admin" when viewed in the "User Management" page.

Basic User Management

The User Management page enables you to manage other users and administrators of the MARS system, including the roles and groups to which those users belong. From the User Management page, you can define new user accounts and enable their access to specific features of the web interface. You can also define user-specific notification settings for the user, such as a valid e-mail address or pager number. Some system-wide settings-including pager and cell phone service provider settings-are also accessible exclusively through this page. To access the User Management page, click either **Management > User Management** or **Admin > User Management**.

In MARS, four separate user roles exist that can be assigned to any user who needs to access the web interface:

- **Admin**—This user role has full read/write privileges via the web interface. Users in this role can define new users with any desired role. Users in the role can change the password settings of the accounts in any user role.
- **Security Analyst**—This user role has full read privileges, via the web interface, but is restricted to write for reports privileges. Users in this role can only define new users (and change passwords of users) with the Notifications Only role.
- **Operator**—This user role has read only privileges. Users in this role cannot define new users or change passwords, even of their own user account. However, users in this role can resubmit reports.
- **Notifications Only**—This user role has no permissions to access to the MARS web interface. Use this role to identify users who will receive notifications, such as e-mail, SMS, or pager notifications.

No limit exists on the number of user accounts that can be defined in MARS.

While user roles are system defined, you can define, edit, and delete user groups. For more information, see [Creating a User Group, page 6-15](#) and [Adding or Removing a User from a Custom User Group, page 6-15](#).

Global and Local Controller User Management Functions

Users created on the Global Controller are propagated down to the Local Controller .

When you create users with the same login name or the same first name/last name combination on both the Global Controller and a Local Controller, both appear in the list of users on the Local Controller: once as a local user, once as global.

Global users are maintained only on the Global Controller; local users are maintained only on individual Local Controllers. Users created on Local Controllers are not propagated up to the Global Controller. If you want a user of a Local Controller to have access to the Global Controller or any of its information, you must also create that user at the Global Controller level.

User Credentials

Good security practices dictate strong passwords for use with the MARS Appliances. When defining user names and password, keep the following guidelines in mind:

Login names and passwords:

- Can be alphanumeric characters
- Can contain special characters (!, @, #, etc.)
- *Cannot* contain single or double quotes ('or “)
- Are case sensitive

Login names can have up to 20 characters. Passwords can have up to 64 characters.

Adding a New User

Defining a new user involves specifying the username, password, role, contact information, and notification information.

To add a new user, follow these steps:

- Step 1** From the **Management > User Management** tab, click **Add**. The User Configuration page appears, as shown in [Figure 6-4](#).

Figure 6-4 *User Configuration Page*

The screenshot shows the 'User Configuration Page' with the following fields and values:

- Role: Admin
- Login: padmin
- Password: [masked]
- Re-enter password: [empty]
- First Name: Administrator
- Last Name: Administrator
- Organization: Cisco Systems, Inc.
- Email: admin@cisco.com
- SMS: 8887779999@svp.com
- Work Phone: 888-555-1212
- Home Phone: 8885552121
- Fax: 8885558888
- Pager: 8885551212 (Cell phone or pager number e.g: 4082345678)
- Service Provider: TestPage (dropdown menu) [Edit Provider button]

At the bottom right, there are 'Cancel' and 'Submit' buttons. A vertical text '143791' is visible on the right edge of the form area.

- Step 2** From the **Role** list, select one of the following values for the user.
- **Admin**—has full use of Local Controller.
 - **Notification Only**—for a non-user of the appliance, use this to send alerts to people who are not admins, security analysts, or operators.
 - **Operator**—has read-only privileges.
 - **Security Analyst**—has full use of Local Controller, except cannot access the Admin tab.
- Step 3** Create or change the user's password if necessary.
- Step 4** Enter the user's credentials and personal information. The information can include the following:
- First name
 - Last name
 - Organization name
 - Email address
 - PGP Key (on Global Controller only)
 - Short Message Service (SMS) number—for example, 8885551212@servprov.com
 - Work telephone number
 - Home telephone number

- FAX number
- Pager number— may also be a mobile telephone number, for example, 5552345678

Step 5 If you are creating a notification by pager, go to the next section, [Adding a Service Provider \(Cell phone/Pager\)](#), page 6-14, otherwise click **Submit** to complete the procedure for adding a user.

Adding a Service Provider (Cell phone/Pager)

When configuring a notification by pager, add a service provider (cell phone or pager company) by performing the following procedure:

Step 1 From the **Service Provider** field, select **New Provider** from the list. Additional fields appear, as shown in [Figure 6-5](#).

The drop-down list is populated as you add new service providers.

Figure 6-5 Select a New Provider and Provide Contact Details

Provider Name:

Provider Phone No: (e.g: 9,18002345678)

Provider Baudrate:

143372

Step 2 Specify values for the following fields:

- **Provider Name**—The name of the service provider.
- **Provider Phone No**—The service provider's telephone number. This is the number the service provider uses for accepting alpha-numeric messages using the IXO/TAP protocol. The format is like a regular phone number, such as: 18001234567. The format of 1-800-1234567 is also acceptable. If dialing "9" is required to access a number outside your private branch exchange, type a "9," before the full telephone number (for example, 9,1-800-1234567).
- **Provider Baudrate**—The baud rate specified by the provider. This is the baud rate the service provider requires for the specified phone number. Common values are 1200, 2400, 4800, and 9600.

Consult your service provider's website for more information on their baud rates, if necessary.

Step 3 Click **Submit** to close the User Configuration page and return to the User Management tab.

Searching for a User

Step 1 Enter the text that you want to search for in the **Search** field.

Step 2 Click **Search**.

Editing or Removing a User

-
- Step 1** From the **Management > User Management** tab, check the box next to the user's name.
- Step 2** Do one of the following:
- Click **Delete** to delete the user.
 - Click **Edit** to change the user's configuration information. The User Configuration page appears. Edit the User Configuration page, as necessary.
- Step 3** Click **Submit**.
-

Creating a User Group

-
- Step 1** Click **Add Group**.
- Step 2** In the Name field, enter a name for the group.
- Step 3** To add to the group, check the users from the list on the right hand side. Click **Add**.
The checked names move to the lefthand side of the dialog box.
- Step 4** To remove users from the group, select the users from the left hand side with Ctrl+click . Click **Remove**.
The selected names move to the righthand side of the dialog box.
- Step 5** Click **Submit**.
-

Adding or Removing a User from a Custom User Group

**Note**

Admin, Operator, Notification, and Security Analyst are system groups and cannot be edited. The user is automatically added to the User Group that corresponds to their role.

To add or remove a user from a custom User Group, follow these steps:

-
- Step 1** Select the User Group from the **Select Group** field.
The members of the group are displayed.
- Step 2** Click **Edit Group**.
The User Group dialog box appears.
- Step 3** To add to the group, check the users from the list on the right hand side. Click **Add**.
The checked names move to the lefthand side of the dialog box.
- Step 4** To remove users from the group, select the users from the left hand side with **Ctrl+click** . Click **Remove**.
The selected names move to the righthand side of the dialog box.
- Step 5** Click **Submit**.

You are returned to the User Management tab.

Filtering by Groups

From the **Select Group** list, select a group. Only the members of the selected group are displayed.

Promoting Global User Roles on Local Controller

A global “Admin” user can log into the Local Controller and promote a global “System Analyst” or “Operator” user to a higher role. For example, a global “Operator” can be promoted to become an “Admin” or “System Analyst” on the Local Controller. However, his/her role as an “operator” on the Global Controller remains the same as the changes remain on the local controller and do not get pushed up to the Global Controller. Once these users get promoted to a higher role, they cannot be demoted afterward.

Global “Notification” users cannot be promoted given that these users have no login password information.



CHAPTER 7

Network Summary

This chapter describes the MARS web interface and certain components of the Summary and Admin tabs.

This chapter contains the following topics:

- [Global Controller Network Summary Page Concepts, page 7-1](#)
- [Global Controller Technologies, page 7-1](#)
- [Navigation within the MARS Appliance, page 7-2](#)
- [Help Page, page 7-6](#)
- [Set the GUI and CLI Timeout Interval, page 7-7](#)
- [Set the Logon Banner Message, page 7-9](#)
- [Activate Button, page 7-10](#)
- [Summary Pages, page 7-13](#)

Global Controller Network Summary Page Concepts

The Global Controller Summary page differs from the Local Controller Summary page in the following ways:

- Devices common to Local Controllers are merged in the Global Controller topology. If you have a router listed on both Local Controllers LC1 and LC2, it only shows up once in topology graphs and on the Summary page.
- Networks common to Local Controllers are not merged in the Global Controller topology, but are displayed as separate topologies even if they are the same network.

Global Controller Technologies

The Global Controller is a complete threat mitigation Global Controller that combines network intelligence, ContextCorrelation™, SureVector™ analysis, and AutoMitigate™ capability in a high performance Global Controller indispensable to subvert real security incidents.

ContextCorrelation groups multiple events and network behavior across NAT boundaries in a session. System and user-defined correlation rules are then applied to multiple sessions to identify valid incidents—significantly reducing raw event data and prioritizing response.

SureVector analysis processes incidents to determine if threats are valid or have been countered by assessing the attack path components—end to end. The result eliminates false positives and resolved threats, and enables full path drill-down visualization and investigation.

AutoMitigate capability identifies available choke point devices along the attack vector and allows you to automate appropriate device commands that can mitigate the threat. The result responsively and accurately prevents or contains an attack by leveraging the infrastructure.

Navigation within the MARS Appliance

The MARS web interface runs within a single browser window. The MARS product functions are categorized with labeled tabs, each tab subdivided with subtabs.



Note

Do not use the browser navigation buttons with the MARS Appliance GUI (for example, Back, Forward, Refresh, or Stop).

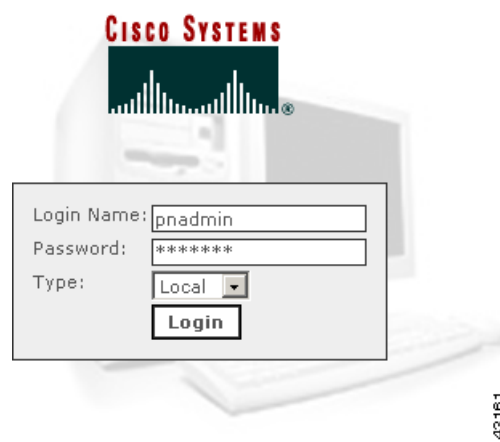
This section contains the following topics:

- [Log In to the Local Controller, page 7-2](#)
- [Log In to the Global Controller, page 7-3](#)
- [Basic Navigation, page 7-4](#)

Log In to the Local Controller

- Step 1** To login to the Local Controller, enter its IP or DNS address into the browser address field.
The login box appears.

Figure 7-1 Local Controller Login Box



- Step 2** Enter your login name and password.
If you do not have a login name, contact your network administrator.

Step 3 From the **Type** drop-down list, select **Local** if you are logging in to a user account created on this MARS, or select **Global** if you are logging in to a user account created on the Global Controller to which this Local Controller reports.

Step 4 Click **Login**.

The first page to appear after a login is the Summary tab Dashboard page. The duration of the delay in displaying information results from a combination of the following causes:

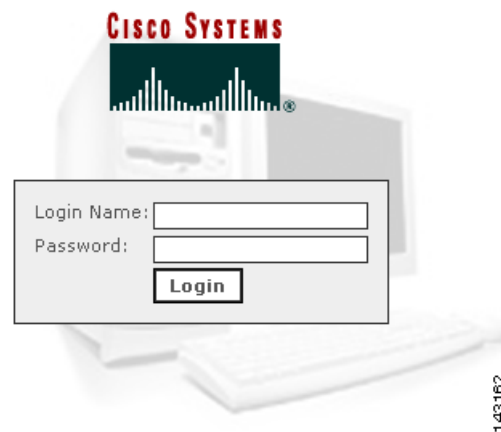
- How long the Local Controller has been powered up and connected to the network.
- Amount of traffic on your networks.
- Reporting syslog levels of the reporting devices.
- Size of the network.
- The number and type of reporting devices.

For most networks, the Summary page populates shortly after configuration. Some values are only relevant after an interval of time. For example, the values in the **24 Hour Events** and **24 Hour Incidents** tables.

Log In to the Global Controller

Step 1 To login to the Global Controller, enter its IP or DNS address into the browser address field. The login box appears.

Figure 7-2 Global Controller Login Box



Step 2 Enter your login name and password.

If you do not have a login name, contact your network administrator.

Step 3 Click **Login**.

The first page to appear after a login is the Summary tab Dashboard page. The duration of the delay in displaying information results from a combination of the following causes:

- How long the Global Controller has been powered up and connected to the network.

- Amount of traffic on your networks.
- Reporting syslog levels of the reporting devices.
- Size of the network.
- The number and type of reporting devices.

For most networks, the Summary page populates shortly after configuration. Some values are only relevant after an interval of time (for example, the values in the **24 Hour Events** and **24 Hour Incidents** tables).

Basic Navigation

The MARS Appliance uses a tab-based, hyperlinked user interface. Elements of the interface, for both the Local and Global Controllers, are illustrated in the figures that follow.

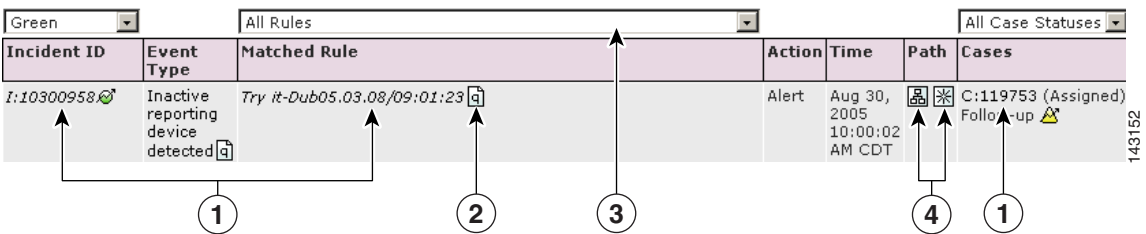
This section contains the following topics:

- [Links, Icons, and Filters for Navigation, page 7-4](#)
- [Tabs for Navigation, page 7-4](#)

Links, Icons, and Filters for Navigation

When you mouse over an alphanumeric string or an icon that is a clickable hyper-link, the mouse cursor changes to a pointing finger cursor . [Figure 7-3](#) shows some of the clickable objects on the Dashboard page.

Figure 7-3 *Links, Icons, and Filters*



Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:10300958 	Inactive reporting device detected 	Try it-Dub05.03.08/09:01:23 	Alert	Aug 30, 2005 10:00:02 AM CDT	 	C:119753 (Assigned) Follow-up 

1	Link to the item’s detail page or popup window.	2	Query icon links to query page. The corresponding query field is populated with the item.
3	Dropdown lists filter what is displayed.	4	Path icons launch Path or Incident Vector pop-up diagrams.

Tabs for Navigation

Click any of the seven tabs to navigate to the pages relevant to the tab’s sub-tabs, as shown in [Figure 7-4](#) through [Figure 7-11](#).

**Note**

Do not use the browser navigation buttons with the MARS Appliance GUI (for example, Back, Forward, Refresh, or Stop).

Figure 7-4 Summary Tab: Global Controller



Figure 7-5 Summary Tab: Local Controller



Figure 7-6 Incidents Tab



Figure 7-7 Query/Reports Tab



Figure 7-8 Global Controller Rules Tab



Figure 7-9 Local Controller Rules Tab

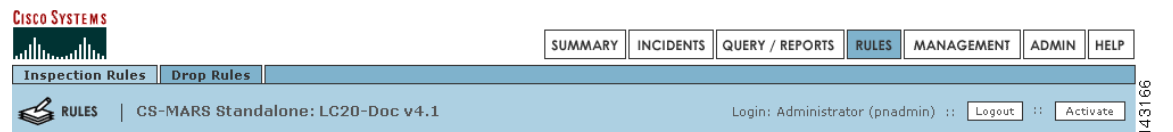
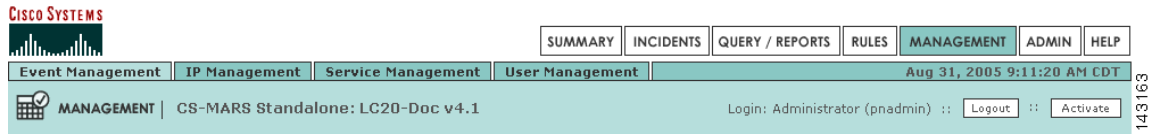
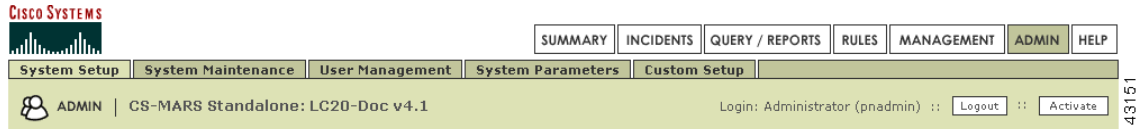
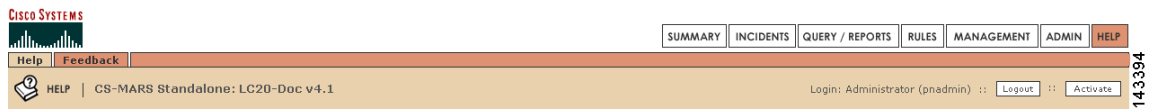
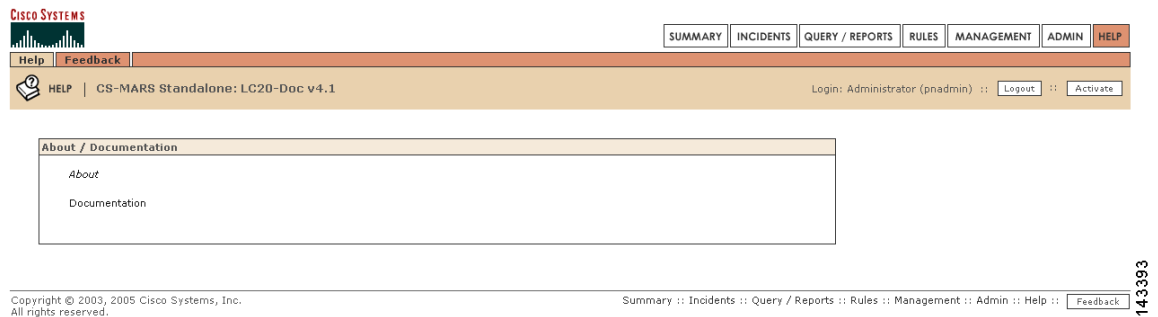


Figure 7-10 Management Tab**Figure 7-11 Administration Tab****Figure 7-12 Help Tab**

Help Page

The Help page, as shown in [Figure 7-13](#), provides URLs to online documentation and a feedback form to submit constructive comments to the MARS development engineering team.

Figure 7-13 Help Page

Click **About** to display the software version number running on the MARS.

Click **Documentation** to display URLs to MARS documentation on the Cisco Systems, Inc. website (<http://www.cisco.com>).

Your Suggestions Welcomed

The **Feedback** button appears at the bottom of most pages, as shown in [Figure 7-13](#).

When you click the feedback button, or navigate to the Feedback page, the feedback dialog box appears, as shown in [Figure 7-14](#).

Figure 7-14 Feedback Dialog Box

CISCO SYSTEMS

Standalone: LC20-Doc v4.1 Login: Administrator (pnadmin) :: Close

Contact Email:
The return email address can be set permanently via User Management.

Subject:

Include log files: ☐

Message:

Submit

143158

To send your comments to the MARS development engineering team, type in your email address and comments then click **Submit**. When you click the **Include log file** a MARS log file is sent with your message.

Set the GUI and CLI Timeout Interval

When a user is inactive on the GUI or CLI for a duration exceeding the timeout interval, that user is logged out and must login again to continue accessing the MARS Appliance. The settings for the timeout interval are **Never** (indefinite duration) **15**, **30**, **45**, and **60** minutes.

In general, GUI activities that initiate access to the MARS webserver restart the timeout interval. [Table 7-1](#) lists GUI activities that do not restart the timeout interval.

Table 7-1 *User Activities That Do Not Restart the Timeout Interval*

GUI Area	Activity
Throughout the GUI	• Mouse Motion • Random keystrokes • Clicking inactive areas • Clicking drop-down lists without selecting • Clicking radio buttons, checkboxes, add remove, or arithmetic operators in configuration dialog boxes • Typing alphanumeric values in text boxes of configuration dialog boxes
Real-Time Event Viewer (Query/Reports > Query)	• Selecting the Scroll Speed • Clicking Pause • Clicking Resume
Incidents Detail Page (Incidents > View)	• Clicking “+” or “-” to expand a table • Clicking Expand All or Collapse All

To set the timeout interval, follow these steps:

Step 1 Navigate to **Admin > System Parameters > Timeout Settings**, as shown in [Figure 7-15](#).

Step 2 Select the timeout intervals for each role.

The timeout interval for the Administrator, Security Analyst, and Operator roles are set separately. The **Admin** timeout setting is also the timeout interval for the CLI.

Figure 7-15 *Timeout Interval Configuration Page*

Set GUI timeout intervals for user roles:

Admin: (Also sets CLI timeout interval)	30 minutes
Security Analyst:	30 minutes
Operator:	30 minutes

Back Submit

Copyright © 2003–2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

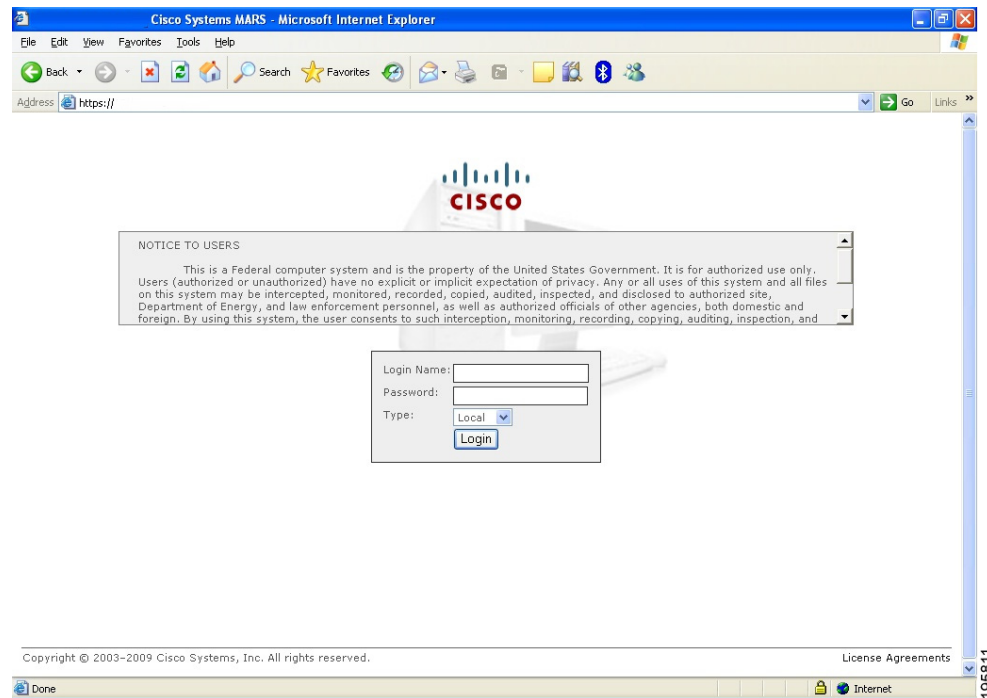
Step 3 Click **Submit**.

End of Procedure

Set the Logon Banner Message

Some MARS administrators or environments require that a message be displayed on the logon page to notify users of authorization requirements or operational restrictions. This message, or logon banner, is configurable by MARS administrators who have the requisite permission. An example of a logon banner message is shown in [Figure 7-16](#).

Figure 7-16 Example Logon Banner Message



Complete the following steps to set the Login Banner Message:

- Step 1** Navigate to the **Admin > System Parameters** page. The System Parameters page appears as shown in [Figure 7-17](#).

Figure 7-17 **Systems Parameters Page**

Copyright © 2003–2009 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Step 2 Click to select Banner Settings. The Banner Message Input page appears.

Figure 7-18 **Banner Message Input Page**

Copyright © 2003–2009 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Step 3 Paste in, or type, the text to be displayed at logon. Note that the maximum number of characters allowed is 2000.

Step 4 Click Submit.

Activate Button

This section discusses the Activate button.

Changes made to MARS configurations and settings, (most notably to devices, rules, and reports) must be passed to the MARS background processes either by clicking **Activate**, or by scheduling an automatic activation process.

**Note**

The activation process is CPU intensive. It is best to activate after all changes are complete. For example, if you are adding multiple devices, it is better for system performance to activate the changes after adding all devices rather than activating after adding each device.

This section contains the following topics:

- [Activate Button Color Changes, page 7-11](#)
- [Global Controller Activation Considerations, page 7-12](#)
- [Automatic Activation Settings Page, page 7-12](#)
- [Set the Activation Interval, page 7-13](#)

Activate Button Color Changes

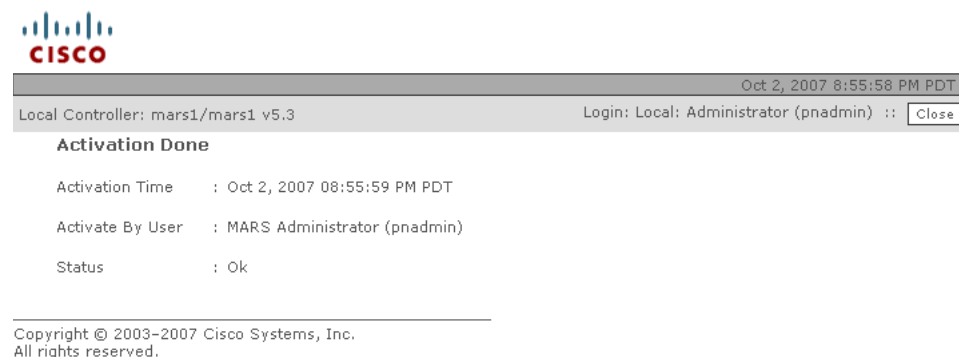
The Activate button displays red with bold italic print when a configuration change requires activation, as shown in [Figure 7-19](#). The Activate button is on all tabs.

Figure 7-19 *Activate Button Turns Red When GUI Configuration Change is Submitted*



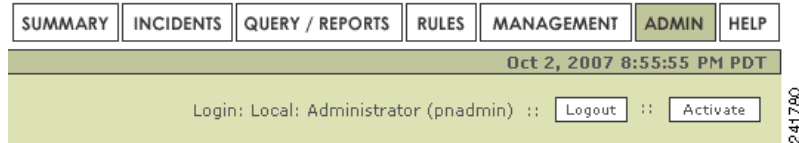
For the user account that made the changes, the Activate button displays red in every new session or already open session of that account. It does not display red in any sessions of any other accounts. When you click the red Activate button, a pop-up window appears displaying the time, login name, user role, and activation status, as shown in [Figure 7-20](#). The Status field can display `Ok`, or `Error`. The action for `Error` is to try again later.

Figure 7-20 *Popup Message Received when Activation Completed*



Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

When an Activation is complete, the Activate button displays white in all open and subsequently launched sessions, as shown in [Figure 7-21](#).

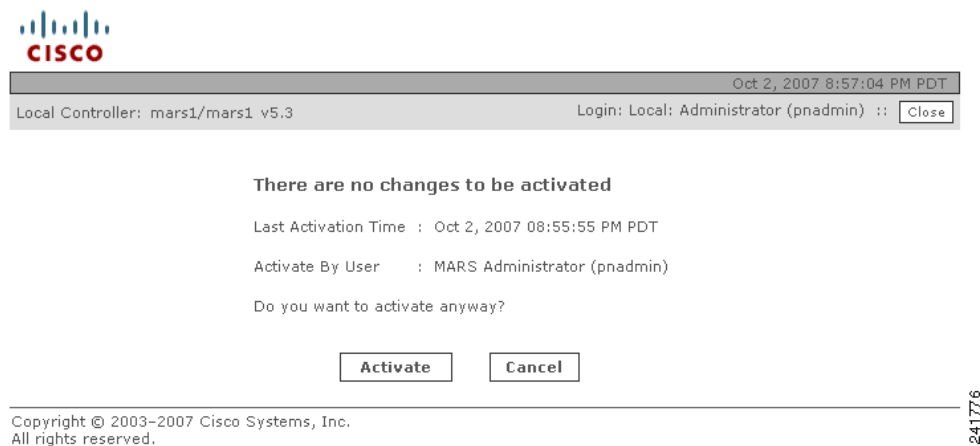
Figure 7-21 Activate Button Resets to White When Activation Completes

Multiple Logged-in Users Making Changes at the Same Time

Clicking Activate, activates all changes made by all user accounts. If two different accounts both make changes, the red Activate button displays in both of their session GUIs. If one account clicks Activate, the changes of all other accounts are also activated, and the Activate button displays white in the GUI of all accounts (after a page refresh, or when clicking another tab).

Clicking the White Activate Button

Clicking the white **Activate** button launches a pop-up message window displaying the last activation event time, the login name and role of the initiator, and an activate option as shown in [Figure 7-22](#). Clicking the Activate option in the pop-up window forces an activation process. Any changes made by other accounts are activated, and an Activation Done pop-up window appears, as shown in [Figure 7-20](#).

Figure 7-22 Popup Message When White Activate Button is Clicked

Global Controller Activation Considerations

A topology synchronization occurs between Global and Local Controllers when an activation process is initiated on either platform.

Automatic Activation Settings Page

A scheduler daemon that wakes up every minute can be configured to execute automatic activations. The Activations Setting Page sets the time interval between automatic activations executed by the scheduler (**Admin > System Parameters > Activation Settings**). There is no CLI command for the scheduler.

The time intervals are **Never** (default), **15**, **30**, **45**, and **60** minutes.

Set the Activation Interval

Complete the following steps to set the automatic activation schedule:

- Step 1** Navigate to the **Admin > System Parameters** page as shown in [Figure 7-17](#).
- Step 2** Click **Activation Settings**.
- The Activation Interval page appears, as shown in [Figure 7-23](#).

Figure 7-23 Automatic Activation Interval Page

Set the interval for automatic activation

Automatic Activation Interval: NEVER

15 minutes
30 minutes
45 minutes
60 minutes

[Back](#) [Submit](#)

Copyright © 2003–2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

- Step 3** Select an Activation Interval from the drop-down list.
- The possible values are **NEVER** (default), **15 minutes**, **30 minutes**, **45 minutes**, and **60 minutes**.
- Step 4** Click **Submit**.
- End of [Set the Activation Interval](#), page 7-13.

Summary Pages

From the Summary pages, you can very quickly evaluate the state of the network. The Summary pages include the **Dashboard**, **Network Status**, **HotSpot Diagrams** (Global Controller only), and **My Reports**, as shown in [Figure 7-24](#) and [Figure 7-25](#).

Figure 7-24 Local Controller Summary Tab

Summary

Dashboard Network Status My Reports ASA Botnet Reports

Aug 11, 2009 1:42:01 PM PDT

Page Refresh Rate

Figure 7-25 Global Controller Summary Tab**Note**

If you experience long page refresh times for the Dashboard or Network Summary pages when changing the query timeframes of charts to values greater than the default (Day), try the following workarounds:

1. Refresh Workaround 1
 - Reset all chart timeframes back to Day.
 - Change a chart timeframe and run the report per your requirements.
 - Reset the chart to Day before changing the next chart timeframe.
2. Refresh Workaround 2
 - Open a new session in a separate browser instance to view a chart.
 - Change the chart time interval and run the report per your requirements.

**Note**

Charts revert to default settings in each new session. The view type and timeframe settings are retained during a session, but the legend display is retained only while the page is viewed.

This section contains the following topics:

- [Dashboard, page 7-14](#)
- [Diagrams, page 7-18](#)
- [Network Status, page 7-20](#)
- [Hotspots, page 7-23](#)
- [My Reports, page 7-24](#)

Dashboard

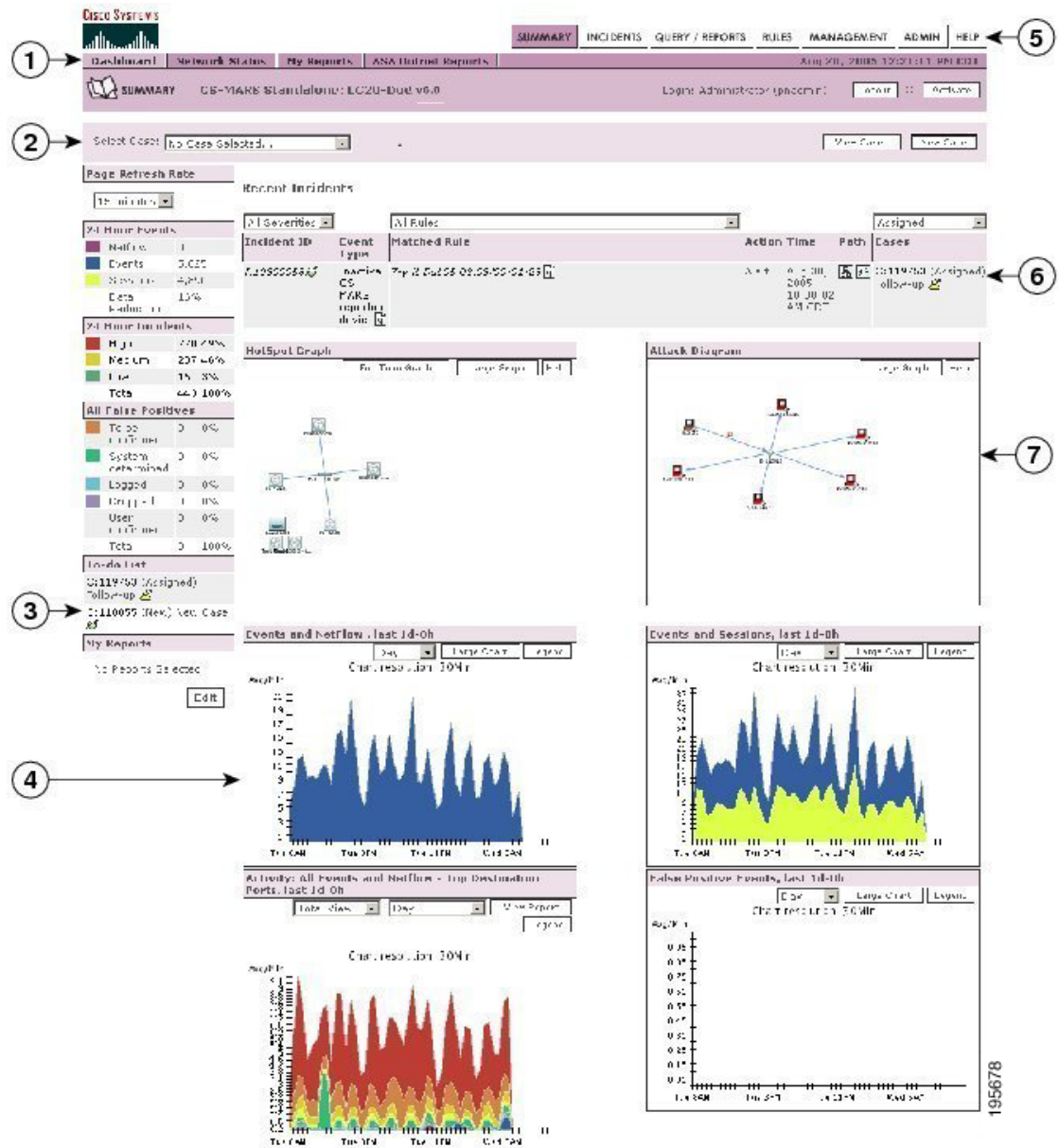
**Note**

When you first view the Summary page after upgrading the MARS, expect a small delay while the Java Server pages recompile.

**Note**

For all of the charts on this page, you can set different query timeframes, toggle the size of the chart, view the latest report, and so on, by clicking on the buttons in the chart's window.

Figure 7-26 The Working Areas on the Dashboard



1	Subtabs	5	Tabs
2	Case Bar (Local Controller only)	6	Recent incidents information
3	Links to Cases assigned to you.	7	HotSpot and Attack diagrams
4	Charts		

This section contains the following topics:

- [Recent Incidents, page 7-16](#)
- [Sessions and Events, page 7-16](#)

- [Inactive Device Events, page 7-17](#)
- [Data Reduction, page 7-17](#)
- [Page Refresh, page 7-17](#)

Recent Incidents

The first feature to notice about the Dashboard is the recent incidents that have fired. Cisco Security Monitoring, Analysis, and Response System (MARS) comes with pre-defined rules, and these incidents are the result of those rules firing. These rules are generic, globally applicable, and should serve you well as a starting point once you begin to tune the MARS.

Figure 7-27 Drilling-down into Incidents

Green		All Rules		All Case Statuses		
Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:10300958 	Inactive reporting device detected 	Try it-Dub05.03.08/09:01:23 	Alert	Aug 30, 2005 10:00:02 AM CDT	 	C:119753 (Assigned) Follow-up 
1	2	3	5	6	7	8
		4				

1	Link to the Incident sessions detail page	5	Link to the rule details page
2	Incident severity icons •  Red—Severe threat •  Yellow—Possible threat •  Green—Unlikely threat	6	Incident Path icon  launches the topology diagram popup window
3	Link to the Event Type Details page	7	Incident Vector icon  launches the incident attack vector diagram
4	Query icon  links to Query page	8	Link to the View Case page

Sessions and Events

Within a given time window, a session is a collection of events that all share a common end-to-end:

- Source and destination address
- Source and destination port
- Protocol

Event sessionization aggregates event data making it easier to sort and examine. Event sessionization lets the system treat events as single units of information and helps you understand if an attack truly has materialized. It gives you the context of the attack by giving you all the events on that session.

Sessionization works across NAT (network address translation) boundaries - if a session traverses a device that does NAT on that session, MARS is able to sessionize events even if they are reported by two devices on either side of that firewall.

Networks start to show immediate action in the events and sessions categories. Note that the 24 Hour Events table and the Events and Sessions chart are different ways of presenting the same information.

Inactive Device Events

MARS generates an inactive device event for any device that does not report an event within 1 hour of the last received event. Inactive device events are generated for all security and monitoring devices except MARS, CSA, Symantec AntiVirus, FoundScan, eEye REM, QualysGuard, and Security Manager.

Data Reduction

Data Reduction is a representation of how much event data MARS collapsed into sessions. For example a data reduction of 66% measures three events per session on the average - this number is dependent on many variables particular to your network.

Figure 7-28 Data Reduction

24 Hour Events	
Netflow	442,302
Events	7,664,847
Sessions	5,896,067
Data Reduction	23%

143404

Page Refresh

The Page Refresh Rate polls the LC/GC TOGGLE according to the setting you assign. The default setting is fifteen minutes. The refresh setting remains the same until you log out. This setting only applies to the pages that have the Page Refresh pull-down.

Figure 7-29 Page Refresh

Page Refresh Rate	
15 minutes	▼
24 Hour Events	
Netflow	0
Events	2,132,436
Sessions	462,803
Data Reduction	78%

143401



Note

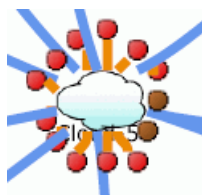
You can change the refresh rate with the dropdown list.

Diagrams

The Summary page has two diagrams: the Hot Spot Graph and the Attack Diagram. The Global Controller uses the configuration and topology discovery information that were propagated up from the Local Controllers. The following table shows you the icons used in the diagrams.

You can start drilling-down into the diagrams by clicking any of the icons listed in [Table 7-2](#). You can start drilling-down attack paths in the Attack Diagram by clicking the Path icon . Drilling-down into these diagrams is one of the fastest ways to uncover real-time information about your network.

Figure 7-30 Clickable Hot Spots: Brown = Attackers & Red = Compromised



Note

Clouds can represent collections of gateways in the Hotspot graph. A gateway cloud is a device that is unknown to MARS. You can discover gateway clouds by clicking them if you have the SNMP information.

Table 7-2 Icons and States in Topology

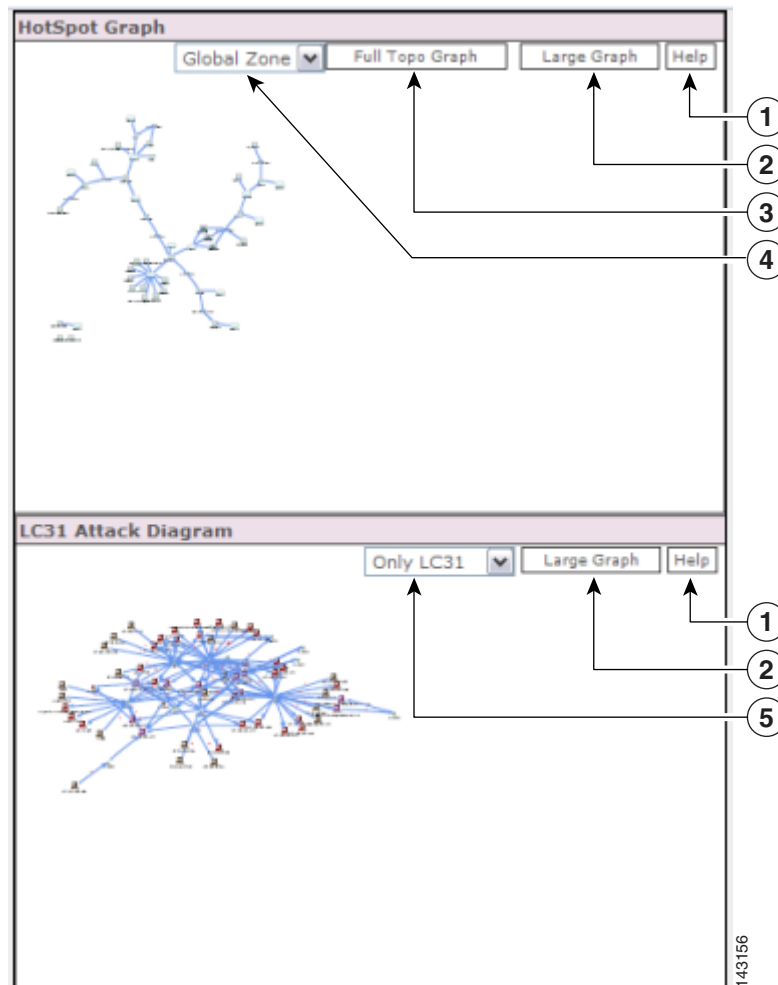
	Healthy	Attacker	Compromised	Compromised and Attacking
Clouds		—	—	—
Firewall				
Reporting Host				
Host				
IDS				
Network				
Router				
Switch				
Global Controller (Global Controller or Local Controller)				

To see the diagrams, you need the Adobe SVG viewer plug-in. The Adobe SVG viewer plug-in should automatically install.



Note

If you click **No** on the SVG auto-installer, MARS does not prompt you to install it again. If you want to run the auto-installer, open the browser and click **Tools > Internet Options > General > Delete Cookies**.

Figure 7-31 The Hot Spot Graph and Attack Diagram

1	Displays SVG Help	2	Displays clouds for selected devices on a full page
3	Displays all devices on a full page	4	Selects zone to be displayed (Global Controller only)
5	Selects zone to be displayed (Global Controller only)		

This section contains the following topics:

- [Diagram Manipulation, page 7-19](#)
- [Display Devices in Topology, page 7-20](#)

Diagram Manipulation

- **Pull down** the menu labeled **Global Zone** to select an individual local zone.
- Right-click the diagram to zoom in and out, to reset the diagram to its original size, to set the diagram's viewing quality, to search, and to manipulate the SVG image.

- **Alt+click** to use the hand to move the image.
- **Ctrl+click** to use the magnifying glass to zoom in.
- **Ctrl+click and drag** to select an area.
- **Ctrl+shift+click** to use the magnifying glass to zoom out.

**Note**

If the MARS discovers an unknown device, it displays that device using a unique name in the form of the string “eth” followed by a hyphen (“-”), followed by the IP address in 32 bit notation, such as “eth-168034561”.

Display Devices in Topology

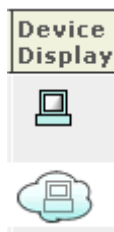
You can specify how to display a reporting device in the HotSpot Graph. By clicking the icon in the Device Display column, you can specify whether to display the device as an individual node on the graph or collapse it within a cloud. By having a device “hidden” in a cloud, you can cut down on the number of devices displayed in the graph, thus making it easier to read at a higher level.

A cloud identifies a collection of networks for which you do not want to define the complete physical topology. Much like when you draw a network diagram on a piece of paper, you can use a cloud to depict networks in which you have no direct interest, but which are needed to represent to complete the diagram. For example, you may want to display only gateway devices or mitigation devices, representing other reporting devices as part of a cloud.

To toggle the display status of a device, follow these steps:

-
- Step 1** Click **Admin > Security and Monitor Devices**.
- Step 2** Click the icon in the Device Display column of the device that you want to toggle.

Figure 7-32 *The Device Display icons*



The icon changes from a host icon to a host within a cloud or vice versa.

- Step 3** Click **Activate**.
-

Network Status

The Network Status page is where you come to get the big picture. On the Network Status page, you can see the charts for:

- **Incidents** —Rated by severity.

- **Attacks: All - Top Rules Fired**—Rated by the highest number of incidents fired.
- **Activity: All - Top Event Types**—Rated by the highest numbers of events of that type.
- **Activity: All - Top Reporting Devices**—Rated by the total number of events reported by each security device.
- **Activity: All - Top Sources**—The top IP addresses that appear as session sources, ranked by session count.
- **Activity: All - Top Destinations**—The top IP addresses that appear as session destinations, ranked by session count.

For all of the charts on this page, you can set different time frames, the size of the chart, view the latest report, and so on, by clicking on the buttons in the chart's window.

Improving Status Display Refresh

If you experience exceedingly long page refresh times for the Dashboard or Network Summary pages when changing the query timeframes of charts to values greater than the default (Day), try the following workaround:

-
- Step 1** Reset all chart timeframes back to *Day*.
- Step 2** Change a single chart timeframe and run the report per your requirements.
- Step 3** Reset the chart to *Day* before changing the next chart timeframe.

**Tip**

Alternatively, you can open a new session in a separate browser instance to view a chart. Then, change the chart's time interval and run the report per your requirements.

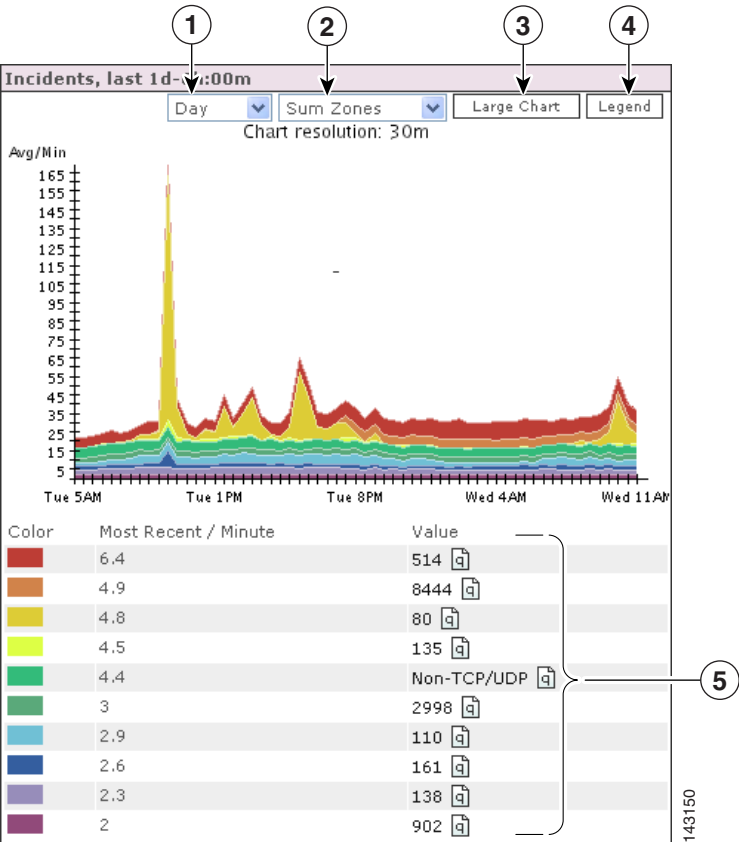
**Note**

Charts revert to default settings in each new session. The view type and timeframe settings are retained during a session, but the legend displays only while the page is viewed.

Chart Reading

These are stacked charts. You can tell which severity of incident your network has most experienced for the day by looking for the dominant shade. In the figure below, low priority green incidents cover less area than high priority red incidents because they have occurred less often.

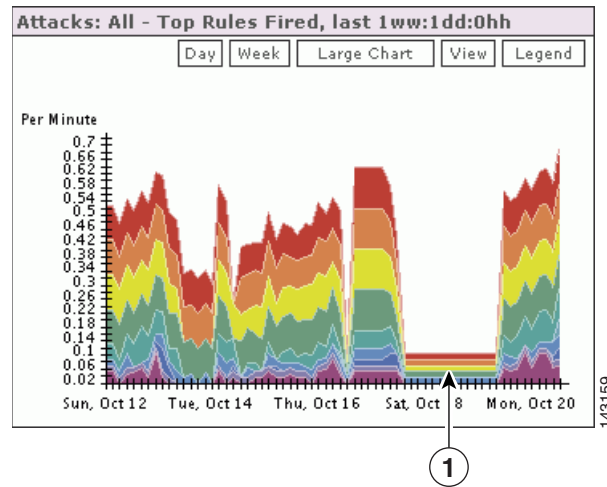
Figure 7-33 A Day's Events and NetFlow with the Legend Displayed



1	Displays values by hour, day, week, month, quarter (the last 3 months), or year.	2	Sets chart to represent the sum of all zones or each individual zone (Global Controller only).
3	Displays a larger version of the chart.	4	Displays the chart legend.
5	The chart legend		

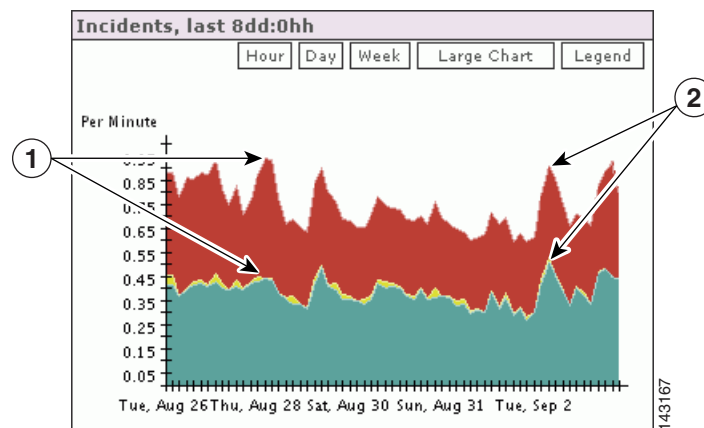
To read the charts most efficiently, note that it is solely the thickness of a particular color that determines its value at that point - and that a spike (or drop) in any particular color could be caused by a spike (or drop) of a different color lower down in the stack.

A perfectly flat line indicates that MARS received no data during that time period.

Figure 7-34 A Flat Line in a Week's Top Rules Fired

1	The flat line in the Top Rules Fired chart

In the following Incidents chart, you can see the top incidents for the week, starting eight days in the past.

Figure 7-35 Eight Days of Incidents

1	A more drastic spike in red is not offset by the green incident	2	Incident spikes are built upon each other

Hotspots

The Hotspots page contains topology graphs of the hotspots on each of the Local Controllers connected to your Global Controller. You can use the pull-down menu to select whether to view the hotspot for a single Local Controller or combined hotspots for all the Local Controllers connected to your Global Controller.

Clicking on the **Full Topo Graph** button displays a detailed graph of the topology; clicking the **Large Graph** button displays the attack on a full page. Clicking the Details button logs you into the Local Controller and displays the hotspot graph there.

My Reports

The My Reports page is where you can choose the reports that you want to view. As long as you are using the MARS with your log-in name, the reports that you have selected appear here.

Set up Reports for Viewing

-
- Step 1** Click the **Edit** button on the My Reports page.
- Step 2** Select the radio button next to the report that you want to see as a chart.
- Step 3** Click **Submit**.
- LC/GC TOGGLE now displays the chart that you selected on the My Reports page.



Note Reports must be scheduled to run periodically, that is, every hour or every day. If you activate a report, allow for some time for the data to accumulate.

You can display any number of charts on the My Reports page, however expect slower loading times for large numbers of charts.

The reports that you can select from are pre-defined. When you create your own reports, you can select those to display. See [Reports, page 8-26](#) for more information.



CHAPTER 8

Queries and Reports

MARS provides a variety of features for defining, viewing, and saving queries and reports. The essential distinction between queries and reports is that queries are typically shorter, reactive, and their specifications not recorded, while reports tend to be longer, and have specifications defined and recorded in the system. However, a query can be saved as a report or a rule for later use, and a report (even a scheduled report) can be run on demand. (For information on rules see [Rules Overview, page 4-1](#); for a list, see the appendix [System Rules by Category, page E-1](#)).

A batch query is a larger scale query that (may) require extensive processing, and is run in the background. Whenever you run a query that appears as though it might require extensive processing, MARS provides you with an option to run it as a batch query, that is, in the background.

MARS comes with a series of "stock" pre-defined reports that you can use as they are, or modify for your particular purpose. Reports can be duplicated or "cloned" and then edited to your particular requirements.

Defining queries and reports within MARS is essentially an exercise in using filters to define the parameters (what, where, when, and who) that comprise the information you wish to view.



Note

Submitting a query or report that is exceedingly general and processes a large amount of data may consume more system resources—or time—than expected. Therefore, it is important to understand the scope of the queries. When you run a query as a batch query, you retain the ability to cancel it.

This chapter contains the following topics:

- [Understanding Queries, page 8-1](#)
- [Query Operations, page 8-12](#)
- [Viewing Events in Real-time, page 8-22](#)
- [Reports, page 8-26](#)

Understanding Queries

From the Query subtab, you can load and run reports as on-demand queries, or define and run a query. Many links from other pages bring you to the query subtab and partially populate the query's criteria. After you have submitted a query, you can save it as a report or a rule.

The scope of queries you can perform at a Global Controller differ from those at the Local Controller. These differences are detailed in the sections that follow:

This section contains the following topics:

- [Global Controller Query Interface, page 8-2](#)
- [Local Controller Query Interface, page 8-3](#)
- [Selecting the Query Type, page 8-3](#)
- [Select Query Criteria, page 8-7](#)
- [Query Criteria Descriptions, page 8-9](#)
- [Saving the Query, page 8-12](#)

Global Controller Query Interface

Queries performed at the Global Controller level are similar to those on an Local Controller, but also include the **Zone** parameter (see item (1) of [Figure 8-1](#)). You can run a query across one or more Local Controllers by specifying their zones. This enables a query at the Global Controller to select zone-specific objects.

When you submit a query from the Global Controller, it is sent out to the Local Controllers specified in the **Zone** parameter. The Local Controllers perform the actual query and send it back to the Global Controller, which then merges and presents the results at the global level.

Figure 8-1 The Global Controller Query Table

The screenshot shows the Cisco MARS Global Controller Query Interface. It includes a navigation bar with tabs like SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The main area contains a 'Query Event Data' section with a 'Query type' dropdown set to 'Event Types ranked by Sessions, 0h:10m' and a 'Zones' dropdown set to 'ANY'. Below this is a table with columns for Source IP, Destination IP, Service, Events, Device, Reported User, IPS Risk Rating, IPS Threat Rating, IPS Global Correlation Score, Keyword, Operation, Rule, and Action. The table has a row with 'ANY' values for most fields. At the bottom right, there are buttons for 'Save As Report', 'Save As Rule', and 'Submit Batch'. Numbered callouts 1 through 7 point to specific UI elements: 1 points to the 'Zones' dropdown, 2 points to the 'Query type' dropdown, 3 points to the 'Clear' button, 4 points to the 'ANY' dropdown in the table, 5 points to the 'ANY' dropdown in the table, 6 points to the 'Save As Report' button, and 7 points to the 'Submit Batch' button.

1	Click on Any to select the zone or zones that contain the Local Controllers you want to query.	2	Click to set the query type and time range criteria. See Selecting the Query Type, page 8-3
3	Click Clear to return query values to default values.	4	Quick query fields permit entry of IP and Service values without opening dialog box for the field.
5	Click on Any under a field value to open the dialog box for that field's criteria selection. See Select Query Criteria, page 8-7 .	6	Save the query as a report or as a rule.
		7	Click Submit Batch to run the query.

Except for the Zone parameter, running queries on the Global Controller and Local Controller is done the same way.

Local Controller Query Interface

Making queries from a Local Controller is nearly identical to the Global Controller process, except that you can not specify a zone (the query simply runs on that Local Controller)

The following table details local queries:

Figure 8-2 The Local Controller Query Table

1	Click to set the query type and time range criteria. See Selecting the Query Type, page 8-3	2	Click Clear to return query values to default values.
3	Quick query fields permit you to enter values without opening dialog box for the field.	4	Click on a field value to open the dialog box for that field. See Select Query Criteria, page 8-7 .
5	Save the query as a report or as a rule.	6	Click Submit Inline to run the query.

Selecting the Query Type

Figure 8-3 Clicking the Query Type or Edit link



You can select different query criteria by clicking the **Query Type** link or **Edit** button as shown in [Figure 8-3](#). [Figure 8-4](#), as shown below, enables you to determine a query's result format, rank, time, whether it only uses only firing events, and the maximum number of rows returned.

Figure 8-4 *The Query Criteria: Result Page*

Result Format:

Order/Rank By:

Filter by Time:

☐ Last: Days Hrs Mins

☒ Start: Hrs Mins

End: Hrs Mins

☐ Real Time

Use Only Firing Events: ☐

Maximum rank returned:

Each of these parameters, and profiles of the possible values within each, is further described in the subsections that follow.

This section contains the following topics:

- [Result Format, page 8-4](#)
- [Order/Rank By, page 8-6](#)
- [Filter By Time, page 8-6](#)
- [Use Only Firing Events, page 8-7](#)
- [Maximum Number of Rows Returned, page 8-7](#)

Result Format

- **Event Type Ranking**—Returns the most reported event types. Ranked by either: number of sessions containing at least one of the event type or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Event Type Group Ranking**—Returns either pre-defined or user defined grouped event types. Ranked by either: number of sessions containing at least one event type contained in the group or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Network Group Ranking**—Returns top network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.
- **Network Ranking**—Returns top networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.
- **Source Network Group Ranking**—Returns top source network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- **Source Network Ranking**—Returns top source networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.
- **Source IP Address Ranking**—Returns source IP addresses. Ranked by number of sessions with that source IP address or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Destination Network Group Ranking**—Returns top destination network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.
- **Destination Network Ranking**—Returns top destination networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.
- **Destination IP Address Ranking**—Returns destination IP addresses. Ranked by either: number of sessions with that destination IP address or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Source Port Ranking**—Returns source ports. Ranked by either: number of sessions with that source port or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Destination Port Ranking**—Returns destination ports. Ranked by either: number of sessions with that destination port or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Protocol Ranking**—Returns most used protocols. Ranked by either: number of sessions with that protocol or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Reporting Device Ranking**—Returns most active reporting devices. Ranked by either: number of sessions that contain events from the device or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Reporting Device Type Ranking**—Returns most active reporting device types. Ranked by either: number of sessions that contain events from a device of that type or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Reported User Ranking**—Returns information about users from reporting devices such as: Windows clients, Solaris clients, etc. Ranked by either: number of sessions that contain events from a reported user or by bytes transmitted in sessions that contain events that meet the query criteria.
- **Matched Rule Ranking**—Returns top firing rules. Ranked by number of incidents.
- **Matched Incident Ranking**—Returns incidents. Ranked by either: number of sessions that contain events that meet the criteria that contributed to the incident or by bytes transmitted real time in sessions that contain events that meet the query criteria.
- **All Matching Sessions**—Returns incidents. Ranked by either: number of sessions that contain events that meet the criteria that contributed to the incident or by bytes transmitted real time in sessions that contain events that meet the query criteria.
- **All Matching Sessions, Custom Columns**—Returns incidents. Ranked by either: number of sessions that contain events that meet the criteria that contributed to the incident or by bytes transmitted real time in sessions that contain events that meet the query criteria. You can customize the number and order of the columns returned by this result format. For more information see [Select Custom Columns for Query Result Display, page 8-19](#).

- **All Matching Events**—Returns events. Ranked by time with the most current first. Real Time results are available for this Result Type.
- **All Matching Event Raw Messages**—Returns the raw messages associated with events. Ranked by time with the most current first. Real Time results are available for this Result Type.
- **NAT Connection Report**—Returns NAT connections. Ranked by time with the most current first.
- **MAC Address Report**—Returns MAC addresses. Ranked by time with the most current first.
- **Unknown Event Report**—Returns events that are not fully processed by the MARS. In some cases, event information such as the five tuple (source IP, source port, destination IP, destination port, and protocol) might not be present, hence can not be queried in real time.
- **Detailed NAC Report**—Returns ACS syslog message elements that have been received and stored by MARS.

Order/Rank By

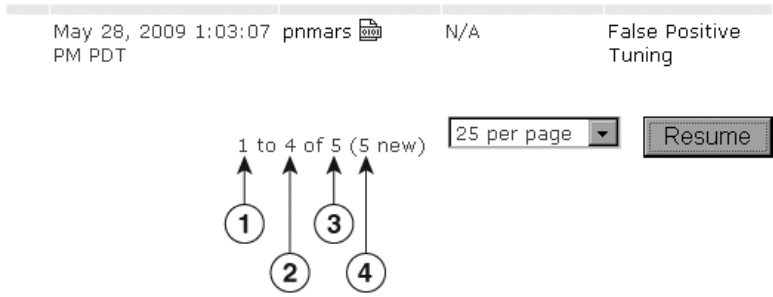
This selection determines the ranking or order of the query's results. These selections are determined by the kind of Result Format that you use when you run the query.

- **Session Count**—The number of sessions that contain events that meet the criteria that contributed to the incident.
- **Bytes Transmitted**—The number of bytes transmitted in sessions that contain events that meet the query criteria.
- **Time**—Most current results appear first.
- **Incident Count**—Largest number of incidents appear first.

Filter By Time

- **Last**—The present time minus the number of days, hours, and minutes entered.
- **Start/End**—The present time minus the number of days, hours, and minutes entered.
- **Real Time**—Streams rolling real-time results from recent past to current time. Result Formats that work in real time are:
 - All Matching Sessions
 - All Matching Events
 - All Matching Event Raw Messages

Real Time results appear in a normal browser window. Moving the scroll bar stops the “rolling” behavior. Clicking Resume on the bottom of the page allows the scrolling to resume.

Figure 8-5 Click Resume to Start the Page Rolling


The screenshot shows a query results page. At the top, there is a header bar with the following information: May 28, 2009 1:03:07 PM PDT, pmnars, N/A, and False Positive Tuning. Below this, there is a pagination control showing '1 to 4 of 5 (5 new)' and a '25 per page' dropdown menu. A 'Resume' button is visible. A diagram with numbered circles 1 through 4 and arrows indicates the row selection process. A vertical text '275998' is on the right side of the page.

1	Top row visible	2	Bottom row visible
3	Total rows queried since start	4	Number of new queries pulled when this page last refreshed per the Page Refresh Rate setting on the Query/Reports > Batch Query page.

Use Only Firing Events

Select this if you want only events that fired incidents to return information.

Maximum Number of Rows Returned

Select the maximum number of rows that you want displayed.

Select Query Criteria

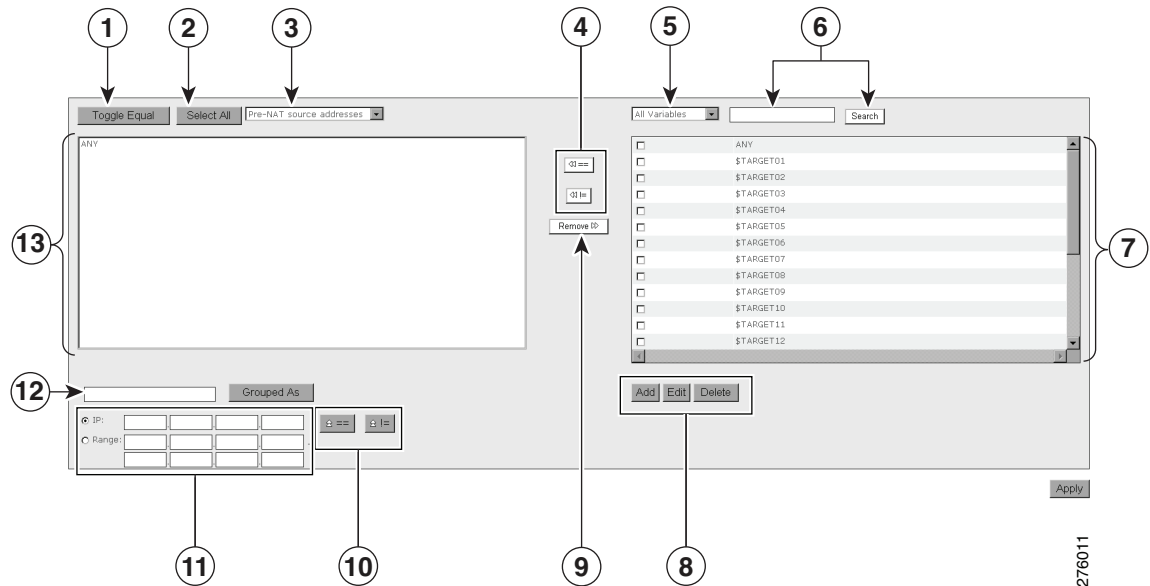
When you initially view the Query Event Data page, most the criteria are set to their default setting: *Any*, as shown in Figure 8-2. You can narrow and filter the criteria by clicking on *Any* under the criterion you wish to narrow. This opens the filtering page for that criterion, from which you select the filter elements to apply.

- Step 1** Select the criterion that you want to filter by clicking on the corresponding word **Any**.

Figure 8-6 Clicking ANY to narrow your criteria, in this case, Destination IP

The filtering page for that criterion appears.

- Step 2** Move the items that you want to query from the right to the left of the filter by selecting the check box next to them, and clicking the Equal and Not Equal buttons.

Figure 8-7 **Selecting Variables**

- Step 3** You can select a variety of different variables, events, devices, addresses from the filter page. The following list numbers correspond with the numbers in the preceding graphic:
1. To change selected source items from equal to not equal, you check the boxes next to the items in the Sources Selected field (13) to select them, and click the **Toggle Equal** button.
 2. To select all items in the Sources Selected field, click the **Select All** button. (Note: if you have items highlighted in the Sources Selected field, clicking **Select All** will de-select them.)
 3. Filter variables with drop-down list, if shown. (Not all variables will present drop-down list.)
 4. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field (7) into the **Sources Selected** field(13).
 5. Filter sources from this drop-down list.
 6. Enter search text, and click **Search** to filter the **Sources Available** list to show items that match the search criteria You can then move all or some of them to the **Sources Selected** field.
 7. The Sources Available list shows items that fit your currently selected criteria.
 8. To add a new item to the Sources Available list, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button. See [IP Management, page 6-3](#) for more information.
 9. To remove an item from the Sources Selected field, click the item or items and click the **Remove** button.
 10. To move IP values up into the Sources Selected field, click the **Equal** (Up) icon, or the **Not Equal** (Up) icon.
 11. To enter an IP address or Range to the Sources Selected field, select the radio button next to **IP** or **Range**, and enter an IP address, or a range of IP addresses, into their respective fields. (Then use the Equal or Not Equal buttons to move the value into the list.)
 12. To group items in the Sources Selected field, select them, enter a group name, and click the **Grouped As** button.
 13. After you have chosen the query criteria that interests you and they are listed in the Sources Selected field (13), click **Apply** to return to the Query page.

You can repeat this selection process for other query data.

Step 4 Click the **Submit** button to run the query.

Query Criteria Descriptions

The following lists describe the selections in the Query Event Data table.

Source IP

- **Pre NAT source addresses**—Specifies that the constraints entered are the session endpoints.
- **Post NAT source addresses**—Specifies that the constraints entered are the source as appearing at the destination.
- **ANY**—No constraint is placed on the source IP addresses.
- **Variables**—Selections include All, Network Groups, All Networks, All Devices, All IP Addresses.
- **IP**—IP address(es) present on devices in the system or user entered dotted quads.
- **Range**—The range(s) of addresses between two dotted quads.
- **Networks**—Topologically valid networks.
- **Devices**—The hosts and reporting devices present in the system.

Destination IP

- **Post NAT destination addresses**—Specifies that the constraints entered are the session endpoints.
- **Pre NAT destination addresses**—Specifies that the constraints entered are the destination as appearing at the source.
- **ANY**—No constraint is placed on the source IP addresses.
- **Variables**—Selections include All, Network Groups, All Networks, All Devices, All IP Addresses.
- **IP**—IP address(es) present on devices in the system or user entered dotted quads.
- **Range**—The range(s) of addresses between two dotted quads.
- **Networks**—Topologically valid networks.
- **Devices**—The hosts and reporting devices present in the system.

Service

- **ANY**—No constraint is placed on the source or destination ports, or the protocol.
- **Service variables**—Any one set of destination port and protocol, only useful for queries in tandem with the same variable.
- **Defined services**—Services on the database. These services will be listed only after you have defined them.

Events

- **ANY**—No constraint on the event type.
- **Event types**—Events that have been merged into types.
- **Event type groups**—Groups of event types.

Device

- **Device**—The reporting devices present in the system. This restricts the query to a subset of the devices that report to the MARS.

Reported User

- **Reported User**—The reported users of the system. This restricts the query to a subset of known users and can include one or many specific users.

IPS Risk Rating

- **IPS Risk Rating**—Can be selected to restrict the query to:
 - Match any event.
 - Match events without a Risk Rating.
 - Match events with a specified Risk Rating. (The value can be expressed as a specific range or by using Boolean operators.) See figure [Figure 8-8 on page 8-11](#).

IPS Threat Rating

- **IPS Threat Rating**—Can be selected to restrict the query to:
 - Match any event.
 - Match events without a Threat Rating.
 - Match events with a specified Threat Rating. (The value can be expressed as a specific range or by using Boolean operators.) See figure [Figure 8-8 on page 8-11](#).

IPS Global Correlation Score

- **IPS Global Correlation Score**—Can be selected to restrict the query to:
 - Match any event.
 - Match events without a Global Correlation Score.
 - Match events with a specified Global Correlation Score. (The value can be expressed as a specific range or by using Boolean operators.) See figure [Figure 8-8 on page 8-11](#).

Figure 8-8 Running a IPS-based query

Query Event Data
Click the cells below to change query criteria:

Query type: **Event Types ranked by Sessions, 0h:10m** [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	> 3.0	ANY	None	ANY	ANY

Filter by IPS Risk Rating, IPS Threat Rating and IPS Global Correlation Score

Apply

IPS Risk Rating

☒ Match any event
☐ Match events without a Risk Rating
☐ Match events with a Risk Rating
Value: -
☒ Also include events without a Risk Rating
(Valid range values are from 0 to 100)

IPS Threat Rating

☒ Match any event
☐ Match events without a Threat Rating
☐ Match events with a Threat Rating
Value: -
☒ Also include events without a Threat Rating
(Valid range values are from 0 to 100)

IPS Global Correlation Score

☐ Match any event
☐ Match events without a Global Correlation Score
☒ Match events with a Global Correlation Score
Value: -
☒ Also include events without a Global Correlation Score
(Valid range values are from -10.0 to 10.0)

Apply

Copyright © 2003–2009 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

134481

Keyword

- **Keyword**—You can use this criteria to restrict the query on the basis of specific strings. You can add multiple strings and use operators such as AND/OR/NOT/None.

Figure 8-9 Running a free-form query

Specify raw message keywords:

Open (	Search String	) Close	Operation	Highlight
	pop3		OR	
	imap		None	
			AND	
			OR	
			NOT	
			None	
			None	
			None	
			None	
			None	
			None	
			None	
			None	

143435

Operation

The operation field is not used as a query criterion. Leave it as the default: *Any*.

Rule

- **Empty field- *Rules Chosen field***—When this field is empty, it acts like an ANY selection. No constraint is placed on the sub-set of events.
- **Rule**—Restricts the query to the sub-set of events that contributed to the incidents of the specified rules firing. Enables you to further specify rule criteria that include:
 - Active system Rules
 - Active User Rules
 - Inactive Rules
 - Specific Rule Groups

Action

- **Empty field - *Empty Actions Chosen field***—When this field is empty, it acts like an ANY selection. No constraint is placed on the subset of events.
- **Actions**—Restricts the query to the subset of events that contributed to the incidents of rules that have the specified notifications as part of their actions.

Saving the Query

You can save your query (criteria selection) to re-use as either a report, or as a rule.

- **Save as a report**—This takes the query that you are using and creates a report. For more information on creating reports, see the [Reports, page 8-26](#) section.
- **Save as a rule**—This takes the query to the rules page, populating the rules with the selected query criteria. Likely, you must identify additional criteria to complete the rule. For more information on creating rules, see [Chapter 4, “Rules”](#).

Query Operations

This section contains the following topics:

- [Run a Quick Query, page 8-12](#)
- [Run a Keyword Query, page 8-13](#)
- [Batch Query Operations, page 8-14](#)
- [Perform a Long-Duration Query Using a Report, page 8-17](#)
- [Select Custom Columns for Query Result Display, page 8-19](#)
- [View a Query Result in the Report Tab, page 8-21](#)

Run a Quick Query

You can use the quick query fields (see item (3) on [Local Controller Query Interface, page 8-3](#)) to enter IP and Service criteria without opening a dialog box for the field. This is a simple way to run a quick query.

To run a quick query, based on IP or Service criteria, follow these steps:

-
- Step 1** From the **Query** subtab, enter any combination of Source IP, Destination IP, or Service into the query criteria fields. To enter a service, you must specify a port and protocol pair.
- Step 2** Click the **Apply** button to load the value(s) into the query criteria table.
- Step 3** Click the **Submit Inline** button to run the query.
- The query results are displayed.
-

Run a Keyword Query

You can quickly create and run a query based on a keyword.



Tip

Keyword queries might be simple constructions that you run one time, or elaborate constructions (that specify inclusion, combination, or exclusion of strings or combinations of strings) that are saved for repeated use as a report or rule.

- Step 1** Limit the scope of the query, as desired, by entering a source IP, destination IP, or a Service into the corresponding criteria fields.
- Step 2** From the **Query** subtab, locate the Query type: line and click **Edit** (see item (2) on [Local Controller Query Interface, page 8-3](#)).
- a. Examine the **Result Format** criterion and change the selection as necessary.
 - b. Examine the **Order/Rank By** criterion and change the selection as necessary.
 - c. Examine the **Filter by Time** criterion and change the selection as necessary.



Tip

Be sure that the Filter by Time criteria is set to match the scope you intend to examine.

- d. Examine the **Use Only Firing Events** criterion and change the selection if necessary.
 - e. Examine the **Maximum number of rows returned** criterion and change the selection if necessary.
 - f. Click **Apply**.
- Step 3** Click **ANY** below the Keyword heading.

Figure 8-10

Specify raw message keywords:

Open (	Search String	) Close	Operation	Highlight
	pop3		OR	
	imap		None	
			AND	
			OR	
			NOT	
			None	
			None	
			None	
			None	
			None	
			None	
			None	
			None	

143435

The specify raw message keywords: box appears.

- Step 4** Under Search String heading enter one or more strings to query; under Operation, select an operation (AND, OR, NOT) if desired. (For the final item in the list, set the Operation to **None**.)



Tip To build a nested query, you can click the parentheses icon () to add parentheses or click the trash can icon () to remove parentheses from each line.

- Step 5** Click **Apply**.

- Step 6** Click **Submit Inline** to run the query.

MARS processes the keyword query and displays results. You are also given options to save the query as a report, or save it as a rule, or to submit it again.

- Step 7** To save the query

Batch Query Operations

This section details procedures you can perform on batch queries.

This section contains the following topics:

- [Define and Run a Batch Query, page 8-15](#)
- [Stop a Batch Query, page 8-16](#)
- [Resubmit a Batch Query, page 8-17](#)
- [Delete a Batch Query, page 8-17](#)

Define and Run a Batch Query

A batch query runs in the background and its definition is recorded in the Batch Query Selection list under the Batch Query subtab. This list works in the same manner as the Report Selection list. To run a previous batch query you select it and click **Resubmit**. For more information see [Run a Report, page 8-31](#)).

When you first define a query, MARS calculates the time necessary to run the query and returns one of three results:

- **Submit Inline**—Indicates that the query is within normal processing capability and, although you cannot run it as batch query, you can still save the query as a report.
- **Submit Batch**—Indicates that the query exceeds normal processing capability and must be batch processed (run in the background).
- **Submit . . .**—Indicates that the query's processing requirements border on normal capability and may be submitted either as an inline or batch query. The option to run inline or as a batch appears, as shown in [Figure 8-11](#)(the **Submit Batch** button appears along with **Submit Inline**).



Note

The display of the **Submit Batch** button is an indication that inline execution might take longer than the current time-out period allows. If you still decide to run the Query in inline mode, its completion cannot be guaranteed.

To define and run a batch query, follow these steps:

- Step 1** Click the **Query / Reports** tab and, from **Query** subtab, enter your query type and criteria. For more information see [Selecting the Query Type, page 8-3](#) and [Select Query Criteria, page 8-7](#).
- Step 2** Click **Submit Batch** or **Submit...**, which ever one is displayed. If you click **Submit...**, the following dialog box appears:

Figure 8-11 *Choosing the Query Submission Method*

Choose Query Submission Method

This query will likely take a significant amount of time to complete.

To have the query run in the background, select "Submit Batch." The results will be sent to you via email (assuming a correct entry in your user profile), and will be saved for viewing later. If you desire, the query can be run again at a future time and the previously computed results will be reused.

To run the query immediately, select "Submit Inline." The results will be displayed in your browser as soon as the query completes; no results will be saved and no email will be sent.

143436

To submit your query as a batch query, click **Submit Batch**. Your query is submitted, and you are automatically taken to the **Batch Query** tab.



Tip

If your query is very large, you may only be given the options of **Save as Rule**, **Save as Report**, or **Submit Batch**. On the other hand, only **Submit Inline** appears if batch processing is not required.

**Note**

The display of the **Submit Batch** button is an indication that inline execution might take longer than the current time-out period would allow. If you still decide to run the Query in inline mode, its completion cannot be guaranteed.

**Note**

If your batch query is configured to filter by event and specifies a restriction by severity (Red, Yellow, Green), the Batch Query page lists the Query, but does not show the severity restriction. The batch query results list all results and criteria in the same format as the inline query results.

Figure 8-12 **Select Batch Query**

Page Refresh Rate

Never

Batch Query Selection

Owner	Query	Status	Submitted	Time Range
Administrator, Administrator (pnadmin)	Query Type: Event Types ranked by Sessions Time: 4ww:2dd:0hh:10mm:0ss	Not Run	Never	May 5, 2004 11:52:25 AM PDT - Jun 4, 2004 12:02:25 PM PDT

View HTML

View Results

Resubmit

Stop

Delete

1 to 1 of 1 25 per page

143434

Step 3 To watch the status of the query in real-time, you can use the drop-down list to change the **Page Refresh Rate** from **Never** (the default) to 1 minute, 3 minutes, 5 minutes, 10 minutes, 15 minutes, or 30 minutes.

Step 4 To view the results of the batch query as it is running, click **View Results**. This can be done while the query is in progress.

If the email address in your user profile on the MARS is valid, the results of your batch query are emailed to you when the query has completed, and can also be viewed by clicking **QUERY / REPORTS > Batch Query > View Results**.

**Note**

When you click **View Results** while the query is in progress, the results compiled up to that moment are recomputed. This can make the display take longer to appear.

Stop a Batch Query

Stopping a batch query can be done simply. However, there is no way to stop a query submitted inline.

Step 1 Click **QUERY/REPORTS**, then click the **Batch Query** tab.

Step 2 Click **Stop**.

The **Status** of the query changes to **Finished**.

Resubmit a Batch Query

You can resubmit a batch query if you want to restart it. A resubmitted batch query will use previously computed results, thus resulting in a faster query than one submitted for the first time.

-
- Step 1** Click **QUERY/REPORTS**, then click the **Batch Query** tab.
- Step 2** Click **Resubmit**.
- The **Status** of the query changes to **In Progress**.
-

Delete a Batch Query

-
- Step 1** Click **QUERY/REPORTS**, then click the **Batch Query** tab.
- Step 2** Click **Delete**.
- Step 3** In the confirmation window, click **Delete** to confirm.

**Note**

You can only see your own batch queries and their results. The batch queries of others and their results are not viewable by you, and your batch queries and their results are not viewable by others.

Perform a Long-Duration Query Using a Report

This section explains how to create and view a long-duration query on the MARS. There are two ways to perform a long-duration query on the MARS:

1. **Modify an existing report.**

Advantages:

- The report is compiled relatively quickly.
- You can compile data gathered over a longer time period.

Disadvantage.

This type of query can only be used without any changes to query criteria other than time range, and can only be used with the following reports:

- Activity: All - Top Destination Ports
- Activity: All - Top Destinations
- Activity: All - Top Event Types
- Activity: All - Top Reporting Devices
- Activity: All - Top Sources
- Activity: Attacks Seen - Top Reporting Devices
- Activity: Denies - Top Destination Ports

- Activity: P2P File sharing/Chat - Top Event Types
- Activity: Scans - Top Destination Ports
- Activity: Scans - Top Destinations
- Activity: Unknown Events - All Events
- Activity: Web Usage - Top Destinations by Sessions
- Activity: Web Usage - Top Sources
- Attacks: All - Top Rules Fired
- Attacks: All - Top Sources

2. Perform a batch query.

Advantages:

- You can modify any of the query criteria.
- Best suited for data that spans a short time period.

Disadvantages

- This type of query can be slow and may take a substantial amount of time to complete.
- Only Admin users can perform a batch query.

For more information see [Define and Run a Batch Query, page 8-15](#)

If you want to observe activity on your MARS over a long period, you can edit an existing report that runs on a regular basis, such as hourly or daily, to run for a more extended period.



Note

Trying to run a long-duration query using a report that only runs “on demand” has the same effect as running a query; it can take just as long because it has to compile data, whereas data from the regularly-run reports has been precompiled on an ongoing basis.

To query using a report, follow these steps:

-
- Step 1** In the **QUERY / REPORTS** tab, click the **Reports** tab to obtain the Main Report window.

Figure 8-13 Main Report Window

Report Selection

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
☐ Activity: All - NAT Connections	Run on demand only	Normal	None	Query Type: NAT connections ranked by Time Time: May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT	This report lists Network Address Translations performed on non-denied sessions as reported to MARS.	Finished: Jun 16, 2004 4:40:36 AM PDT	Jun 15, 2004 8:32:09 PM PDT	May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT
☐ Activity: All - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 10, 2004 4:17:02 PM PDT	Jun 10, 2004 4:16:58 PM PDT	Jun 10, 2004 3:16:58 PM PDT - Jun 10, 2004 4:16:58 PM PDT
☒ Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT

143798

Step 2 Navigate to and then click the radio button next to the regularly-scheduled report you want to modify (in this example, we use **Activity: All - Top Destinations**). Click the **Query** column to edit the report. The Build Report window appears.

Figure 8-14 Build Report window**Build Report**

Click the cells below to define the report:

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 16, 2004 7:15:42 PM PDT	Jun 16, 2004 7:15:42 PM PDT	Nov 29, 2003 6:05:42 PM PST - Jun 16, 2004 7:15:42 PM PDT

Time Range:

☒ Last: 200 Days 0 Hrs 10 Mins

☐ Start: 2004 June 16 19 Hrs 42 Mins

End: 2004 June 16 19 Hrs 52 Mins

143686

Step 3 In the lower portion of the Build Report window, change the **Time Range** the report (**Activity: All - Top Destinations**) covers to the duration you want it to cover.

Step 4 Click the **Submit** button to run the report and return to the Main Report window.

Select Custom Columns for Query Result Display

When you have a query type that specifies the *All Matching Sessions, Custom Columns* result format, you can select the number and order of the results returned for display. (For more information see [Selecting the Query Type, page 8-3.](#))

To set the number and order of columns in an All Matching Sessions report, follow these steps:

- Step 1** From the Query/Report tab, click **Edit** on the Query Type line.
- The system displays [Figure 8-4](#).
- Step 2** From the Result Format list, select **All Matching Sessions, Custom Columns**.

Figure 8-15 Result Page: Custom Columns

The screenshot shows the Cisco MARS Local Controller interface. At the top, there's a navigation bar with tabs: Query, Batch Query, and Report. Below this, a header bar displays 'CS-MARS Local Controller: pnmars/161 v6.0' and a login status 'Login: Local: Administrator (pnadmin)'. The main content area is titled 'Query Event Data' and includes a 'Query type: Event Types ranked by Sessions, 0h:10m' dropdown. Below this is a table with columns: Source IP, Destination IP, Service, Events, Device, Reported User, IPS Risk Rating, IPS Threat Rating, IPS Global Correlation Score, Keyword, Operation, Rule, and Action. The 'Result Format' dropdown is set to 'All Matching Sessions, Custom Columns'. The 'Select Columns' section shows a list of columns with 'None' selected for each. The 'Filter by Time' section includes fields for 'Last' (0 days, 0 hrs, 10 mins), 'Start' (2009 May 28 12:29), and 'End' (2009 May 28 12:39). There's also a 'Use Only Firing Events' checkbox and a 'Maximum number of rows returned' field set to 5000. The bottom of the page shows a copyright notice for Cisco Systems, Inc. and a summary of the page content.

The Query Criteria Result Page changes to show the Select Columns list boxes in place of the single Order/Rank By list box.

- Step 3** From the top, use the Select Columns list boxes to select one or more columns you want displayed.



Note The results will be sorted on the first column you select.

- Step 4** Specify the [Filter By Time](#), [page 8-6](#), [Use Only Firing Events](#), [page 8-7](#), and [Maximum Number of Rows Returned](#), [page 8-7](#) criteria, as required.
- Step 5** Click **Apply**.

View a Query Result in the Report Tab

To view a query in the Report tab, follow these steps:

- Step 1** At the bottom of the Main Report window, click the radio button next to the report (**Activity: All - Top Destinations**).

The display similar to the following table appears:

Figure 8-16 Main Report window (bottom)

☒	Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT
☐	Activity: All Events and Netflow - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 8, 2004 9:28:03 PM PDT	Jun 8, 2004 8:28:51 PM PDT	Jun 8, 2004 8:28:51 PM PDT - Jun 8, 2004 9:28:51 PM PDT
☐	Activity: All Sessions - Top Destination Ports by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination Ports ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destination ports by bytes transferred.	Not Run	Jun 8, 2004 9:29:20 PM PDT	Jun 8, 2004 9:19:20 PM PDT - Jun 8, 2004 9:29:20 PM PDT
☐	Activity: All Sessions - Top Destinations by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination IPs ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destinations by bytes transferred.	Not Run	Jun 8, 2004 9:29:57 PM PDT	Jun 8, 2004 9:19:57 PM PDT - Jun 8, 2004 9:29:57 PM PDT

- Step 2** From the drop-down list on the bottom of the Reports page, select either:

- **View HTML:** to view the report as an HTML file.
- **View CSV:** to view the report as a CSV (comma-separated values) file.

- Step 3** Click the **View Report** button.



Note

The **Status** column shows the percent completion of the report. You can view a partially-completed report, but it might not contain the data you require. The **Status** column updates when the page refreshes per the **Page Refresh Rate** setting on the **Query/Reports > Batch Query** page.



Note

In general, do not use the browser refresh or other browser navigation buttons with the MARS Appliance GUI.

Viewing Events in Real-time

The Real-time Event viewer is a query option on the local controller that permits you to view real-time events as follows:

- View raw events as they stream to MARS before they are sessionized, with a maximum 5-second delay.
- View a sessionized event stream—more delay is possible when there are many events in a session.

The real-time events display as a continuously scrolling screen. You can configure query criteria to filter what is displayed. When viewing raw events, sessionization is not impeded, all the parsed raw events are sessionized per normal MARS operation.

The Real-time Event viewer can only display query-result formats that support ranking by time (**Order/Rank** field set to **Time**), these include the following:

- Matched Incident Ranking
- All Matching Sessions
- All Matching Sessions, Custom Columns
- All Matching Events
- All Matching Event Raw Messages
- NAT Connection Report
- MAC Addresses Report
- Unknown Event Report
- Detailed NAC Report

Restrictions for Real-time Event Viewer

The Real-time Event Viewer is available only for Local Controllers.

Real-time event queries should be made *only* from a browser instance that was used to login to MARS. The real-time query will not have reliable results if it is executed from a browser instance spawned from the original login instance (for example, a new browser window launched with **Ctrl+N**, **File>New>New Window**, or **right-click** {link on MARS GUI}>**Open in New Window**).

Multiple real-time queries can operate in multiple browser instances at the same time, but you *must* login to MARS with each browser instance. MARS allocates 1GB of shared buffer for incoming events per query instance. The following restrictions for simultaneous Real-time Event Viewer sessions exist for the specified model:

- MARS 20R and 25R are limited to 1 Event Viewer
- MARS 20 and 25 limited to 2 Event Viewers
- MARS 50 and 55 limited to 3 Event Viewers
- MARS 100, 100e, 200, 110, 110R, and 210 are limited to 5 Event Viewers

Invoke the Real-Time Event Viewer on a Local Controller

To invoke the real-time event viewer, complete the following steps:

- Step 1** Navigate to the **Query** home page as shown in [Figure 8-17](#).

Figure 8-17 Query Home Page

Copyright © 2003-2009 Cisco Systems, Inc. All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

275934

- Step 2** Click **Edit**. The Query edit dialog appears, as shown in [Figure 8-18](#).

Figure 8-18 Configuring Real-Time Event Viewer Query

Copyright © 2003-2009 Cisco Systems, Inc.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

194484

- Step 3** Perform the following substeps:

- From the **Result Format** dropdown list, select a format that can be ranked by time.
The formerly grayed-out **Real Time** radio button becomes clickable.
- Click the **Real Time** radio button, and select **Raw events** or **Sessionized Events** from the dropdown list.
Only **All Matching Events** and **All Matching Events Raw Messages** have the **Raw events** option.

- **All Matching Events** with **Raw events** displays Event ID, Event Type, Source IP/Port, Destination IP/Port, Protocol Time, and Reporting Device fields.
- **All Matching Events Raw Messages** with **Raw events** displays Event ID, Event Type, Time, Reporting Device, and Raw Message fields.
- A Result Format with the **Sessionized Events** option displays Event/Session/Incident ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, Reporting Device, Path/Mitigation, and Tune fields.

c. Click **Apply**.

The Query Event Data screen appears with the Save as Report and Save as Rule buttons gray and inactive, as shown in [Figure 8-19](#).

Figure 8-19 Real-Time Event Query to Submit

Copyright © 2003–2009 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

194485

Step 4 Modify the parameters of the Query Event Data filter as you require and click **Submit**.



Note The Operation, Rule, and Action parameters of the Query Event Data filter do not function for the real-time event viewer.

Real-time results begin to scroll up from the bottom of the page within 5 seconds, as shown in [Figure 8-20](#). Real-time raw events are shown in this example.

Figure 8-20 View of Events in Real-Time

Query Results

Event ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device
5156709	Cisco PIX and ASA Time-to-Live DoS	172.20.10.174	6155 239.255.2.3	6155 UDP	Aug 22, 2008 2:35:38 AM PDT	ips-5.1
5156710	Denied packet due to Cisco ICS OPACL	172.20.10.218	138 172.20.10.255	138 UDP	Aug 22, 2008 2:35:38 AM PDT	ips-5.1
5156711	Denied packet due to Cisco ICS OPACL	172.20.10.216	N/A N/A	N/A UDP	Aug 22, 2008 2:35:38 AM PDT	ips-5.1
5156712	Denied packet due to Cisco ICS OPACL	172.20.10.166	N/A N/A	N/A UDP	Aug 22, 2008 2:35:38 AM PDT	ips-5.1
5156713	RFC 1918 Addresses Seen	172.20.10.41	138 172.20.10.255	138 UDP	Aug 22, 2008 2:35:38 AM PDT	ips-5.1
5156714	Denied packet due to Cisco ICS OPACL	172.20.10.41	138 172.20.10.255	138 UDP	Aug 22, 2008	ips-5.1
5156735	Cisco PIX and ASA Time-to-Live DoS	172.20.10.174	N/A N/A	N/A UDP	Aug 22, 2008 2:36:08 AM PDT	ips-5.1
5156736	Cisco PIX and ASA Time-to-Live DoS	172.20.10.174	6155 239.255.2.3	6155 UDP	Aug 22, 2008 2:36:08 AM PDT	ips-5.1
5156737	Denied packet due to Cisco ICS OPACL	172.20.10.43	N/A N/A	N/A UDP	Aug 22, 2008 2:36:08 AM PDT	ips-5.1
5156738	RFC 1918 Addresses Seen	172.20.10.160	138 172.20.10.255	138 UDP	Aug 22, 2008 2:36:08 AM PDT	ips-5.1
5156739	Denied packet due to	172.20.10.160	138 172.20.10.255	138 UDP	Aug 22,	ips-5.1

Number of Rows: [Set Rows](#) (Range: 1-200) Scroll speed: [Pause](#)

The Real-time event viewer display is governed by the following controls:

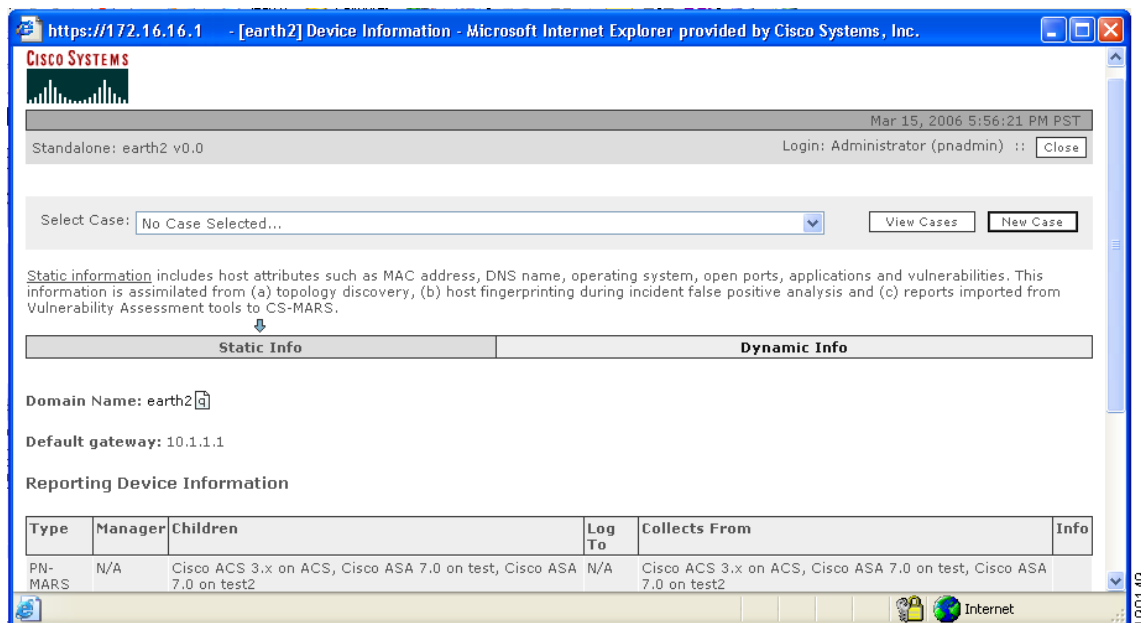
- **Scroll Speed**—Select one of four scrolling rates.
- **Scroll Bar**—Enables you to scroll up and down in the visible event list.
- **Pause button**—Suspends the scrolling display.
- **Restart button**—Restarts the display from the current time. This button appears when you pause the scrolling display.
- **Resume button**—Restarts the display from the time when paused. This button appears when you pause the scrolling display.
- **Clear**—Terminates the real-time query.
- **Number of Rows**—Select the number of rows to be visible in the list. The range is 1–200.
- **Set Rows button**—Sets the display to the number of rows entered in the **Number of Rows** field.

**Note**

Clicking Pause, Resume or setting Scroll Speed are GUI actions that do not reset the MARS GUI timeout interval. These actions will not prevent the GUI from timing out.

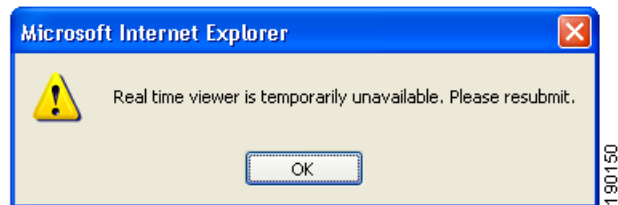
Step 5 Click the active links within a real-time event record to view the related pop-up windows. For example, the Reporting Device Information pop-up window is shown in [Figure 8-21](#).

Figure 8-21 Reporting Device Information Pop-up Window



Should errors occur during the display of events, a message box appears, as shown in Figure 8-22.

Figure 8-22 Real-time Event Viewer Error Message



Click **OK** to clear the message box, and restart the Real-time event viewer by clicking **Submit**.



Tip

To view the most recent real-time events, you can click **Submit** at any time, or **Pause** and **Restart** to reinitialize the Real-Time Event Viewer. The most recent events are always at the bottom of the output queue, and their freshness when you view them is limited by the number of events in the queue and the scroll speed of the display.

Reports

Using the Reports page, you can build repeatable queries, edit and delete current reports, run reports, and view reports in either HTML or CSV (comma separated value) format.

Reports can be configured to run automatically on a specified schedule (scheduled reports) or can be run manually like a query (on-demand reports). On-demand reports collect matching data stored in the MARS database for the specified report duration then display the results. A scheduled report continually collects matching data from MARS memory and does not access the MARS database. A scheduled report begins to compile matching data from the time the report is created. It does not match data still in memory but received before the report was created. Scheduled reports have better performance than on-demand reports because they avoid database operations.

**Note**

Because the data collection for scheduled reports starts when the report is created, a user-configured scheduled report may not return complete results if it is requesting data received by MARS before the scheduled report was created.

This section contains the following topics:

- [Global Controller Reports, page 8-27](#)
- [Local Controller Reports, page 8-27](#)
- [Report Type Views: Total vs. Peak vs. Recent, page 8-27](#)
- [Report Charts and Graphs, page 8-29](#)
- [Report Creation, page 8-29](#)
- [Operations on Existing Reports, page 8-30](#)

Global Controller Reports

Reports performed at the Global Controller level are similar to those on an Local Controller, but also include the **Zone Collapsing** parameter. You can run a report across one or more Local Controllers by specifying their zones. This enables a report at the Global Controller to select zone-specific objects.

When you submit a report from the Global Controller, the report request is sent to the Local Controllers monitored by that Global Controller. Each Local Controller generates the report and sends summary data back to the Global Controller, which merges the results at the global level. The merged report is sent to any recipients, as defined by the report definition on the Global Controller.

Local Controller Reports

Predefined System Reports are treated as global reports. Global Controller receives report data once its connected to the Local Controller. Previous report results (prior to managing the Local Controller) will not be pushed up to Global Controller. Thus viewing of reports will not include the information before the Local Controller becomes active.

Report Type Views: Total vs. Peak vs. Recent

Whereas alerts provide up-to-the-minute views of high-priority incidents, reports aggregate sessions into different views. Reports correlate three factors:

- **Period of time**—defines boundaries around the analyzed session data based on when it was recorded.

- **Query criteria**—restrict the set of sessions that will be aggregated to that which matches your criteria. Criteria can include source address, destination address, network service, event, reported user, and reporting device.
- **View type**—defines how to aggregate the matched data into a meaningful report view—one that matches the type of study in which you are interested.

**Note**

In each view type, you can refine the report criteria to filter out expected activity—the data you know about. You can filter this activity by refining the query criteria. These criteria should be tuned to a specific network. Reports can be valuable in detecting behaviors beyond the normal traffic flows of your network. You can determine the expected activities using reports that are not filtered and vetting those results against normal network use.

MARS provides three view types, each of which restricts the matched sessions to a user-defined limit of *N*. The following view types exist:

- **Total View.** For each result type matching the query criteria, this view counts the occurrences of that result type that transpire during the specified time period. It presents the total count of the top *N* matched result types, ranked by number of sessions, as determined by which ones occurred most frequently over the period of time. You can use these reports to determine your network's condition relative to the studied sessions. For example, you can use this view to identify attacks that launched at frequent intervals. This view does not present spikes in network activity; it simply presents the top occurring result types.

**Note**

CSV. Generates the Total View but presents the report in the CSV format for processing by another tool or script. This option is intended for use with e-mail notifications where post-processing is required.

- **Peak View.** Within MARS, all report result data is stored in 10-minute time slices. The Peak View studies each of the 10-minute time slices within the specified time period to which one contained the highest number of matched sessions for a specific result type. It also determines an additional nine peaks within the time period, where each peak identifies a unique result type relative to the other peaks.

Each peak value is charted relative to the other nine peaks. For each time slice containing a peak value, the Peak View lists the top *N* matched result types that occurred. It is possible to have multiple peaks within the same time slice, as it is the result type, not the time slice, that must be unique across peaks.

**Note**

To be detected within this view, the result type must peak above normal traffic. Therefore, you must tune the query data to filter out expected traffic.

Unlike the Total View, the Peak View does not focus on the overall top occurring results, instead it identifies a high volume of traffic over a short time period. Its purpose is to detect temporary bursts of traffic on your network that overshadow normal traffic usage. These bursts identify possible issues, such as worm outbreaks.

- **Recent View.** This view is similar to Total View; however, it identifies the top *N* result types that occurred within the past hour. It then plots all occurrences of those result types over the selected time period.

Report Charts and Graphs

The three types of charts are:

- **Bar Chart.** Summary of the top sessions and the count.
- **Pie Chart.**
- **Graphs:** Events/Time.



Note

Peak values in the past are not displayed unless they fall into the current top ten results. Also, not every item in a particular time slice's top ten is charted.



Note

The charts presented as part of reports highlight up to the 10 most significant items. In cases where fewer than 10 items are significant, the

Report Creation

You can create a report through the **Query** page, or you can create a report from scratch on the **Reports** page. This section details creating Local Controller and Global Controller reports from the **Reports** page, but is applicable to editing reports and to creating reports from the **Query** page.

This section contains the following topics:

- [Create a New Local Controller Report, page 8-29](#)
- [Create a New Global Controller Report, page 8-30](#)

Create a New Local Controller Report

- Step 1** On the Reports page, click **Add**.
- Step 2** In the **Report Name** and **Report Description** fields, enter a report name and description. Click **Next**.
- Step 3** Select the schedule parameters for the report.
- Step 4** Select a View Type for the report. You can receive these reports in your email or view them in the UI. Your choices are: **Total View**, **Peak View**, **Recent View**, and **CSV** (see [Report Type Views: Total vs. Peak vs. Recent, page 8-27](#)). Click the **Next** button.
- Step 5** Select users in the Recipients Available field by expanding the user groups, clicking users or user groups, and clicking the **Add** button. See [Green-field, Multi-box Deployment, page 1-6](#) for more information.
- Step 6** Repeat, as required, for other users. Click the **Next** button.
- Step 7** Build or modify the query. To edit the query time range, either click the Report type link or click the **Edit** button. See [Result Format, page 8-4](#) for information on query parameters; see [Query Criteria Descriptions, page 8-9](#) for more information on building queries. Click **Apply** to save your changes; click **Next** when the query is complete.
- Step 8** Click **Submit** to save your report.

Create a New Global Controller Report

-
- Step 1** On the Reports page, click **Add**.
- Step 2** In the **Report Name** and **Report Description** fields, enter a report name and description. Click **Next**.
- Step 3** Select the schedule parameters for the report.
- Step 4** Select a format for the report's output. Under **View Type and Zone Collapsing**, select one of the following:
- **Total View/Sum Zones**—This view displays the summed total of the top N results over the specified time range.
 - **Total View/List Zones**—This view displays the total, grouped by zone, of the top N results over the specified time range.
 - **Peak View/Sum Zones**—This view finds the top ten largest results in the time range, and displays the top ten results for the times when those peaks occurred.
 - **Peak View/List Zones**—This view finds the top ten largest results in the time range, groups them by zone, and displays the top ten results for the times when those peaks occurred.
 - **Recent View/Sum Zones**—This view finds the top N results from the past hour, and displays them versus their summed totals over the specified time range.
 - **Recent View/List Zones**—This view finds the top N results from the past hour, groups them by zone, and displays them versus their summed totals over the specified time range.
 - **CSV/Sum Zones**—This view displays the summed total of the top N results as a comma-separated values file. (See [Report Type Views: Total vs. Peak vs. Recent](#), page 8-27).
 - **CSV/List Zones**—This view displays the summed total of the top N results, grouped by zone, as a comma-separated values file. (See [Report Type Views: Total vs. Peak vs. Recent](#), page 8-27).
- Step 5** Click **Next**.
- Step 6** Select users in the Recipients Available field by expanding the user groups, clicking users or user groups, and then clicking **Add**. See [Green-field, Multi-box Deployment](#), page 1-6 for more information.
- Step 7** Repeat [Step 6](#) for other users.
- Step 8** Click **Next**.
- Step 9** Build or modify the query. To edit the query time range, either click the Report type link or click **Edit**.
- Step 10** Click **Apply** to save your changes; click **Next** when the query is complete.
- Step 11** Click **Submit** to save your report.
-

Operations on Existing Reports

This section details operations you perform on existing reports.

This section contains the following topics:

- [View a Report](#), page 8-31
- [Run a Report](#), page 8-31
- [Delete a Report](#), page 8-31
- [Edit a Report](#), page 8-31

- [Duplicate a Report, page 8-32](#)

View a Report

You can use this procedure to view the results of regularly scheduled reports.

-
- Step 1** Click the radio button next to the report.
- Step 2** From the drop-down list on the bottom of the page, select either:
- **View HTML:** to view the report as an HTML file.
 - **View CSV:** to view the report as a CSV file.
- Step 3** Click the **View Report** button.



Note If you chose to view the report as a CSV file, you need to save the file to your computer and open the CSV file in a third-party application.

Run a Report

You can use this procedure to override the defined schedule and cause a report to run immediately.

-
- Step 1** Click the radio button next to the report.
- Step 2** Click the **Resubmit** button.



Note Due to caching issues, reports with a time range of less than one hour are not recommended.



Tip To see the results, click **View Report**

Delete a Report

-
- Step 1** Click the radio button next to the report.
- Step 2** Click the **Delete** button to delete the report.
- Step 3** On the Delete Confirmation page, click **Delete**.
-

Edit a Report

You can not edit system generated reports. Editing report criteria is meant for minor tweaking to a previously generated report.

**Note**

See the [Duplicate a Report, page 8-32](#) procedure for a method to clone and then edit an existing report.

- Step 1** Click the radio button next to the report.
- Step 2** Click the **Edit** button to edit the report.
- Step 3** Navigate using the **Previous** and **Next** buttons, or clicking on the report criteria.

Figure 8-23 Navigating to the Recipients column by clicking its criteria

Name	Schedule	Format	Recipients
Test	Run on demand only	Normal	None

- Step 4** Edit the report, and click the **Apply** button to apply changes to the report.
- Step 5** Click the **Submit** button to finalize the report.

**Note**

Changing the report's query criteria will not re-generate a new result. New edited criteria is based on the previously generated report. In some situation such as filtering out specific IP source, user should create a new report.

**Note**

Email notification of a global generated report will be sent from the Global Controller and not the Local Controller.

Duplicate a Report

You can duplicate or "clone" any report as a template for a new report. After you have duplicated and saved an existing report specification, you can edit the new report's specification as you require. Often, this approach is a more effective way to establish a new report than building it from scratch.

- Step 1** Click the radio button next to the report.
- Step 2** Click **Duplicate** to duplicate the report.
- The duplicated report appears in the list of reports. To the report name is appended: "copied: [yy.mm.dd/hh.mm/ss]".
- Step 3** Edit and save (or run) the report, as required. (See [Edit a Report, page 8-31](#) for details.)



CHAPTER 9

Incident Investigation and Mitigation

An incident is a chain of events that are correlated by a rule to signal an attack upon your network. Cisco Security Monitoring, Analysis, and Response System (MARS) simplifies and expedites the detection, mitigation, reporting, and analysis of the incident. The Network Summary dashboard and the Incident pages help to detect recent incidents and show the rules and the events that compose them. Mitigation refers to the ability of MARS to isolate the attacking and compromised network devices by identifying and configuring enforcing devices that act as choke points in the network. Queries and reports reveal the scope of a problem and gather data for analysis and regulatory compliance. All this information can be captured in a case report with Case Management and escalated to the relevant personnel.

This chapter contains the following topics:

- [Incidents Overview, page 9-1](#)
- [The Incidents Page, page 9-2](#)
- [Incident Details Page, page 9-4](#)
- [False Positive Confirmation, page 9-7](#)
- [Mitigation, page 9-11](#)
- [Layer 2 Path and Mitigation Configuration Example, page 9-18](#)
- [View Session via a Query, page 9-23](#)

Incidents Overview

An attack can consist of a reconnaissance activity (for instance, a port scan), followed by a penetration attempt (such as, a buffer overflow), followed by malicious activity on the target host (for example, a local privilege escalation attack or the installation of backdoors).

An incident, which is generated by a Local Controller, collects the interesting events that constitute an attack scenario and uses rules to describe them. MARS provides you with pre-defined, system rules—that you can fine tune—and enables you to create your own rules.

Incidents that appear on the Global Controller are fired by global rules at the Local Controller level and are compiled at the Global Controller level. Incidents that appear on a Local Controller are fired by rules local to that Local Controller. They are used by Local Controllers for local reporting and are *not* propagated *up* to the Global Controller.

Predefined System Rules are treated as global rules. When an incident is fired by a system rule on the Local controller, it gets propagated to the Global Controller.

Incidents are sub-divided into instances to make it easier for you to investigate the attack scenario. Each instance alone is a full attack scenario.

For example, if your network is probed for a DoS attack and then attacked, a rule fires when it sees the follow up attack. The incident displays the instances of this attack.

Figure 9-1 A DoS probe followed by a DoS attack

Incident ID: 42998483

Offset	Firing Event / Session / Incident ID	Event Type	Source IP/Port
Instance 1			
3		[1906920] Net Flood TCP	+ Total: 5
Instance 2			
3	S:45754259, I:42998483, I:42998484	[1906910] Net Flood UDP	10.4.17.4
Instance 3			
1		[1905037] WWW SGI MachineInfo Info Leak	10.1.1.21
1	S:45775179, I:42998480, I:42998481, I:42998483, I:42998487, I:42998490, I:42998492, I:42998493, I:42998495	[1905110] WWW SuSE Installed Packages Info Leak	10.1.1.21

The Incidents Page

Click the **Incidents** tab to view the Incidents page. The Incidents page displays recent incidents.

Incidents are collections of events and sessions that meet the criteria for a rule, each having helped to cause the rule to fire. An incident’s duration only includes the events that contributed to the incident firing.

Figure 9-2 Incidents Navigation Page: Global Controller

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
1:347915126  (pluto)	Built/teardown/permitted IP connection 	System Rule: Client Exploit - Sysbug Trojan 		Sep 20, 2005 10:17:07 AM PDT	 	C:119662 (New) Security Team 
1:347915135  (apollo)	Built/teardown/permitted IP connection  PIX reserved a network state container for a host 	abcRule-New2 		Sep 20, 2005 10:16:42 AM PDT - Sep 20, 2005 10:17:06 AM PDT	 	
1:347915137  (pluto)	Deny connection - no xlate  Built/teardown/permitted IP connection  PIX reserved a network state container for a host 	test save as rule 		Sep 20, 2005 10:16:42 AM PDT - Sep 20, 2005 10:17:06 AM PDT	 	

1 2 3 4 5 6 7 8 9 143429

1	Name of the Local Controller reporting the incident, also links to the Local Controller Incident page.	2	Links to the Incident Detail page of the reporting Local Controller.
3	The incident severity indication icon	4	The events that compose the Incident. Links to the Event Type Details popup window.
5	Query icon. Links to the Query page and populates the corresponding query field with the item.	6	The rule that fired to create the incident. Links to the rule page to display the details of the rule.
7	Start and end time of the incident.	8	Links to the reporting Local Controller Incident Path and Incident Vector diagrams.
9	Links to the View Case page of the reporting Local Controller		

Figure 9-3 Incidents Navigation: Local Controller

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
1:347918013 	Deny connection - no xlate 	System Rule: Client Exploit - Sysbug Trojan 		Sep 22, 2005 2:38:50 PM PDT	 	
1:342595342 	Sudden increase of traffic to a port 	System Rule: DoS: Network - Attempt 		Sep 22, 2005 2:33:29 PM PDT - Sep 22, 2005 2:33:31 PM PDT	 	
1:347917458  	PIX firewall login failed 	System Rule: Password Attack: System - Attempt 		Sep 22, 2005 2:33:25 PM PDT - Sep 22, 2005 2:33:26 PM PDT	 	C:214192 (Assigned) Acc_team 

1 2 3 4 5 6 7 8 143428

1	The Incident ID— Link to the Incident Detail page.	2	Incident Severity Icon
3	The events that compose the Incident— Launches the Event Type Details popup window.	4	Query icon—Link to the Query page and populates the corresponding query field with the item.
5	The rule that fired to create the incident. Links to the rule page to display the details of the rule.	6	Time range of the incident.
7	Launches the Incident Path and Incident Vector diagrams Click to query on the matched rule	8	Link to the View Case page

The Incident page's table:

- *Incident ID*

An incident's unique ID. On a Global Controller, this ID is followed by the Local Controller on which the incident occurred.

- *Severity*
Low (green), medium (yellow), and high (red) icons.
- *Event Type*
The normalized signature sent from the reporting devices.
- *Matched Rule*
The rule whose criteria were met.
- *Action*
The description of the notification taken when this rule fires (epage, email, etc.)
- *Time*
A single time or a time range (see [Time ranges for Incidents, page 9-4](#) for more information).
- *Incident Path*
The icon that takes you to the incident's path diagram. From the Global Controller, it takes you to the diagram on the Local Controller.
- *Incident Vector*
The icon that takes you to the source, event type, and destination diagram. From the Global Controller, it takes you to the diagram on the Local Controller.

Time ranges for Incidents

The time column displays both single entries for time (Sep 6, 2003 12:09:54 PM PDT), and time ranges (Sep 6, 2003 12:06:43 PM PDT - Sep 6, 2003 12:06:47 PM PDT).

A single time tells you that all of the firing events were received in the same second. The duration of the incident includes only events that have fired that incident.

Incident Details Page

Global Controller Consideration: When you click the Incident ID, the Incident Details table appears in a separate browser connected to the Local Controller that recorded the event.

Clicking the Incident ID takes you to its Incident Details page. The Incident Details page is rich in information and information gathering tools. This page answers questions, such as who did it, what event types happened, when it happened, and to whom it happened.

Figure 9-4 The Incident Details Page

Incident ID: 1111253 [Show](#)

Session ID: [Show](#)

Rule Name: System Rule: Modify Network Config [i](#) **Status:** Active

Action: None **Time Range:** 0h:10m

Provider: Cisco

Description: This rule detects attempts to modify the configurations on a network device such as routers, switches, firewalls etc.

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Severity	Count	Close	Operation
1		ANY	ANY	ANY	Persist/ModifyNetworkConfig	ANY	None	ANY	ANY	ANY	ANY	ANY	1		

Incident ID: 1111253 [Expand All](#) [Collapse All](#)

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
1	S:737340, I:1111253	CS-MARS Detected Conflicting SSL Certificate	N/A	171.69.229.10	N/A	Jun 4, 2009 10:29:33 AM PDT	pnmars			False Positive Tuning

Copyright © 2003-2009 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

On the top of this page are the tools that let you search for Incident and Session ID and view the Matched Rule.

Search for a Session ID or Incident ID

Step 1 Enter the ID into either the Incident ID field or Session ID field on the page's upper right.

Step 2 Click the **Show** button.

To view a partially hidden rule, click the **Show** button next to the Rule Description.



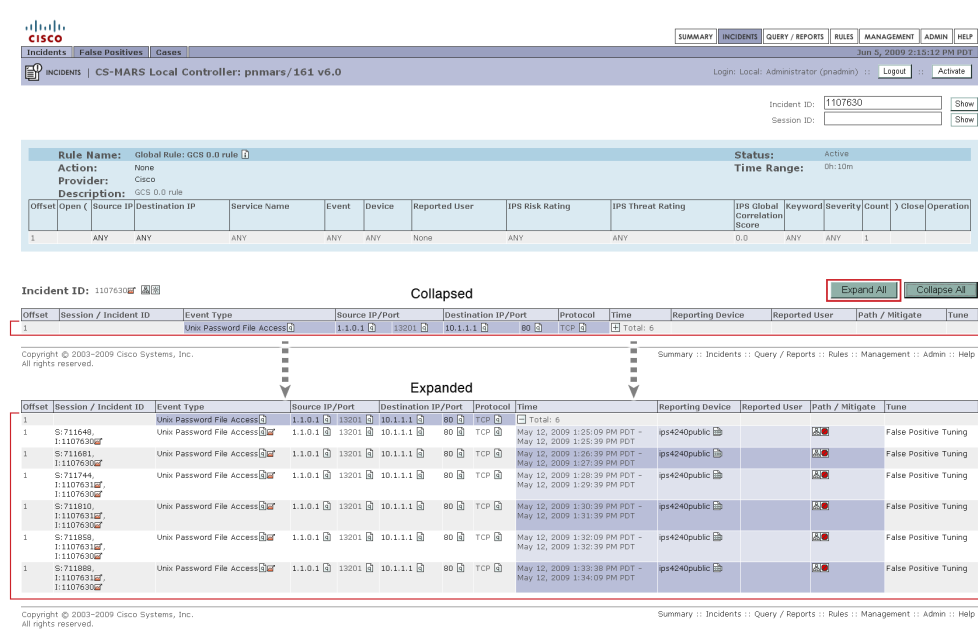
Note Incidents can only be included in a case or mitigated from the Local Controller.

Incident Details Table

Global Controller Consideration: When you click the Incident ID, the Incident Details table appears in a separate browser connected to the Local Controller that recorded the event.

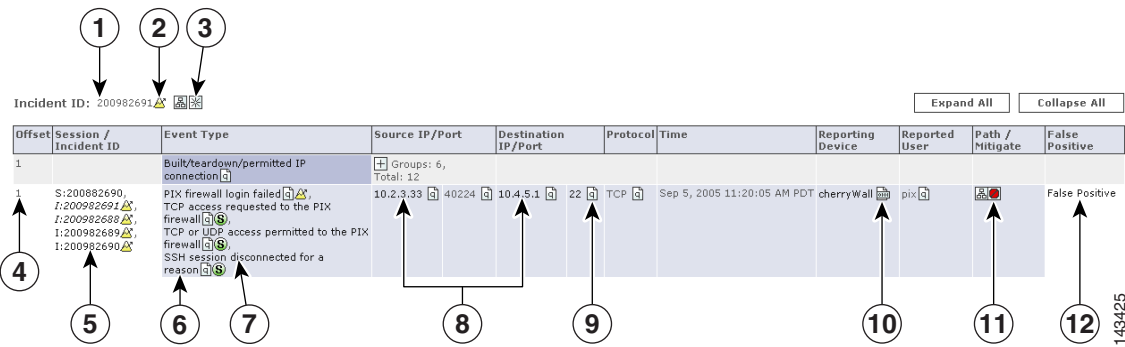
Each row of the Incident Details table represents either a session or the information common to a group of sessions. You can see all of the collapsed session information by clicking the plus signs to expand the group. You can expand or collapse all of the incident's information by clicking the **Expand All** or **Collapse All** buttons.

Figure 9-5 Expanding a Row in a Table



This high-density information table lets you drill deep into incidents. Click the Query icon anywhere on this page to query on a particular criteria. Click the Raw Events icon for raw events for a particular session. You can click the **Tune** link to tune incidents for False Positives, see [The False Positive Page, page 9-9](#) or click the **Mitigate** link to mitigate an attack.

Figure 9-6 Incident Table



1	Incident ID	2	Severity icon
3	Path and Incident Vector icons. Launch popup windows to display Path and Incident Vector diagrams (L2 or L3 attack path information)	4	Offset number
5	Links to Session and Incident Detail pages of all incidents within the session	6	Links to the Event Type Details pages
7	Launches False Positive popup window	8	Link to the Device Information page
9	Query icon links to Query page	10	Click Device icon to launch popup window to display raw message information

11	Link to the Mitigation page.	12	Link to the False Positive Tuning page

The following information describes some of the fine points of this table.

- *Instances*
Sometimes rows are split into instances. The *only* relationship among the different instances is that they fired the same rule in the same time frame.
- *Session/Incident ID*
This column shows the sessions that contributed to the incident, and the other incidents those sessions belong to.
- *Events column*
The Events column shows types of the firing events. Multiple firing events of the same types are shown once per session.
- *Time column*
An incident's duration only includes the events that contributed to the incident firing.

False Positive Confirmation

When investigating incidents, you will invariably come across false positive events. In some cases, firing events are classified automatically by MARS as system-confirmed false positives and unconfirmed false positives. Vulnerability scanning often identifies the false positive events, but at times you must investigate events to determine their validity.

To understand the false positive nomenclature and what tasks you are expected to perform within the user interface, we must study the possibilities among three variables surrounding possible attacks: legitimate attack, valid target, and attack detected. We examine these differences in [Table 9-1](#).

Table 9-1 **Attack Type Truth Table**

	Legitimate Attack	Valid Target	Attack Detected
<i>invalid scenario</i>	0	0	0
False Positive	0	0	1
<i>invalid scenario</i>	0	1	0
False Positive	0	1	1
False Negative	1	0	0
Attack/Alarm (noise)	1	0	1
True False Negative	1	1	0
Intrusion/True Alarm	1	1	1

Based on the valid cases in [Table 9-1](#), we can clearly distinguish the false positive terminology:

- A *legitimate attack* is an actual attempt by an attacker to gain access to or information about a specific host using a known exploit.

- A *valid target* is a host that is susceptible to the launched attack. A host can become an *invalid target* if it is properly patched or has some other preventative measure in place, such as a local firewall, virus scanner, or intrusion prevention software that guards against the attack.
- *Attack detected* refers to whether the monitoring device detected the attack and generated an alarm.
- A *false positive* is when the monitoring system generates an alarm for a condition that is benign. In this case, there is no legitimate attack, despite the alarm generation.
- An *unconfirmed false positive* is one where the monitoring system, based on data not available to the reporting device, has determined that an alarm is a false positive. Unconfirmed refers to the fact that the administrator must review and accept or reject the assessment of the false positive.
- A *false negative* is when the monitoring system fails to detect a legitimate attack.
- *Noise* refers to those alarms that are triggered due to attacks against invalid targets. While they can represent real attacks, the target cannot be compromised due to preventative measures. Attacks that fall within the noise category are of secondary importance in terms of investigation and mitigation.
- *Intrusion* identifies a successful attack against the host, where the host is compromised by the attacker.
- A *true false negative* identifies an intrusion that remains undetected by the monitoring system.
- A *true alarm* identifies an intrusion that is detected by the monitoring system.

When a Local Controller receives an event, it is evaluated against the conditions of the defined rules. If the event satisfies the conditions of a rule, the incident triggers. When an event triggers an incident, we refer to that event as a *firing event*. False positive analysis is performed for such firing events to reduce the number of false alarms.

Using built-in event vulnerability data, learned topology paths, sessionized event data, ACL analysis of layer 2 and 3 reporting devices, supporting data from 3rd-party vulnerability analysis (VA) software (such as Foundstone and eEye), and information that you provide about hosts, MARS analyzes the firing events reported to it determine whether they hold up to a higher-level review.



Note

To determine whether specific incidents are false positives, MARS uses Nessus 2.x GPL plug-ins and custom scripts mapped to specific MARS event types. MARS does not use Nessus to perform vulnerability assessments or related reporting.

In the case of MARS, a *system-confirmed false positive* is where, after further analysis, a firing event is determined to be invalid. Example system-confirmed false positives include:

- When an IDS device monitoring the network outside of a firewall reports an attack; however, the firewall drops that session as part of its standard access restrictions. Therefore, the attack never reaches the target.
- Cisco Security Agent detects an attack and blocks it.

An *unconfirmed false positive* is where, after further analysis, the firing event is believed to be invalid primarily due to the attack being against an invalid target. Example unconfirmed false positives include:

- A reporting device reports a valid attack against a host; however, the host is not susceptible to that attack because it targets a different operating system. You can reduce these types of false positives by employing OS fingerprinting technologies on the reporting devices.
- A reporting device reports a valid attack against a host's application; however, the host is not susceptible to that attack because it targets a different application.
- A reporting device reports a valid web attack against TCP port 80, however, dynamic probing determines that no services on the target host listen to TCP port 80.

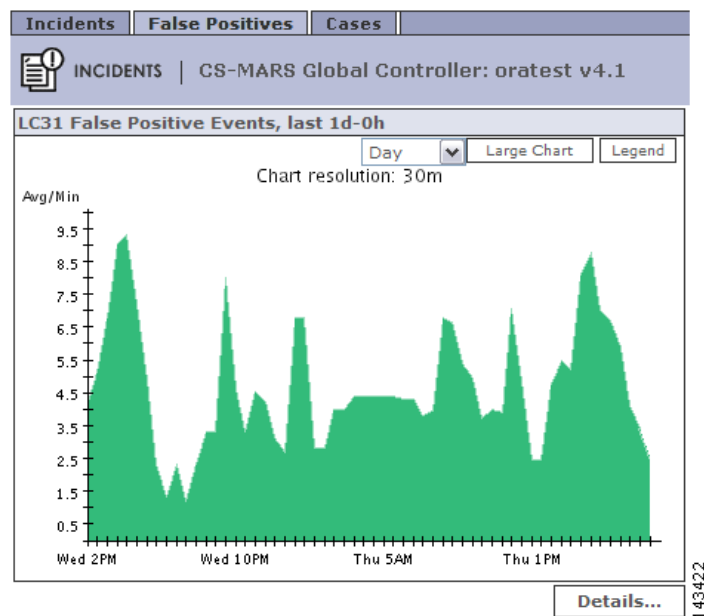
For unconfirmed false positives, you must manually investigate the alarm and specify in Local Controller whether it is an actual false positive. For actual false positives, you should define a drop rule for the event. Defining a drop rule does not mean that the event is not stored in the database, you have the option of dropping the event from incident evaluation and either shoring it in the database or not. Whether you store the event in the database or not, events matching the event type and target host can no longer act as firing events. By refining the event processing in this fashion, MARS frees up your time to focus on actual incidents by more accurately correlating events into incidents and reducing noise.

As part of your operational strategy, you should strive to refine event generation and processing to tune out the possibility for false positives. You can perform such tuning at the device level, by refining what traffic or action can generate an event, and at the Local Controller level by providing more information about your network, such as identifying the operating system of hosts attached to the network segments monitored by that Local Controller.

The False Positive Page

To navigate to the False Positives page, click **Incidents**, and click the **False Positives** subtab.

Figure 9-7 False Positive Graph for a Local Controller (Global Controller only page)



From the Global Controller, the False Positives page is where you can see groupings of False Positives for each Local Controller or for the sum of all the Local Controller zones. You can change the graph by selecting **Hour**, **Day**, **Week**, **Month**, **Quarter**, or **Year** from the first pull-down menu, and **Sum Zones** or an individual local zone from the second menu.

If you want to see details of the false positive on the Local Controller, click the Details button.

From the Local Controller, you can filter categories by clicking on the **Select False Positive** drop-down list. Your choices are:

- *Unconfirmed false positive type*

For this type, the MARS needs user confirmation to determine if the target host is vulnerable to the event type in question.

- *User confirmed false positive type*

For this type, a user has provided confirmation that a firing event is a false positive.

- *User confirmed positive type*

For this type, a user has provided confirmation that a firing event is a true attack.

- *System determined false positive type*

For this type, the system has determined that a firing event is a false positive.

In the False Positives table, you can see how many sessions the false positive has appeared in, the event type, the false positive status confirmation icons, the event type information icon, the destination IP and its port, the destination IP information icon, its protocol, zone, and you can see the sessions that are related to the false positive.

Figure 9-8 False Positive Table

Session Count	Event	Destination IP/Port	Protocol	Zone	Related Sessions	
192	[1905035] WWW HylaFAX Faxsurvey Command Exec	10.4.17.2	80	TCP	CA	Show

1

2

3

4

5

6

143423

1	Link to the Event Type Details page	2	Query icon links to the Query page and automatically populates the corresponding Query field
3	False Positive type and severity icon	4	Launches the Security Device Information popup window
5	Launches Port Information popup window	6	Launches False Positive Sessions Details popup window

The following table shows false positive status confirmation and severity icons: Tuning False Positives

Icon	Description
	Low, medium, and high severity false positives that require confirmation.
	Low, medium, and high severity user determined false positives.
	Low, medium, and high severity system determined false positives.

From the Incidents page or the False Positives page, you can tune false positives - to verify if they are true or false.

Tune a False Positive

- Step 1** Click one of the **Confirm False Positive** icons (
- Step 2** On the False Positive Confirmation page, review the information.
- Step 3** If you decide that the event type is a false positive, click the **Yes** radio button, and follow the steps in [Tune an Unconfirmed False Positive to False Positive](#), page 9-11.

- Step 4** If you decide that the event type is a true positive, click the **No** radio button, and follow the steps in [Tune an Unconfirmed False Positive to True Positive, page 9-11](#).
-

Tune an Unconfirmed False Positive to False Positive

- Step 1** After you determine that a false positive is false, and you have clicked the **Yes** button, click **Next**.
- Step 2** On the next page, decide whether or not you want MARS to keep this event type in the database by selecting the appropriate radio button:
- **Dropping these events completely** (that stops logging those events)
 - **Log to DB only** (that logs the events to the DB)
- Step 3** Once you have decided, click the **Next** button.
- Step 4** On the next page, carefully review the information for the false positive and the new rule.
- Step 5** When you are ready to commit this new information to the appliance, click the **Confirm** button.
-

Tune an Unconfirmed False Positive to True Positive

- Step 1** After you determine that a false positive is true, and you have clicked the **No** button, click **Next**.
- Step 2** Make a final confirmation that this is a true positive, and click the **Confirm** button.
-

Activate False Positive Drop Rules

After you have completed tuning false positives, click **Activate** to immediately implement the changes.

Mitigation

Mitigation refers to the action of limiting an attacking network element's access to the network by modifying the configuration of an enforcement device, usually a switch, router, or firewall.

CS-MARS can perform the following actions related to mitigation:

- Identify attacking and compromised hosts
- Plot Layer 2 and Layer 3 topology of the affected network segment to identify mitigation points and enforcement devices
- Recommend configuration commands for Layer 2 and Layer 3 enforcement devices
- Push (that is, download) recommended configuration commands to supported Layer 2 devices

With Telnet, SSH, or SNMP access to switches and routers, CS-MARS can recommend and push mitigation configurations to enforcement devices, as well as generate interactive topology and incident path diagrams. Without Telnet, SSH, or SNMP access, some mitigation information can still be obtained from Cisco switches running specific IEEE 802.1X Port Based Network Access Control protocol

configurations, but recommended mitigation commands must be configured manually on the enforcement devices. See [Layer 2 Path and Mitigation Configuration Example, page 9-18](#) for further information and procedures for configuring Layer 2 devices to receive CS-MARS mitigation commands.

Static and Dynamic Network Information

Topology information obtained from access to relatively permanent Layer 2 and Layer 3 devices is called Static Information in the HTML interface. Dynamic Information refers to frequently changing information such as host names, or DHCP-leased IP addresses obtained through devices or agents that report dynamic events, such as 802.1X access control configurations, the Cisco Security Agent, or other security suite software.

The CS-MARS can determine a mitigation point and an enforcement device if a Cisco 802.1X-enabled switch is running DHCP-snooping with RADIUS authentication through a Cisco Access Control Server (ACS). When a DHCP-snooping transaction is completed, the switch sends a log message to the ACS. The ACS logs are sent to the CS-MARS to report the Source IP address, username, connection start and stop times, physical interface, and MAC address of each 802.1X client. Because 802.1X clients are often mobile, remember that 802.1X mitigation actions can occur only when the attacking host is currently connected to the network.



Note

For some 802.1X switch configurations, it is not possible for CS-MARS to determine the correct physical interface to which to push a mitigation command. This occurs for switches, such as the Cisco Catalyst 3550 Multilayer switch, where a FastEthernet and a Gigabit Ethernet port can have the same *module /port* designation (for example, 0/1). Because CS-MARS receives only the *module /port* information from the Cisco ACS logs, it cannot identify the specific port to mitigate. The following message appears in these circumstances:

No mitigation possible. Enforcement device exists but interface names conflict. Determine appropriate interface and mitigate manually.

802.1X Mitigation Example

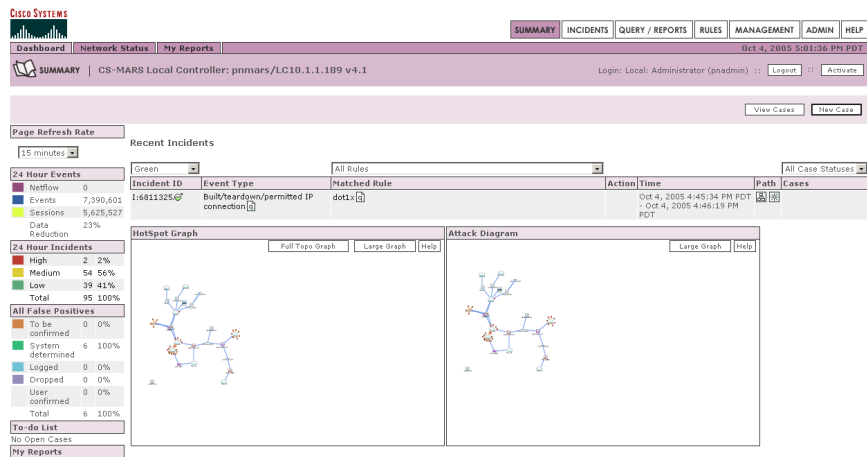
In this procedure, an incident is observed on the Network Summary page, as shown in [Figure 9-9](#), and mitigated through 802.1X network mapping.

Prerequisites for Mitigation with 802.1X Network Mapping

To perform mitigation with 802.1X network mapping with CS-MARS, the following prerequisites are required:

- Cisco switch running Cisco CatOS or IOS and configured with IEEE 802.1X Port Based Network Access Control protocol.
- The switch Reporting IP address must be configured on the CS-MARS Security and Monitoring Information page (**Admin > Security and Monitor Devices**).
- Cisco DHCP-Snooping enabled on the switch
- The switch performs Remote Access Dial-In User Service (RADIUS) authentication, authorization, and accounting through a Cisco Access Control Server (ACS).
- The Cisco ACS is running pnLogAgent to send logs to CS-MARS.
- The Cisco ACS is configured to log Update (Watchdog) packets.

Figure 9-9 Summary Page Displaying Incident to Mitigate

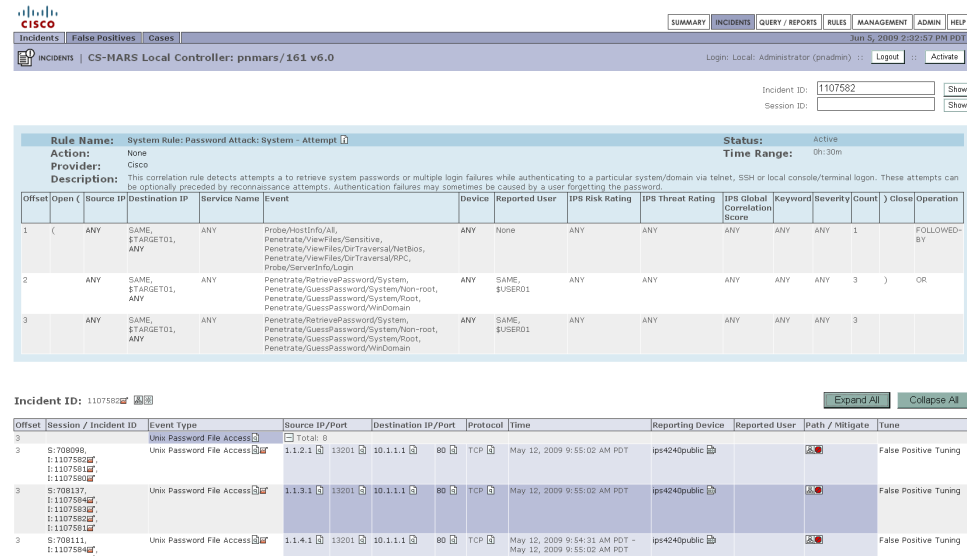


141315

Perform Mitigation with 802.1X Network Mapping

- Step 1** Click the Incident ID of the recent incident to Mitigate.
- Step 2** Click the Incident ID to display the session summaries, shown in Figure 9-10.

Figure 9-10 Incident Detail Page Displaying Red Mitigation Icon

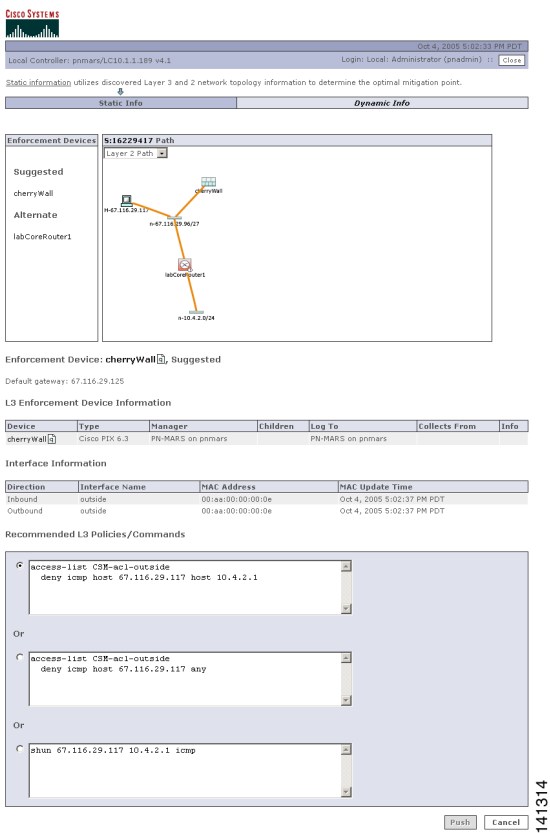


276 48

- Step 3** Click the red path information icon in the **Path/Mitigation** column.
- The Mitigation pop-up window appears, with any possible Static topology and mitigation information, as shown in Figure 9-11.

CS-MARS recommends enforcement devices and mitigation commands. For static information, if the network is entirely discovered and CS-MARS has command level access to a Layer 2 enforcing device, the Push button appears red, otherwise it is gray. In [Figure 9-11](#), CS-MARS does not have sufficient static information to identify a Layer 2 enforcing device, but can suggest mitigation commands for discovered Layer 3 devices (Cisco PIX Firewall, and a Cisco router). Layer 3 mitigation commands must be configured manually on the Layer 3 devices.

Figure 9-11 Path Information Pop-up Window



Step 4 Click **Dynamic Info** to view Layer 2 mitigation recommendations derived from 802.1X configurations. The Dynamic Mitigation window appears with hostname, IP address, MAC address, and connection status as shown in [Figure 9-12](#).

Figure 9-12 **Dynamic Mitigation Information**


Local Controller: pnmars/LC10.1.1.189 v4.1 Login: Local: Administrator (pnadmin) :: [Close](#)

Dynamic information utilizes current host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

↓

Static Info	Dynamic Info								
Host IP Address: 20.1.1.210 Host MAC Address: 00-11-11-31-e3-48 Cisco ACS NAS IP: 10.1.1.243 Cisco ACS NAS Port: 313 AAA User Name: cisco	Enforcement Device: <table border="1"> <thead> <tr> <th>Enforcement Device (Device Name:Module/Port)</th> <th>Start Time</th> <th>End Time</th> <th>Update Time</th> </tr> </thead> <tbody> <tr> <td>dot1x_switch:3/13</td> <td>Oct 3, 2005 2:18:53 PM PDT</td> <td>Present</td> <td>Oct 3, 2005 2:18:53 PM PDT</td> </tr> </tbody> </table>	Enforcement Device (Device Name:Module/Port)	Start Time	End Time	Update Time	dot1x_switch:3/13	Oct 3, 2005 2:18:53 PM PDT	Present	Oct 3, 2005 2:18:53 PM PDT
Enforcement Device (Device Name:Module/Port)	Start Time	End Time	Update Time						
dot1x_switch:3/13	Oct 3, 2005 2:18:53 PM PDT	Present	Oct 3, 2005 2:18:53 PM PDT						

Recommended Policy/Command

☒ `configure t`
`interface 3/13`
`shutdown`

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved. [Feedback](#) 141313

Step 5 Review the enforcement device.

Step 6 Review the Recommended Policies/Commands.

Step 7 Click **Push** to download the recommended mitigation command to the enforcement device. The mitigation confirmation dialog appears, as shown in [Figure 9-13](#).

If the Push button is gray, the mitigation command must be manually configured on the enforcement device.



Note

The **Push** button is red and functional when the 802.1X target host is present on the network, and CS-MARS has command access to the enforcement device otherwise, it appears gray and is not functional.

Figure 9-13 Mitigation Confirmation Dialog

The screenshot shows a web interface for incident management. At the top, there is a header bar with a document icon and the word 'INCIDENTS'. To the right of the header, it displays the login information: 'Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT ::' followed by a 'Close' button. Below the header, the main content area is titled 'Download Mitigation Command'. It contains a form with the following fields: 'Device Name:' with the value 'CatSw', 'Port/Interface Name:' with the value '5/9', 'Access Type:' with the value 'SNMP', 'SNMP RW Community String:' with a masked value '*****', and 'Policy/Command:' with the value 'set port disable 5/9'. Below this form is a confirmation dialog box with the text 'Are you sure you want to download the mitigation command to this device?' and two buttons: 'Yes' and 'No'.

143376

Step 8 Click **Yes** to confirm.

Display Dynamic Device Information

To display current, session, and all historical information for an IP address on an 802.1X connection, follow these steps:

-
- Step 1** Click the Incident ID to display the session summaries as shown in [Figure 9-10](#).
 - Step 2** Click the **Source IP/Port** or **Destination IP** link of a session.
When examining an attacking host, the Source IP address is more relevant.
 - Step 3** The current connection information pop-up window appears to display any static connection information.
 - Step 4** Click **Dynamic Info** to display current connection information. Dynamic information can be derived from 802.1X configurations, Cisco Security Agents, or from other security software suites. The current connection information is the most recent network information available for the selected IP address.
 - Step 5** Click **Session** to display the connections related to the specific session, as shown in [Figure 9-15](#).

Figure 9-14 Dynamic Information—Current Connection Status


Local Controller: pnmars/LC10.1.1.189 v4.1 Login: Local: Administrator (pnadmin) :: [Close](#)

[View Cases](#) [New Case](#)

Dynamic information includes host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

Static Info Dynamic Info

IP Address: 20.1.1.210

[current](#) [session](#) [all](#)

Host Name	MAC Address	AAA User	Enforcement Device (IP:Module/Port)	Reporting Device	Start Time	End Time	Update Time
N/A	00-11-11-31-E3-48	cisco	20.1.1.1:0/2	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:12:37 PM PDT	Present	Oct 4, 2005 4:12:37 PM PDT

Copyright © 2003, 2005 Cisco Systems, Inc. All rights reserved. [Feedback](#)

141312

Step 6 Click **All** to display the entire dynamic information for the specified IP address, as shown in [Figure 9-15](#).

Figure 9-15 Dynamic Information History of a Specified IP Address


Oct 4, 2005 10:35:15 PM PDT
Local Controller: pnmars/LC10.1.1.189 v4.1 Login: Local: Administrator (pnadmin) :: [Close](#)

[View Cases](#) [New Case](#)

Dynamic information includes host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

Static Info Dynamic Info

IP Address: 20.1.1.210

[current](#) [session](#) [all](#)

Host Name	MAC Address	AAA User	Enforcement Device (IP:Module/Port)	Reporting Device	Start Time	End Time	Update Time
N/A	00-11-11-31-E3-48	N/A	20.1.1.1:0/18	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:55:00 PM PDT	Sep 30, 2005 3:59:00 PM PDT	Sep 30, 2005 3:55:00 PM PDT
N/A	N/A	cisco	20.1.1.1:N/A	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:55:00 PM PDT	Sep 30, 2005 4:44:14 PM PDT	Sep 30, 2005 3:55:00 PM PDT
N/A	00-11-11-31-e3-48	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:59:01 PM PDT	Sep 30, 2005 4:44:14 PM PDT	Sep 30, 2005 3:59:01 PM PDT
N/A	N/A	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 3, 2005 2:18:52 PM PDT	Oct 3, 2005 11:16:55 AM PDT
N/A	00-11-11-31-e3-48	N/A	10.1.1.243:N/A	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 4, 2005 4:42:27 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	N/A	cisco	10.1.1.243:N/A	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 4, 2005 4:50:17 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	N/A	N/A	10.1.1.243:3/13	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 2:18:53 PM PDT	Oct 4, 2005 4:09:46 PM PDT	Oct 3, 2005 2:18:53 PM PDT
N/A	N/A	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:09:47 PM PDT	Oct 4, 2005 4:42:27 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	00-11-11-31-E3-48	N/A	20.1.1.1:0/1	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:42:28 PM PDT	Oct 4, 2005 4:50:17 PM PDT	Oct 4, 2005 4:42:28 PM PDT

141311

Step 7 Click the **Push** button if available or mitigate from the device. If you select the push button, a confirmation screen appears.

**Note**

To mitigate a device of Access Type SNMP you must have the SNMP Read/Write Community String.

Click the **Yes** button to confirm the mitigation command and have it take effect.

Virtual Private Network Considerations

Currently, MARS cannot display accurate Path/Mitigation information or compute the complete route of an attack originated by a host with a source IP address on a virtual private network (VPN). MARS can identify the attacking host if the VPN IP address of the host was supplied by a Cisco 3000 Series VPN Concentrator configured as a MARS reporting device.

**Note**

You must be able to recognize from your knowledge of your network that the IP address of the attacking host is an IP address allocated to a VPN.

To identify a host attacking from a VPN, perform a query of “Cisco VPN User connected/disconnected” events for the Cisco VPN Concentrator device. The attacking host name or next network element is disclosed in the raw messages of the events.

Layer 2 Path and Mitigation Configuration Example

This section provides a starting point for configuring MARS to perform Layer 2 (L2) path analysis and mitigation using a Cisco switch.

This section contains the following topics:

- [Prerequisites for Layer 2 Path and Mitigation, page 9-18](#)
- [Components Used, page 9-18](#)
- [Network Diagram, page 9-18](#)
- [Procedures for Layer 2 Path and Mitigation, page 9-20](#)

Prerequisites for Layer 2 Path and Mitigation

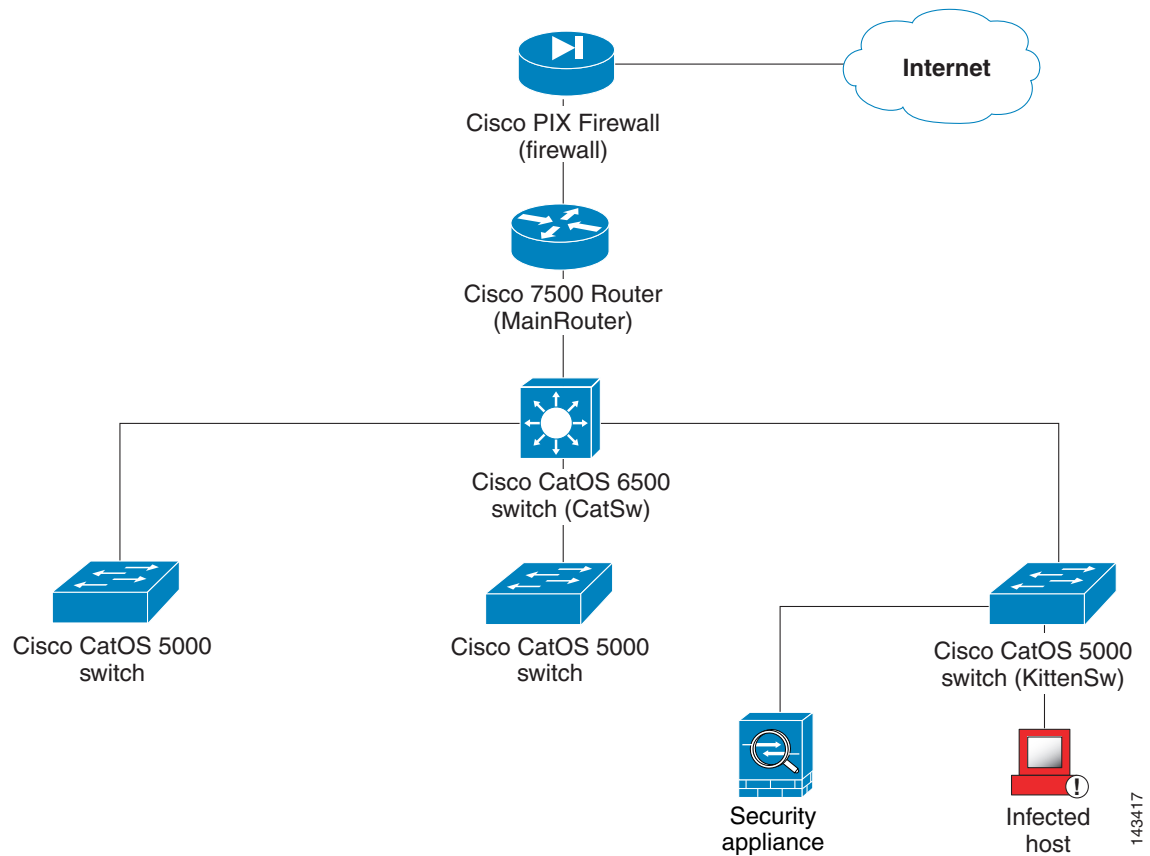
- You need to have the SNMP community strings and IP addresses for the Layer 2 switches and routers.
- You must have STP (Spanning Tree Protocol) configured correctly on the switches.

Components Used

- A Cisco Catalyst 5000 with SNMP access enabled
- A Cisco Catalyst 6500 for Layer 2 with SNMP access enabled
- A Cisco 7500 Router with SNMP or TELNET access enabled
- A MARS running software Version 2.5.1

Network Diagram

This section uses the network setup shown in the [Figure 9-16](#).

Figure 9-16 **Network Setup**

Mitigation uses the Layer 2 path data obtained via SNMP or Telnet protocol to download a mitigation command from the MARS to the device. The Layer 2 path is based on MAC addresses, the Layer 2 forwarding table, and the Layer 3 path. MAC addresses and the Layer 2 forwarding table are obtained using SNMP.

To make the Layer 2 path and mitigation work correctly:

- The associated routers must be discovered via SNMP or a combination of SNMP and Telnet, including the MSFC module in the Catalyst switch.
- The SNMP community string is necessary for L2 switches to be discovered.



Note *L2 devices must be added manually; there is no automatic discovery for these devices. Make sure all the L2 devices (switches) have the SNMP RO community strings specified in the web interface, even if the access type is not SNMP. The SNMP RO community string is always required on Layer 2 devices for L2 mitigation.*

- If the switches are interconnected, make sure STP (Spanning Tree Protocol) is enabled and configured on them.

For example, given a topology such as the one in the preceding figure, follow these instructions to discover these devices.

Procedures for Layer 2 Path and Mitigation

Add the Cisco Catalyst 5000 with SNMP as the Access Type

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

Figure 9-17 *Configure Cisco Switch CatOS*

Device Discovery-Cisco Switch-CatOS ANY

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco Switch-CatOS ANY

Supervisor Module

→ *Device Name:	CatSw
→ *Access IP:	10 1 1 11
→ *Reporting IP:	
→ *Access Type:	SNMP
Login:	
Password:	
Enable Password:	
Config Path:	
File Name:	
SNMP RO Community:	MySNMPCommStr

143361

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-CatOS ANY**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address and **Reporting IP** address (the IP address of the device as it appears to the MARS) of the switch. The **Reporting IP** address is usually the same as the **Access IP** address, but if you are using FTP as Access Type, it must be a different IP address. The **Reporting IP** address is required if the device is sending syslog data to the MARS

Step 5 From the **Access Type** drop-down list, select **SNMP** or **TELNET**. Note that which fields need to be completed, along with which you can complete, depend on which Access Type you select.

SNMP :

- For the **Login ID**, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

Step 6 Click the **Test Connectivity** button to have the MARS discover the device.

Step 7 Click the **Submit** button.

Add the Cisco Catalyst 6500 with SNMP as Access Type (Layer 2 only)

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

Figure 9-18 *Configure Cisco Switch CatOS*

Device Discovery-Cisco Switch-CatOS ANY

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco Switch-CatOS ANY

Supervisor Module

→ *Device Name: KittenSw

→ *Access IP: 10.1.1.12

→ *Reporting IP: . . .

→ *Access Type: SNMP

Login:

Password:

Enable Password:

Config Path:

File Name:

SNMP RO Community: MySNMPCommStr

Test Connectivity Cancel Submit

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-CatOS ANY**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address and **Reporting IP** address of the switch. The **Reporting IP** address is usually the same as the **Access IP** address.

SNMP :

- For the **Login ID**, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

Step 5 Click the **Test Connectivity** button to have the MARS discover the device.

Step 6 Click the **Submit** button.

Add the Cisco 7500 Router with TELNET as the Access Type

Step 1 Click Admin > Security and Monitor Devices > Add.

Figure 9-19 Configure Cisco IOS 12.2

Device Discovery~Cisco IOS 12.2

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * is denotes a required field.

Device Type:
Cisco IOS 12.2

→ *Device Name:
MainRouter

→ *Access IP:
10 1 1 1

→ *Reporting IP:
10 1 1 1

→ *Access Type:
TELNET

Login:
myuserid

Password:
.....

Enable Password:
.....

Config Path:

File Name:

SNMP RO Community:
MySNMPCommStr

Test Connectivity
Cancel
Submit

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-IOS 12.2**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address (optional) and **Reporting IP** address of the switch. The **Reporting IP** address is usually the same as the **Access IP** address.

TELNET :

- For the **Login ID**, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community** (mandatory).

Step 5 Click the **Test Connectivity** button to have the MARS discover the device.

Step 6 Click the **Submit** button.

Verify the Connectivity Paths for Layer 3 and Layer 2

Once you have a session, you can view the Layer 3 and Layer 2 topology paths. There are several ways to obtain a session.

To view sessions that are part of an Incident:

- Step 1** Click the **Incidents** tab to navigate to the Incidents page. Click an **Incident ID** of an incident you want to view (in this example we use Incident number 356120290). The [Figure 9-20](#) appears.

Figure 9-20 Incident Details Screen

Incident ID: 24964272 Show
Session ID: Show

Rule Name: System Rule: Server Attack: Mail - Attempt										Status: Active				
Action: None										Time Range: 0h:30m				
Provider: Cisco														
Description: This correlation rule detects attacks on mail services (SMTP, POP, IMAP) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks to mail services include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.														
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	Keyword	Severity	Count	Close	Operation
1	(	ANY	SAME, \$TARGET01, ANY	ANY	Probe/HostInfo/Mail, Probe/ServerInfo/Mail, Penetrate/GuessPassword/Mail, Penetrate/ViewFiles/Sensitive, Penetrate/SpoofIdentity/TCPID	ANY	None	ANY	ANY	ANY	ANY	1	)	FOLLOWED-BY
2		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/BufferOverflow/Mail, Penetrate/RemoteCmdExec/Mail, DoS/MailServer, Penetrate/Evasion/Mail, Penetrate/SpoofIdentity/Mail, Penetrate/ProtocolAnomaly/Mail	ANY	None	ANY	ANY	ANY	ANY	1	)	OR
3		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/BufferOverflow/Mail, Penetrate/RemoteCmdExec/Mail, DoS/MailServer, Penetrate/Evasion/Mail, Penetrate/SpoofIdentity/Mail, Penetrate/ProtocolAnomaly/Mail	ANY	None	ANY	ANY	ANY	ANY	1		

Expand All Collapse All

Incident ID: 24964272

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
3	S:54322605, I:24964272	SendMail FROM/TO/RCPT Command Exec	1.139.76.65	172.30.1.176	80	TCP	Jul 16, 2008 10:30:15 AM PDT	snorthQ-QA		False Positive Tuning
3	S:54247945, I:24964272	SendMail FROM/TO/RCPT Command Exec	2.150.131.70	172.30.1.176	80	TCP	Jul 16, 2008 10:28:36 AM PDT	snorthQ-QA		False Positive Tuning
3	S:54339819, I:24964272	SendMail FROM/TO/RCPT Command Exec	9.62.99.89	172.30.1.176	80	TCP	Jul 16, 2008 10:30:38 AM PDT	snorthQ-QA		False Positive Tuning
3	S:54196341, I:24964272	SendMail FROM/TO/RCPT Command Exec	10.177.69.79	172.30.1.176	80	TCP	Jul 16, 2008 10:27:26 AM PDT	snorthQ-QA		False Positive Tuning
3	S:54320645, I:24964272	SendMail FROM/TO/RCPT Command Exec	10.189.26.21	172.30.1.176	80	TCP	Jul 16, 2008 10:30:13 AM PDT	snorthQ-QA		False Positive Tuning
3	S:54296626, I:24964272	SendMail FROM/TO/RCPT Command Exec	11.153.149.36	172.30.1.176	80	TCP	Jul 16, 2008 10:29:41 AM PDT	snorthQ-QA		False Positive Tuning

- Step 2** In the [Figure 9-20](#), in the same row as the Event Type you want to examine (in this example we use Windows RPC DCOM Overflow), click the graph icon under the Graph column to view the topology paths.

View Session via a Query

To view sessions by performing a Query:

- Step 1** Click **QUERY / REPORTS** and submit a query using the appropriate query criteria. Note that in our example, we limit the scope of the query so it runs faster. In the following [Figure 9-21](#) we use the result format **All Matching Sessions** and query events from **Source IP 10.1.252.250** and **Destination IP 65.54.153.118** over the last 10 minutes.

Figure 9-21 Query Event Data Screen

Query Event Data

Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 0hh:10mm:0ss* [Edit](#) [Clear](#)

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
H-10.1.252.250	H-65.54.153.118	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [None] [Edit](#)

[Apply](#)

Result Format: All Matching Sessions

Order/Rank By: Time

Filter by Time:

☒ Last: 0 Days 0 Hrs 10 Mins

☐ Start: 2004 June 22 18 Hrs 38 Mins

End: 2004 June 22 18 Hrs 48 Mins

☐ Real Time

Use Only Firing Events: ☐

Maximum rank returned: 100

[Apply](#)

Step 2 After you **Apply** changes to and **Submit** your query, the [Figure 9-22](#) appears.

Figure 9-22 Query Results Screen

Query Event Data

Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 0hh:10mm:0ss* [Edit](#) [Clear](#)

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
H-10.1.252.250	H-65.54.153.118	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [None] [Edit](#)

[Save As Report](#)

[Save As Rule](#)

[Clear](#)

[Apply](#)

[Submit](#)

Query Results 

[Expand All](#)

[Collapse All](#)

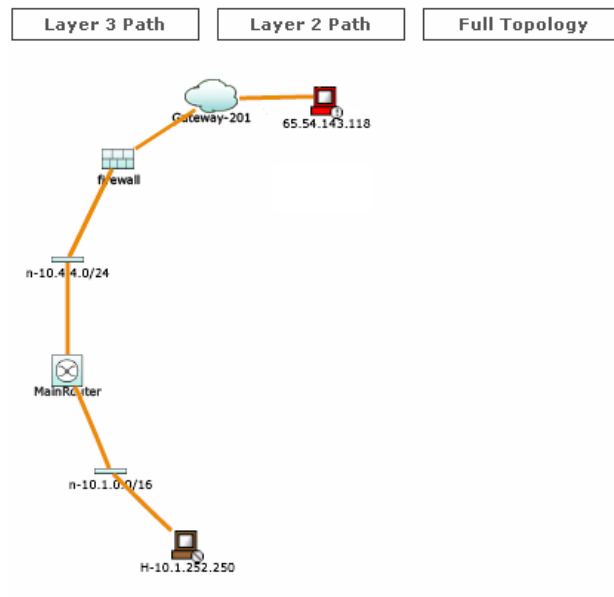
Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
S:381559066	Built/teardown/permitted IP connection 	10.1.252.250 	65.54.143.118 		+ Total: 5 Jun 22, 2004 5:31:15	ProtegoHQ	firewall 		Tune	Mitigate
	Windows RPC DCOM Overflow 	10.1.252.250 	65.54.143.118 	80  TCP 						

Step 3 In the [Figure 9-22](#), in the same row as the Event Type you want to examine (in this example we use Windows RPC DCOM Overflow), click the icon under the Graph column to view the topology paths.

The first topology path to appear is the [Figure 9-23](#):

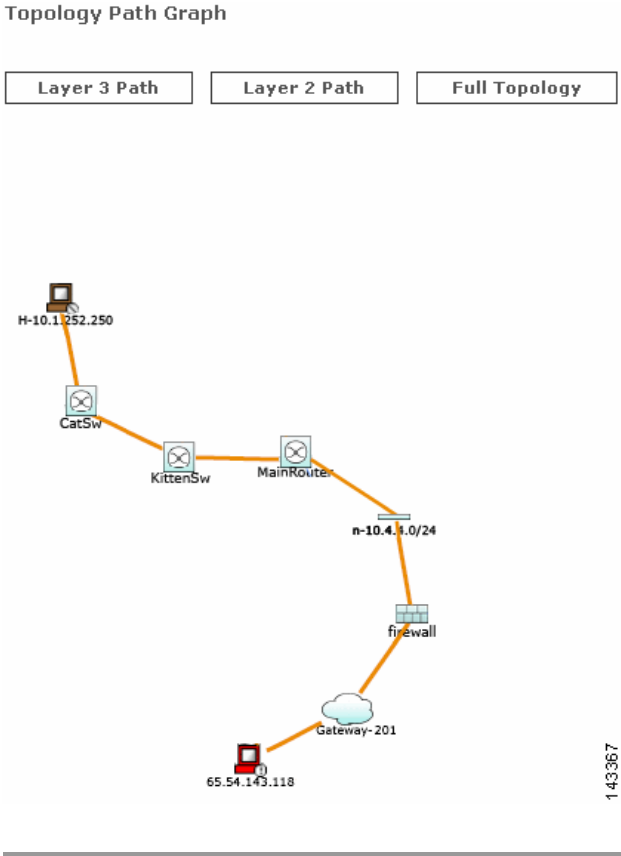
Figure 9-23 Layer 3 Topology Graph

Topology Path Graph



Under **Topology Path Graph**, click the **Layer 2 Path** button to view the [Figure 9-24](#):

Figure 9-24 **Layer 2 Topology Graph**



Perform Mitigation

Once you identify the compromised host (in this example, **10.1.252.250** connected to **CatSw**), it is critical to prevent it from attacking other hosts in the same subnet or other parts of the network. The MARS provides one-click mitigation that lets you isolate the compromised host from the rest of the network.

To perform mitigation, perform these steps:

- Step 1** On the [Figure 9-20](#), click the **Mitigate** link that corresponds with the **Session** or **Event Type** you want to mitigate (in this case, **Windows RPC DCOM Overflow**). The [Figure 9-25](#) appears.

Figure 9-25 Mitigation Information screen

INCIDENTS | Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT :: [Close](#)

Mitigation Information

Enforcement Devices	Enforcement Device - Suggested
CatSw (L2) (suggested)	Name: CatSw
KittenSw (L2) (alternate)	Device type: Cisco Switch-CatOS ANY
MainRouter (alternate)	Outbound Interface: sc0
firewall (alternate)	IP Address: 10.1.1.11
	Mac Address: 00:60:47:f8:7a:ff Jun 22, 2004 5:31:15 PM PDT
	Zone: CA
	Managed by: pnmars
	Status: Active
	Default gateway: 10.1.1.1

Recommended Policy/Command

☒ set port disable 5/10

[Push](#) [Cancel](#)

143377

This screen contains information about the device, along with recommended policies or commands for mitigating the compromised host (in the example, 10.1.252.250).

- Step 2** If the device where the mitigation command to be downloaded is a Layer 2 device (such as in the example [Figure 9-13](#)), a red **Push** button appears that you can click to mitigate the compromised host. If you select the push button, the [Figure 9-13](#) appears.

**Note**

If the device where the mitigation command to be downloaded is a Layer 3 device, the **Push** button shown in red on the [Figure 9-25](#) is greyed out and you must use the suggested commands directly on the device to mitigate the compromised host.

Figure 9-26 Mitigation Confirmation screen

 INCIDENTS

Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT ::

Download Mitigation Command

Device Name:CatSw

Port/Interface Name:5/9

Access Type:SNMP

SNMP RW Community String:

Policy/Command:set port disable 5/9

Are you sure you want to download the mitigation command to this device?

143376



Note

The SNMP RW community string must be enabled for the MARS to download a mitigation command to a device using the Access Type SNMP.

Step 3 Click **Yes** to confirm the mitigation of the device.



CHAPTER 10

Case Management

This chapter contains the following topics:

- [Case Management Overview, page 10-1](#)
- [Hide and Display the Case Bar, page 10-3](#)
- [Create a New Case, page 10-5](#)
- [Edit and Change the Current Case, page 10-6](#)
- [Deselecting the Current Case, page 10-6](#)
- [Add Data to a Case, page 10-7](#)
- [Generate and Email a Case Report, page 10-7](#)

Case Management Overview

The Case Management feature can capture, combine, and preserve user-selected MARS data within a specialized report called a case. The following data can be added to a case:

- Text annotations
- Incident ID page
- Incident device information (source IP address, destination IP address, reporting device)
- Session Information page
- Query Results page
- Build Report page
- Report Results page
- View Case page (the current case can reference another case)

Any user can create or alter any case. You can assign a case to a MARS user on the same machine, and can change the status of a case to assigned, resolved, or closed. The contents of a case are displayed by category on a single GUI page (View Case), and can be automatically assembled into a single HTML case document. You can email the Case Document to any MARS user account or user group.



Note

When a case is closed, you can still email it, annotate it, add device information, and include a reference to another case.

Case information collected on incidents, sessions, queries, reports and mitigation logs are forensic evidence pertinent to the following:

- Audits (for example, regulatory compliance audits)
- Justifications for modifying ACLs or policy changes
- Notes for MARS false positive tuning
- Examples of allowed and prohibited behavior.

The case preserves and displays the selected data as it appeared when the data was added to the case, regardless of subsequent changes to the MARS state. For example, MARS data can be purged, topology can change from automatic discoveries or vulnerability scanning, and overall configuration can change when you edit rules or reports, but the data reported in the case remains the same as the time it was captured.



Note

As of MARS software version 4.1.1 the Case Management feature replaces the incident escalation feature.

The Case Management homepage is the Cases subtab of the Incidents tab as shown in [Generate and Email a Case Report, page 10-7](#).

Figure 10-1 Case Management Tab—Local Controller

Copyright © 2003, 2005 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

1	Case Bar	2	Dropdown Display Filters
3	Individual Cases		

All new, assigned, resolved and closed cases can be accessed from the Cases subtab.

To view the contents of a case, click the Case ID number of a case. The View Case page appears, as shown in [Generate and Email a Case Report, page 10-7](#).

To generate an HTML document of the **View Case** page content that can be emailed, click **View Case Document** at the bottom of the **View Case** page. Graphs and charts plotted from reports are also captured in the Case Document.

Figure 10-2 The View Case Page—Local Controller

1 → Current Case: C:109418 (Assigned) MARS Defends

2 → View Case: C:109418

Case ID	Status	Owner	Summary	Created / Updated
C:109418	Assigned	Local: Administrator (pnadmin)	MARS Defends	Created: Aug 16, 2005 11:07:22 AM PDT Updated: Aug 29, 2005 9:50:11 AM PDT

3 → Case History

User	Action	Comment	Time
Local: Administrator (pnadmin)	Case Opened		Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	State Changed: Assigned	Initial Status: Assigned	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Summary Changed	Initial Summary: Case 4 norm	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Owner Changed: Local: Administrator (pnadmin)	Initial Owner: pnadmin	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Priority Changed: Yellow	Initial Priority: Yellow	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Summary Changed	Case 4 norm2	Aug 16, 2005 11:08:04 AM PDT
Local: Administrator (pnadmin)	Comment	c22	Aug 16, 2005 11:08:04 AM PDT
Local: Administrator (pnadmin)	Session Added: S:5458092		Aug 16, 2005 3:12:29 PM PDT
Local: Administrator (pnadmin)	Device Info Added:	3.1.5.5	Aug 16, 2005 3:12:59 PM PDT
Local: Administrator (pnadmin)	Case Referenced: C:108300 (New) New Case1		Aug 16, 2005 3:17:13 PM PDT
Local: Administrator (pnadmin)	Priority Changed: Red		Aug 16, 2005 3:19:22 PM PDT
Local: Administrator (pnadmin)	Report Added: Activity: All - Top Destination Ports (Peak View)		Aug 16, 2005 3:20:32 PM PDT
Local: Administrator (pnadmin)	Summary Changed	MARS Defends	Aug 29, 2005 9:50:11 AM PDT

4 → Sessions

Display	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune		
☒	S:5458092, I:5336608, I:5336612, I:5336611, I:5336613, I:5336610	Inactive reporting device detected	0.0.0.0	0	3.1.5.5	0	N/A	Aug 16, 2005 3:00:02 AM PDT	pluto	N/A	False Positive

Devices

Display	Device

1	Case Bar—Identifies current case	2	View Case identifier—Shows the attributes of the case
3	Case History—Log of all changes made to the case	4	Summary of data added to the case

Case Management Considerations for the Global Controller

Case management on the Global Controller differs from the Local Controller implementation as follows:

- Cases are not created on a Global Controller. They can be viewed and modified.
- The Global Controller does not have a Case Bar. All Cases are selected from the Incident -> Cases page.
- The Cases page has an additional dropdown filter to display cases per Local Controller.

Hide and Display the Case Bar

The Case Bar displays by default. When displayed, the Case Bar appears at the top of each page. The Case Bar must be displayed to create or modify a case.

This section contains the following topics:

- [Hiding the Case Bar, page 10-4](#)
- [Displaying the Case Bar, page 10-4](#)

Hiding the Case Bar

To hide the Case Bar, follow these steps:

- Step 1** Navigate to the **Cases** subtab (**Incidents > Cases**), as shown in [Figure 10-3](#).

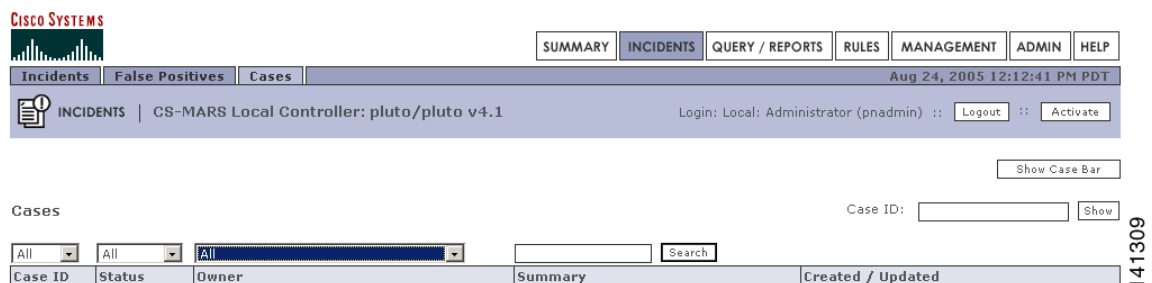
Figure 10-3 Case Bar Displayed on the Incidents Page



- Step 2** Click **Hide Case Bar**.

The Case Bar no longer appears on all tabs, as shown in [Figure 10-4](#).

Figure 10-4 Case Bar Hidden on the Incidents Page



Displaying the Case Bar

To Display the Case Bar, follow these steps:

- Step 1** Navigate to the **Cases** subtab (**Incidents > Cases**) as shown in [Figure 10-4](#).
- Step 2** Click **Show Case Bar**.

The Case Bar, as shown in [Figure 10-3](#) now appears on all pages.

Create a New Case

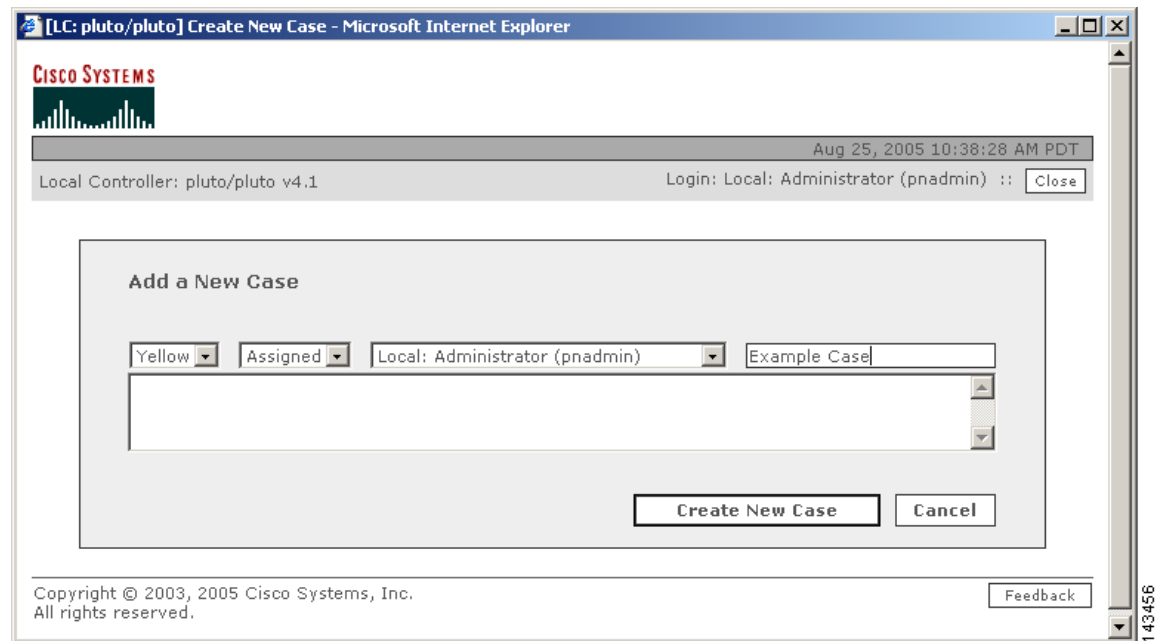
To create a new case, follow these steps:

Step 1 Display the Case Bar as described in the section [Hide and Display the Case Bar](#), page 10-3.

Step 2 Click **New Case**.

The Add a New Case Dialog box appears, as shown in [Figure 10-5](#).

Figure 10-5 Add a New Case Dialog Box



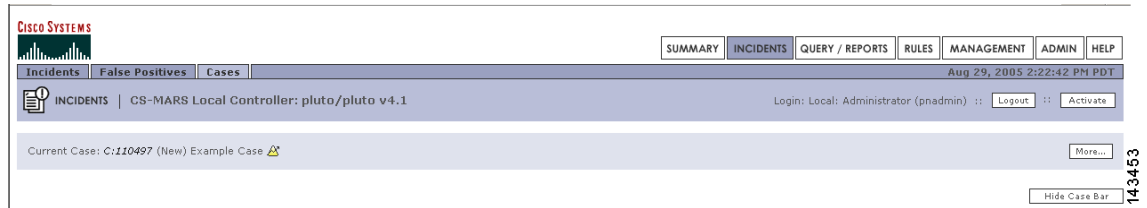
Step 3 Select a severity color, change the state from new to assigned if appropriate, select the owner, replace the default summary name (default is New Case).

[Figure 10-5](#) shows a case with case summary of Example_Case, assigned to the administrator with a yellow priority color (default is Green).

Step 4 Type or paste any annotations into the text space.

Step 5 Click **Create New Case**.

The newly created case is numbered and becomes the current case displayed in the Case Bar as shown in [Figure 10-6](#).

Figure 10-6 Case Bar Shows a Newly-Created Case as the Current Case

Proceed to the section [Add Data to a Case, page 10-7](#) for steps on how to combine various data into a single case.

Edit and Change the Current Case

To edit the Current Case, follow these steps:

- Step 1** Display the Case Bar and click **More**.

The Case Bar Expands to expose the editing options, as shown in [Figure 10-7](#). See the section [Hide and Display the Case Bar, page 10-3](#) for procedures to display the case bar.

Figure 10-7 Expanded Case Bar

- Step 2** Change the severity, status, owner, or summary of the case as required.
- Step 3** Add an annotation in the text box as required.
- Step 4** Click **Submit**.

Deselecting the Current Case

To replace the Current Case case with another, follow these steps:

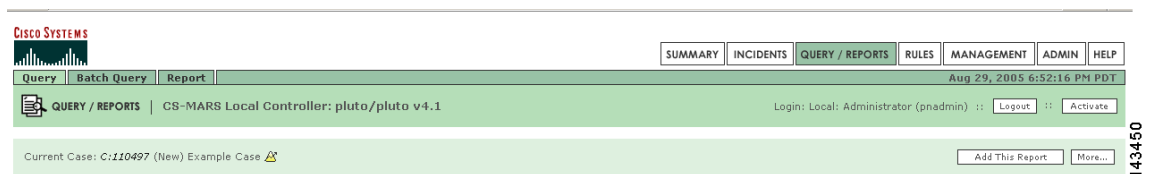
- Step 1** Expand the Case Bar as explained in the previous procedure.
- Step 2** Click **Deselect**.
- The Case Bar drop-down list displays **No Case Selected...** as shown in [Figure 10-4](#).
- Step 3** To select a different Current Case, select a case from the Case Bar drop down list.

Add Data to a Case

To add data to a case, follow these steps:

- Step 1** Select the Current Case. See the section [Edit and Change the Current Case, page 10-6](#) for procedures on selecting the Current Case.
- Step 2** Navigate to the page to be captured in the case. In the example, the Query page is selected.
- Step 3** Click **Add this...** on the Case Bar.

Figure 10-8 Case Bar Add Button



- Step 4** To verify that the selected data was added to the case, click the case ID number in the Case Bar to display the View Case page.

In the example shown in [Figure 10-8](#), the selected report should appear in the Reports section of the View Case page. A partial View Case page is shown in [Figure 10-2](#).

Generate and Email a Case Report

You can generate a case report of the case data and email the report to any MARS user group or individual user account. The email event is logged in the case history listings on the View Case page.

To add a new user account or user group, see [Create a User—Role, Identity, Password, and Notification Information, page 5-13](#).



Note

Make sure that the MARS email server is configured. See [Configure the E-mail Server Settings, page 5-7](#) for further information.

To generate a case report and to email it, follow these steps:

- Step 1** Select a case from the Cases page or from the Case Bar dropdown list.
- Step 2** Click the Case ID number to navigate to the **View Case** page.
- Step 3** Click the check box in an item's **Include** field to select or deselect that item for inclusion in the Case Document. By default, all items are selected.



Tip

Click **Show Include** to show only those items selected for the Case Document. **Show Include** does not function for cases created in Cisco Security MARS version 4.1.1.

Step 4 Click **View Case Document** at the bottom of the **View Case** page.

MARS generates and displays the case report.

Step 5 Click **Email Case** at the bottom of the report page.

The Case Email dialog box appears, as shown in [Figure 10-9](#).

Figure 10-9 Case Management Email Dialog Box

Step 6 Click the check box of the user groups or individual users you want to receive the Case Document, then click << **Add**.



Tip Select **All Users** from the dropdown menu to display all individual user accounts.

The selected recipients appear in the left-hand area of the dialog box.

Step 7 Click **Submit** to send the Case Document to the recipients.

The email is sent and the case history is updated to show the email event as the latest item of the case history.



CHAPTER 11

Security Manager Policy Table Lookup from a MARS Event

This chapter describes how to configure and use Security Manager and MARS to enable bidirectional lookup starting either with events received by MARS or with access rule and signature policy information found in Security Manager.

While Security Manager enables you to centrally manage security policies and device settings in large scale networks, Cisco Security MARS identifies, isolates, and recommends precise removal of compromised network elements. Cisco Security MARS does this by transforming raw security data into an easily-readable format to subvert valid security incidents and maintain compliance. MARS integrates with Security Manager to map traffic-related syslog messages to the firewall or signature policy in Security Manager that triggered the event. Policy lookup enables rapid, round-trip analysis for troubleshooting firewall configuration-related network issues and policy configuration errors, and for fine-tuning defined policies. Following suggestions from MARS on access rule and signature changes to block the traffic, you can use Security Manager to ensure that the configuration management solution stays abreast of the mitigation responses. Security Manager can also publish the same change to all like devices that it manages, providing a more robust containment.

Beginning with Security Manager 3.2, you can modify access rules generating a MARS event seamlessly from the read-only policy table popup window. All the rules associated with an event are displayed, and by clicking the highlighted access rule number you can modify the rule without starting Security Manager separately. Similarly, you can navigate to the signature summary table in Security Manager from MARS events associated with IPS sensors and IOS IPS devices—or virtual devices—and alter the signature properties. This feature enables you to map a syslog message to the policy that triggered that message and modify it directly, thereby reducing time spent configuring and troubleshooting access rules in large or complex networks.



Note

Only with the release of MARS version 6.0.1 could events associated with virtual sensors be tracked back to the individual virtual sensor.

For example, consider the following case where a user cannot connect to *destination X* from *source Y*. To troubleshoot this issue, you can do the following:

1. Log in to the MARS web interface and use an on-demand query to determine whether any received events indicate that traffic was blocked between *source Y* and *destination X*.

2. If such events are found,  can determine which access rule blocks the traffic and then click the Security Manager icon () in the row of one of the selected events. MARS then queries Security Manager to retrieve the list of access rules that match that traffic flow. Assuming that Security Manager manages the routers and firewalls between *source Y* and *destination X*, a list of matching access rules are returned.
3. Finally, you can click the access rule number to log in to Security Manager and may edit the identified policy, or access rule, to allow traffic between *source Y* and *destination X*. MARS reuses the already running Security Manager session, if one exists, or starts a new session using the Security Manager login credentials defined in MARS.

This chapter contains the following topics:

- [Taskflow for Policy Table Query from MARS Events, page 11-2](#)
- [Understanding Security Manager Device Lookup, page 11-4](#)
- [Understanding Access Rule Table Lookup, page 11-5](#)
- [Understanding Signature Table Lookup, page 11-8](#)
- [Issues Regarding Policy Table Lookup from MARS, page 11-8](#)
- [Checklist for Policy Table Lookup from MARS, page 11-14](#)
- [Devices and OS Versions Supported by Both Security Manager and MARS, page 11-15](#)
- [Bootstrapping Security Manager Server to Communicate with MARS, page 11-16](#)
- [Adding a Security Manager Server to MARS GC, page 11-16](#)
- [Adding a Security Manager Server to MARS LC, page 11-20](#)
- [Navigating to Access Rule Policy in Security Manager from MARS, page 11-24](#)
- [Navigating to IPS Signature Policy in Security Manager from MARS, page 11-28](#)
- [Read-Only Security Manager Policy Lookup Page for Access Rules, page 11-35](#)
- [Read-Only Security Manager Policy Lookup Page for an IPS Signature, page 11-39](#)

Taskflow for Policy Table Query from MARS Events

The Security Manager icon () appears in the Reporting Device column of the MARS session display when MARS receives a syslog triggered by the following:

- Matches against access rules from a Cisco PIX Firewall, Cisco Adaptive Security Appliance (Cisco ASA), Cisco Firewall Services Module (Cisco FWSM), or Cisco IOS, and the five tuple information required to establish an event (source IP, destination IP, source port, destination port, and protocol) can be derived.



Note

In earlier versions MARS did not fully support IPS virtual sensors. The events reported from virtual sensors would appear to be coming from the IPS device reporting it on behalf of the virtual sensor. Beginning with MARS 6.0.1, events from virtual sensors now correctly appear as coming from the virtual sensors that created them.

- Connection establishment and tear-down using TCP, UDP, and ICMP on security appliances and FWSM blades.
- Firing of signatures from IPS and IOS IPS devices.

Clicking the icon queries Security Manager, which identifies the access rule in the policy table of the device that created the traffic incident or event. The following steps depict the policy query process between MARS and Security Manager:

1. From the Summary, Incidents, or Query page, navigate to the Incident Details page or the Query Results page for a particular incident ID and click the Security Manager icon in the Reporting Device field to invoke the policy table lookup.
2. MARS establishes an HTTPS connection in one of two ways, depending on the authentication mechanism chosen while adding Security Manager to MARS:
 - by using the MARS credentials or prompting the user for login credentials
 - or, by using the Security Manager username and password saved in the MARS database
3. If authentication fails, MARS displays an error message in a popup window. On successful authentication, MARS requests the device ID from Security Manager by providing the hostname and IP address.
4. If more than one device matches the MARS query criteria, all matching reporting devices are displayed in a popup window from which you can select the device for which you need to modify the access rule. If only one device matches the MARS query criteria, step 5 is performed. If no device matches the query criteria, an error message is displayed. For more information, see [Understanding Security Manager Device Lookup, page 11-4](#).
5. MARS performs one of the following actions, depending on the type of syslog that generated the event:
 - If an access rule triggered the syslog on ASA devices, PIX security appliances, IOS routers, or FWSM blades, MARS sends the syslog message to Security Manager. Security Manager then looks up the policy table for all access rules that match the device ID and five-tuple data. MARS also provides the action, direction, interface, and ACL name information.



Note Beginning with MARS 6.0.1, NetFlow Security Event Logging (using Netflow v9 fields and templates) can be used, in place of syslogs, to enable bidirectional navigation between events from ASA devices that employ NetFlow and corresponding policies in Security Manager.

- If a TCP, UDP, or ICMP connection establishment or teardown resulted in the syslog on ASA, PIX, or FWSM devices, MARS sends the raw syslog message to Security Manager for processing. Security Manager looks for all access rules that match the device ID, five-tuple data, direction of traffic flow, and mapped (NATed) IP addresses in the message.
- If the signature on an IPS or IOS IPS device—or virtual device—triggered the syslog, MARS requests all signature policies that match the device, signature, and subsignature IDs.

For more information on how Security Manager analyzes the syslogs from MARS and retrieves matching policies from the Access Rules page, see [Understanding Access Rule Table Lookup, page 11-5](#). For more information on how the signature associated with an IPS event is retrieved from the signature policy table, see [Understanding Signature Table Lookup, page 11-8](#).

6. The policy table lookup query is done in one of the following three ways, depending on whether Workflow or non-Workflow mode is enabled and Security Manager client is running or not.
 - **Security Manager client is not running and either Workflow or non-Workflow mode is enabled in Security Manager**—the lookup query is performed on the policies committed to the Security Manager database.

- **Workflow mode is enabled and an instance of the Security Manager client is active**—the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in data committed to the Security Manager database.
 - **Non-Workflow mode is enabled and a Security Manager client session is open**—the lookup operation is performed on all policies in the current login session (within the context of the automatically created activity in non-Workflow mode).
7. For events generated by access rules and connection establishment and tear-down syslogs, MARS displays the read-only access rule policy lookup table with matching rules highlighted from which you can navigate to the Access rules page of Security Manager and fine-tune the policy. For IPS events, MARS displays the read-only signature details page from which you can click Edit Signature to navigate to the Signatures policy page in Security Manager and modify the highlighted IPS signature that generated the event.
 8. For access rule and connection-related syslogs, click the hyperlinked rule number from the read-only access rule table window to start the Security Manager client and modify the highlighted rule. For syslogs triggered by IPS signatures, click Edit Signature from the read-only popup window to start the Security Manager client and modify the highlighted signature. You can also configure an event action filter to remove one or more actions from a signature event.

The Security Manager client is started from MARS in one of the following three ways:

- If the Security Manager client is not installed on the system to which the policy lookup query was made, you are prompted to install the Security Manager client and the page for downloading the application is opened.
- If an instance of the Security Manager client is already running, the existing session is reused.
- If the Security Manager client session has timed out or an instance is not active, a new instance of the Security Manager client is started.

Understanding Security Manager Device Lookup

MARS requests the access rule and signature policy table of a device that Security Manager administers by supplying the following criteria to Security Manager:

- **Device Name**—Derived from the Device Name field in the Security and Monitoring Information page of MARS.



Note

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.

When you add FWSM and ASA devices with multiple security contexts to Security Manager, the context name is set as the hostname in the Device Properties page and policy lookup from MARS events for these contexts works properly. If the hostname is not the same as the context name, policy lookup from events fails. In such cases, for policy lookup to work correctly, ensure that the hostname defined for that context in the Device Name field of the MARS GUI matches the hostname configured in the Device Properties page of Security Manager.

- **IP Address**—Derived from the Reporting IP field in the Security and Monitoring Information page of MARS.
- **Domain Name**—If available, derived from the device name in MARS (for example, c3550-225-125.clab.cisco.com).

The Device Lookup query takes the following actions between MARS and Security Manager:

1. Security Manager matches the MARS Device Name to the Security Manager host names. If only one matching hostname is discovered, the process for Policy Table Lookup is invoked.
2. If there are multiple matches on hostname and no unique display name matches, the domain name (if available) is used to narrow the choices.
3. If the domain name is not available, MARS Reporting IP is used to narrow the choices.
4. If a unique device cannot be identified, MARS displays a list of possible devices in a popup window that shows the IP address, host name, display name, and domain name for all possible device matches. The user manually selects the device and the process for the policy table lookup is invoked.

Understanding Access Rule Table Lookup

The device lookup information is combined with the event information to perform the Security Manager access rule table lookup.

Security Manager 3.2 integration with MARS for access rule table lookup supports more accurate mapping of MARS syslogs (events) to Security Manager access rules and reduces the number of irrelevant matches, thereby enabling faster and improved troubleshooting of access rules. This improved behavior is accomplished because MARS sends Security Manager the raw syslog message and not just the parsed event information, such as the event 5-tuple, action, ACL name, interface, and direction of flow. Using the raw event sent by MARS, Security Manager extracts critical data about the direction of traffic flow and other details, such as pre-NAT and post-NAT addresses. After the most accurately matching policy is found, Security Manager passes the information to MARS, which is translated in a readable format.

Beginning with MARS 6.0.1, NetFlow Security Event Logging (using Netflow v9 fields and templates) can be used, in place of syslogs, to enable bidirectional navigation between events from ASA devices that employ NetFlow and corresponding policies in Security Manager. For additional details, see [NetFlow Version 9 Flow-Record Format](#).

TCP and UDP connection setup/teardown syslogs represent the traffic flow through the firewall. A connection setup syslog is generated when a session is established through the device, when traffic flows to the device, or when traffic flows from the device. Each connection setup syslog has an associated teardown syslog, which is generated when the session is terminated. Although both the setup and teardown syslogs share a common connection ID, the teardown syslog does not contain the pre-NATed address and direction information. For teardown syslogs, MARS also transmits the corresponding setup syslog for that connection because it contains the necessary information for an accurate match. For sessionized events, MARS also sends the session object, which contains NATed details, to Security Manager for lookup. Security Manager parses the details from the syslog in raw format and performs two queries, instead of one, on the policy database to find a matching permit ACE in the inbound and outbound interfaces in the “in” and “out” directions, respectively. As a result, each policy query for a connection setup/teardown syslog yields zero, one, or two matches, depending on the configuration of a permit ACE on that interface in the specified direction. A maximum of two matching rules is displayed in the read-only access rule table popup window after the lookup.

ICMP connection setup and teardown syslogs do not contain the ICMP code, type, interface names, direction keyword, and a connection ID. Therefore, lookup of access rules for ICMP setup/teardown syslogs is not as accurate as their TCP and UDP counterparts owing to the absence of necessary details to locate an exact match. However, the ICMP setup/teardown syslogs associated with management traffic to and from a device are handled slightly differently. For management traffic triggered by TCP and UDP connection-related messages, Security Manager checks for the presence of the “NP Identity Ifc” keyword as the second interface in the syslog format for these protocols to obtain the most accurate matches for the lookup query. Although the Security Manager icon is displayed for events generated by ICMP connection teardown syslogs, an error message is displayed when you perform policy lookup from these events. The error message states that the corresponding connection setup syslog for the teardown syslog could not be found and asks you to try this operation after a few seconds. However, the same error is displayed even if you perform lookup at a later time.

Each syslog generated by an access rule or connection setup/teardown is associated with a unique ID. You can navigate to the policy rules that trigger syslogs in MARS from the Incident Details page by clicking the Security Manager icon. You can query policies only from those syslog IDs that are supported by MARS and Security Manager. For details on the syslog IDs supported by MARS and Security Manager for policy lookup from events, see [Security Appliance and Router System Log Messages Supported for Policy Lookup, page 11-7](#).

MARS displays the policy table in a popup window. The matching access rule is displayed in highlight. If MARS was unable to provide the interface, direction, and action information, multiple matched access rules may be highlighted.

Example 11-1 Sample TCP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:05:59 2.168.154.2 : %ASA-2-302013: Built outbound TCP connection 42210
for outside:9.1.154.12/23 (9.1.154.12/23) to inside:2.168.154.12/4402 (192.168.154.12/4402)
Mar 19 2007 21:06:27 2.168.154.2 : %ASA-2-302014: Teardown TCP connection 42210
for outside:9.1.154.12/23 to inside:2.168.154.12/4402 duration 0:00:27 bytes 462 TCP Reset-O
```

Example 11-2 Sample ICMP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:03:44 2.168.154.2 : %ASA-2-302021: Teardown ICMP connection
for faddr 9.1.154.12/0 gaddr 192.168.154.12/768 laddr 2.168.154.12/768
Mar 19 2007 21:03:44 2.168.154.2 : %ASA-2-302020: Built ICMP connection
for faddr 9.1.154.12/0 gaddr 192.168.154.12/768 laddr 2.168.154.12/768
```

Example 11-3 Sample UDP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:08:53 2.168.154.2 : %ASA-2-302015: Built outbound UDP connection 42214
for outside:9.1.154.12/70 (9.1.154.12/70) to inside:2.168.154.12/4403 (192.168.154.12/4403)
Mar 19 2007 21:10:55 2.168.154.2 : %ASA-2-302016: Teardown UDP connection 42214
for outside:9.1.154.12/70 to inside:2.168.154.12/4403 duration 0:02:02 bytes 34
```

Example 11-4 Sample Cisco PIX Firewall Syslog Messages with Access Group Name Information

```
10.33.10.2 <142>%PIX-4-106023: Deny tcp src inside:10.1.5.234/3010 dst outside:5.6.7.8/21
by access-group "Cisco Security Manager-acl-inside"
```

Example 11-5 Sample Cisco IOS 12.2 Syslog Messages with ACL Name Information

```
100.1.20.2 Mon Jun 9 14:46:31 2003 <46>485232: Jun 9 14:46:29 PDT: %SEC-6-IPACCESSLOGP: list
```

```
Cisco Security Manager-acl-FastEthernet0/0 permitted tcp 1.234.51.255(12000) -> 100.1.4.10(25), 1540 packet
10.34.1.1 <46>146570: Dec 19 21:01:57 PST: %SEC-6-IPACCESSLOGP: list
Cisco Security Manager-acl-FastEthernet1/0 denied tcp 10.10.1.20(59399) -> 10.1.5.11(23), 1 packet
```

Security Appliance and Router System Log Messages Supported for Policy Lookup

You can configure logging options on security appliances when a deny ACE matches a packet for network access (an access list applied with the access-group command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, the default logging occurs, using system log message 106023. In devices with multiple contexts, each security context includes its own logging configuration and generates its own messages.

System log messages begin with a percent sign (%) and are structured as follows:

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

A unique 6-digit number identifies each message. The following syslog message IDs are supported for looking up policies in Security Manager from incidents generated in MARS.



Note

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: 106100, 106023, 302013, 302014, 302015, 302016, 302020, 302021

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. For details on the message, explanation, and recommended action for each of these message IDs, see the System Message Guide of the relevant product documentation.

On Cisco IOS routers, system log messages are generated for access lists configured with the **log** or **log-input** keywords. Use the **log** keyword to get access list logging messages, including violations. Use the **log-input** keyword to include input interface, source MAC address, or virtual circuit in the logging output. The first packet that triggers the access list causes an immediate logging message, and subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval. You can look up access rules that generate these log messages by clicking the Security Manager policy query icon in the Incident Details page or the Query Results page of MARS.

For IOS routers, system log messages with the following identifiers support policy lookup and the Security Manager icon is displayed beside them in the MARS GUI:

```
%SEC-6-IPACCESSLOGDP, %SEC-6-IPACCESSLOGNP, %SEC-6-IPACCESSLOGS,
%SEC-6-IPACCESSLOGP
```

For IOS system log messages with IDs other than the ones listed above and that are not generated by access rules, the Security Manager icon is not displayed in the MARS GUI.

Understanding Signature Table Lookup

Security Manager 3.2 and MARS support signature summary table lookup for events generated by IPS devices (Cisco IPS sensors and Cisco IOS IPS devices) and IDS sensors. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as DoS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define. The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alert. Signature-based intrusion detection can produce false positives that you can minimize by tuning your signatures. Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature.



Note

Beginning with MARS 6.0.1, events from virtual sensors now correctly appear as coming from the virtual sensors that created them.

Security Manager looks for the following criteria from the raw event message that MARS sends for IPS events:

- **Signature ID**—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature.
- **SubSignature ID**—Identifies the unique numerical value assigned to this subsignature. A subsignature ID is used to identify a more granular version of a broad signature.



Note

Packet Data events that identify the data that was being transmitted on the network the instant an alarm was detected on IPS and IDS sensors can cause the size of the raw message associated with this event to become very huge. Also, these events are not triggered by signature rules on sensors. As a result, the Security Manager icon is not displayed for Packet Data events in the MARS GUI for policy lookup.

Events triggered by custom signature configured on a sensor are categorized as “Unknown Device Event Type” in the MARS GUI and the Security Manager icon is displayed for these events to enable policy lookup.

After a match is found, Security Manager transmits the signature details to MARS and the matching signature parameters are displayed in a read-only popup window in MARS. You can click Edit Signature to navigate to the signature summary table of Security Manager with the matching signature selected. You can also click Event Action Filter from the read-only popup window to configure a filter on the basis of signature categories to remove one or more actions from the signature event. The filter is applied in the order specified in the summary table. The authentication mechanism that you entered while adding Security Manager to MARS is used to open the signature summary table and a new instance of Security Manager is started if one is not running or the existing session times out.

Issues Regarding Policy Table Lookup from MARS

The following collection of issues and points may assist you when you are establishing or troubleshooting MARS/ Security Manager interoperation:

General Issues

- If you modify the access rule in Security Manager after the read-only policy query window is displayed with highlighted rules that generated the event and start the Security Manager client, the rule table in the read-only policy page is used as the basis for displaying the matched rule in Security Manager and the modified rule table in Security Manager is not considered.
- If an access rule policy contains network/host and service objects, the definitions of the elements contained in these objects are displayed in the read-only policy lookup table. For the matching policy, the definitions of the network and service objects are expanded and displayed.
- MARS displays the Security Manager security policy committed views, not the deployed views. If you change the access rule in Security Manager and do not deploy the changes to the device, the syslog is generated by the older access rule on the device because the changes are not synchronized and policy lookup is performed on the access rule saved on the device and not on the most recently saved changes in Security Manager.
- The same events received by MARS can display the Security Manager policy table lookup icon inconsistently between the low-latency, realtime event query and standard queries, such as sessions ranked by time. Specifically, the icon will not appear in the low-latency, realtime query, but it may appear in queries against sessionized events. This behavior is expected. When MARS receives events, they are parsed, sessionized, written to an event shared buffer, and then written to the database. Because sessionization takes time, sometimes keeping an event in cache for 2 minutes, the low-latency event query displays events right after parsing, but before sessionization. Displaying the event at this point allows the low-latency query to achieve a close to realtime effect. For some events, parsing cannot determine some part of the 5-tuple data, such as a destination address. Later, sessionization later fills in such missing data using configuration data. As a result, the 5-tuple data displayed by the low-latency event query can be different from values stored in the database, which are used to populate the standard queries.
- The Security Manager policy table lookup icon is not displayed for NetFlow events received by MARS from NetFlow-enabled reporting devices that are positioned within your network because they are not triggered by an access rule.
- If a modal window or dialog box is open in Security Manager or the modal window is overlaid with any other application window, an error message is displayed when the policy lookup query is performed. Close the modal dialog box in Security Manager and retry the task.
- For PIX and ASA devices or FWSM blades with multiple security contexts, you must enter the reporting IP address for each context while configuring the device in MARS. Otherwise, the Security Manager icon is not displayed beside events received from the contexts for which the reporting IP address is not defined in MARS and you can query events from such contexts only by running a query for “Unknown Reporting Devices” from MARS.
- A Local Controller can be configured to retrieve the policy tables from only one Security Manager server at a time. An error message is displayed when you attempt to add more than Security Manager server to a Local Controller.
- If you add a Local Controller, to which Security Manager server has been added, to a Global Controller, you can view the Security Manager server in the Security and Monitoring Information list of the Local Controller from the Global Controller interface. However, the Security Manager policy query icon is not displayed beside events or incidents displayed on a Global Controller.
- All users associated with any of the CiscoWorks Common Services roles except the Help Desk role or any of the predefined Cisco Secure ACS roles have permission to modify the matching policy by clicking the Security Manager icon from the read-only policy lookup table.
- While adding a Security Manager to MARS, only users with Admin role can be configured to enable MARS contact and discover Security Manager server configuration. Otherwise, an error message is displayed when you submit your changes.

- If the Security Manager server cannot be reached from MARS when you perform a policy lookup, an error message is displayed asking you to restore the connection between MARS and Security Manager.
- If HTTPS is not enabled on Security Manager for secure access between the Security Manager server and MARS, an error message is displayed when you try to start Security Manager. Ensure HTTPS is enabled on the Security Manager server so that communication between the Security Manager and MARS is encrypted.
- If the Daemon Manager on the Security Manager server is not running, an error message is displayed prompting you to restart the service when you perform the policy table lookup.
- The time taken to display the policy table lookup query results is proportional to the number of rules in the policy table of Security Manager. Increased number of rules might impact the performance of MARS and Security Manager.
- The policy rules retrieved from the Security Manager policy table and displayed in the read-only policy query window in MARS are cached to enhance performance. Caching reduces the time taken to display query results on subsequent lookups as the query results are reused when a request is made to query policies for the same event.
- The Security Manager policy table lookup icon in MARS is displayed only for traffic logs triggered by the following event types:
 - Matching of Access rules from a PIX firewall, ASA device, IOS router, or an FWSM blade, regardless of whether the 5-tuple information is available or not. If the 5-tuple data cannot be derived from the syslog, the most accurate match is displayed after policy table lookup.
 - Connection establishment and tear-down using TCP, UDP, and ICMP on PIX, ASA, and FWSM devices.
 - Firing of signatures from IPS and IOS IPS devices.

**Note**

The versions of software running on the devices that report syslogs to MARS and for which policies are defined in Security Manager must be supported by both Security Manager and MARS. See [Devices and OS Versions Supported by Both Security Manager and MARS, page 11-15](#) for a list of devices supported by both Security Manager and MARS.

Credential Issues

- All users associated with any of the MARS roles with the exception of the Operator and Notifications Only roles can modify the Security Manager authentication credentials while editing an existing user account in MARS.
- The MARS Appliance compares the certificate presented by Security Manager with a previously stored instance of the certificate while establishing a secure connection with Security Manager. If a conflict is detected, MARS accepts and stores the replacement certificate, either automatically or after prompting for manual acceptance, depending on the options configured in MARS. For more information on how MARS responds during attempts to establish a secure connection, see *User Guide for Cisco Security MARS Local Controller 4.3.x and 5.3.x*.
- The Security Manager username and password values that you enter or modify in the Reporting Applications tab is used by MARS to communicate with Security Manager server and discover meta information, such as version of software running on the server and configuration details. These credentials are different from the username and password in the Cisco Security Manager section of the User Configuration page.

The username and password pair in the User Configuration page comprise the credentials that MARS uses to authenticate with Security Manager to look up the policy table, when you select the option to use Security Manager credentials for policy lookup. The Security Manager username and password fields in the User Configuration page are populated with the values you enter in the policy query login dialog box if you chose to allow saving of Security Manager login credentials during policy lookup.

- If you did not specify the username and password for logging in to Security Manager or entered incorrect credentials while adding Security Manager, the connectivity test fails and an error message is displayed. Similarly, if you changed the login credentials in Security Manager but failed to update them in the MARS GUI, an error message is displayed during policy lookup.
- If you selected the option to use the Security Manager login credentials for MARS to authenticate with Security Manager and did not choose to allow the login credentials to be saved in the login dialog box, these credentials are cached until you exit MARS or the idle session timeout period is exceeded; you are not prompted for login details until the MARS session is active. If the Security Manager session times out after MARS has successfully authenticated with Security Manager and you selected the option to be prompted for login credentials for policy table lookup, the login dialog box is displayed when you click the Security Manager icon from a MARS syslog.
- If you selected the option to be prompted for Security Manager login credentials to authenticate MARS during policy table lookup and deleted the Security Manager server from the MARS database, the username and password fields under the Cisco Security Manager section of the User Configuration Page (Management > User Management tab > Add) in the MARS GUI are dimmed. These fields are also dimmed if you chose not to allow saving of Security Manager login credentials while MARS authenticates with Security Manager.
- If you selected the option to use the Security Manager login credentials for MARS to authenticate with Security Manager and chose to allow the login credentials to be saved in the login dialog box, the username and password fields under the Cisco Security Manager section of the User Configuration Page are activated and can be edited by MARS users with Admin or Security Analyst roles.
- If you saved Security Manager login credentials in the Cisco Security Manager section of the User Configuration page and later logged in to MARS using an account with full read/write privileges to modify the cross-launch authentication settings by deselecting the Allow Users to Save Credentials check box in the Reporting Applications tab, the username and password entries in the Cisco Security Manager section of the User Configuration page are deleted. However, if you perform the same task using an Operator or Notifications Only user role, the Security Manager username and password details are not deleted from the User Configuration page, but can only be viewed.
- If you logged in to Security Manager using a user account that is different from the one that is being used to start Security Manager from MARS for the policy table lookup and you selected the option to use Security Manager credentials, a new instance of the Security Manager client is started even if a client session is active.
- If you log in to MARS using an account that is not defined in the Common Services 3.1 UI and selects the option to use MARS credentials in the Reporting Applications tab, you are prompted to enter the user credentials that is configured in Common Services during policy table lookup.

Client/Instance Issues

- If a Security Manager client session is not open at the time you perform policy lookup, you are not logged out from the Security Manager instance (opened for the purpose of policy lookup) when the idle timeout period is exceeded or when you log out of the MARS session. The Security Manager session closes only when you log out from it or when the idle timeout configured for it is exceeded.

- If the Security Manager client is not installed on the system from which you are accessing the MARS web interface, you are prompted to install the Security Manager client during policy lookup and the page to download the client software is opened.
- If an instance of the Security Manager client is already running, the existing session is reused by MARS to display the policy lookup table for editing access rules or signatures.
- If the Security Manager client session has timed out or an instance is not active, a new instance of the Security Manager client is started to query the policy table for matching rules and signatures.
- If a new instance of the Security Manager client is started during policy table lookup, the time taken to display the matching rules might be slightly greater than the time consumed when a Security Manager client session is active.

Workflow Issues

- If an instance of the Security Manager client is not running and either Workflow or non-Workflow mode is enabled in Security Manager, MARS performs the lookup query on the policies committed to the Security Manager database.
- If Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in the data committed to the Security Manager database.
- If non-Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies in the current login session.

Error Message Issues

- When you run a query for realtime or historical events and try to perform policy lookup from an incident in the query results, occasionally, an error message is displayed in the Policy Query popup window stating that an internal error has occurred. This error is temporary and disappears if you retry this operation after a while. You are prompted to log in again to Security Manager and policy lookup should be successful from then on. An error of this type also occurs when RPC connection fails or when policy changes to the device are not submitted to the Security Manager server.
- Although the Security Manager icon is displayed for events generated by ICMP connection teardown syslogs, an error message is displayed when you perform policy lookup from these events. The error message states that the corresponding connection setup syslog for the teardown syslog could not be found and asks you to try this operation after a few seconds. However, the same error is displayed even if you perform lookup at a later time.
- If the access rule associated with a device is empty in Security Manager, an error message is displayed when you perform the policy lookup query from MARS for a syslog generated by an access rule on that device.
- If you perform the policy table lookup for a device added to MARS only and not to Security Manager, an error message is displayed in the read-only policy table window. Make sure that you add the device to Security Manager and discover the policies so that the configuration on the device is synchronized with Security Manager.
- An error can occur with the policy query if a device configuration is discovered using Security Manager but it is not submitted in Security Manager. The following error message is an example of this issue:

```
<190>2312080: *May 9 23:50:02.199: %SEC-6-IPACCESSLOGDP: list permit-all permitted
icmp 10.2.3.8 ->
10.4.21.2 (0/0), 1 packet
An error occurred while querying policies from Cisco Security Manager. Reason: Failed
to retrieve policy
```

```
information from CSM. Reason: Cisco Security Manager Internal error: Failed to get
interfaces in the device!
The device LC2DTM was discovered by CSM without any errors.
```

Before you perform policy queries, verify that all discovered devices have been submitted in Security Manager.

- If no access rule is configured on the lower security interface in the “in” direction of the device for inbound traffic or if the access rule specified in the syslog is not available on the device, an error message is displayed during policy lookup. When you click the Security Manager icon for syslogs associated with such access rules, a message states that a matching rule cannot be found. You are prompted to make sure that the device is added to Security Manager and access rules are configured on it.
- When you click the Security Manager icon for an event triggered by management traffic, an error message is displayed stating that the selected event was not subjected to access rule matches. You are prompted to select another event and retry policy lookup.
- If an event is generated by a connection teardown syslog and the setup and teardown of the connection occur in two different sessions (with a gap of 2 minutes in-between), the corresponding connection establishment syslog is not sent by MARS to Security Manager when you perform policy lookup for such events. As a result, an error message is displayed stating that the connection setup syslog is not available to display the matching rules for that event. An identical error message is also displayed if you attempt to query access rules for a connection teardown event from the realtime event viewer of MARS.
- When you click the Security Manager icon for an event that contains a syslog ID that is not supported for policy lookup, you are prompted to select another supported event. Although the Security Manager icon is displayed in the MARS GUI only for those events that support policy lookup, you might see this error message while looking up policies for events generated by management traffic or connection teardown syslogs without a corresponding setup syslog.
- An error message is displayed stating that the syslog is invalid even when you click the Security Manager icon for one of the syslogs supported for policy lookup. This problem occurs if the syslog is not parsed by Security Manager and the syslog format received from MARS is incorrect.
- When you perform lookup for an event generated by outbound traffic setup/teardown syslog with an access rule configured on the higher security interface in the “in” direction, an error message is displayed stating that an implicit permit statement is present in the access rule. Also, this error message occurs if a firewall device is added to Security Manager and the changes are not submitted to the database at the time of performing policy lookup from MARS.
- If the device for which you perform access rule lookup has been added to Security Manager without submitting the configuration to the database or if the access rule that generated the syslog is not available on the device, an error message is displayed stating that the access rules on the device is not in synchronization with the one configured in Security Manager.
- For inbound traffic, when an event is generated by an access rule present on the lower security interface in the “in” direction and no matching rule found in Security Manager during policy lookup, an error message is displayed stating that the access rules on the device and in Security Manager are not synchronized. This error is also displayed when a matching policy cannot be found for access rules present on the higher security interface in the “in” direction or on the lower security interface in the “out” direction for outbound traffic.
- When you try to lookup a signature policy from an IPS event in MARS, an error message is displayed if invalid event details are passed from MARS to Security Manager.
- If the signature that generated an event in MARS is deleted or modified on the device, an error is displayed stating that the signature is not found when you perform policy lookup for such an event.

Checklist for Policy Table Lookup from MARS

You can use the following checklist to track the tasks required to integrate MARS with a Security Manager server and the reporting and mitigation devices managed by that Security Manager server. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1 Identify devices that need to be managed by both Security Manager and MARS.

The first step in integrating MARS and Security Manager involves identifying those devices for which Security Manager is used to define policy rules. You must ensure that devices are running a software version supported by both MARS and Security Manager.

For more information, see [Devices and OS Versions Supported by Both Security Manager and MARS, page 11-15](#)

Step 2 Identify and enable all required traffic flows between the devices and MARS.

After you identify the devices to be managed by the Security Manager server and monitored by MARS, you must verify that the network services they use for management, reporting, and notification are permitted along the required traffic flows. Ensure that the management, logging, and notification traffic between the MARS Appliance and each monitored device is allowed by intermediate gateways.



Tip

It is a recommended security practice to have all devices, including MARS Appliances, synchronized to the same time.

For more information, see See the section “Required Traffic Flows” in of the “[Deployment Planning Guidelines](#)” chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*.

Step 3 Prepare the devices to be managed by Security Manager.

Before you can manage devices using Security Manager, you must set up the devices with a minimum configuration that provides basic connectivity. To enable communication between Security Manager and devices, you must configure transport settings on the devices, before you add them to the inventory. Bootstrapping involves getting the device up and running on the network, assigning it an IP address, and connecting it to the physical media.

For more information, see See the [Preparing Devices for Management](#) section of the *User Guide for Cisco Security Manager 3.2*.

Step 4 Add the devices to Security Manager.

For more information, see See the [Managing the Device Inventory](#) section of the *User Guide for Cisco Security Manager 3.2*.

Step 5 Bootstrap the devices managed by MARS.

After you identify the devices managed by the Security Manager server and to be monitored by MARS, you must prepare, or bootstrap, that device to ensure that the MARS Appliance can receive or pull any necessary logs from those devices. After you identify and bootstrap the devices and enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices.

For more information, see For more information on adding and activating devices, see the [Configuring Reporting and Mitigation Devices in MARS](#) in the [Device Configuration Guide for Cisco Security MARS, Release 6.x](#).

Step 6 Add the devices to MARS.

For more information, see [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).

Step 7 Bootstrap each Security Manager server and add it to the correct MARS Local Controller.

For more information, see [Bootstrapping Security Manager Server to Communicate with MARS, page 11-16](#)

Step 8 Perform policy lookups as required.

Once an event generated by one of the Security Manager-managed devices is received by MARS, you can perform a policy lookup operation and modify the possible policies that could have affected the generation of that event from the Security Manager server. For more information on how to perform policy table lookup for events generated by access rules and signatures, see the following sections:

For more information, see the following references:

1. [Navigating to Access Rule Policy in Security Manager from MARS, page 11-24](#)
2. [Navigating to IPS Signature Policy in Security Manager from MARS, page 11-28](#)

Devices and OS Versions Supported by Both Security Manager and MARS

You must ensure that devices that need to be monitored by MARS and managed by Security Manager are running a software versions supported by both MARS and Security Manager to perform the policy table lookup from MARS syslogs and events lookup from Security Manager policies.

[Table 11-1 on page 11-15](#) lists the software versions for each device platform supported by both Security Manager and MARS.

Table 11-1 Supported Devices and OS Versions for Security Manager and MARS Integration

Device Platform	Device OS Version
Cisco IOS Routers	12.x and later
PIX Security Appliances	6.0, 6.1, 6.2, 6.3, 7.0, 7.2, 7.2.1
Adaptive Security Appliances (ASA)	7.0.1, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 8.0, 8.0.3, 8.1, 8.2, 8.2.1, 8.2.2
Cisco Intrusion Prevention System (IPS), IDSM-2 module	5.1, 6.0, 6.0.1, 6.0.2, 6.0.3
Cisco IOS Intrusion Prevention System (IOS IPS) sensors	Cisco IOS 12.3(14)T4, 12.4M, 12.4(2)T, 12.4(4)T, 12.4(11)T2
Cisco Catalyst 6500 Series Switches	Cisco IOS 12.2 and later
Firewall Services Module (FWSM)	1.1, 1.2, 2.3, 3.1, 3.1.3, 3.1.5 ¹

1. FWSM support is supported only in Security Manager Enterprise Edition (Professional-50) and higher. The professional version includes support for the management of Cisco Catalyst 6500 Series switches and associated service modules; the Standard versions do not include this support.

**Note**

For a complete list of devices and OS versions supported by Security Manager and MARS separately, see the Supported Devices and Software Versions document of the respective applications. For MARS, see [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#).

Bootstrapping Security Manager Server to Communicate with MARS

To prepare the Security Manager server to be queried by MARS, you must configure the following settings:

- If you are using AAA authentication, such as Cisco Secure ACS, on the Common Services 3.1 server, you must update the administrative access settings to ensure that the MARS Appliance has the necessary access to the Security Manager server.
- Define a user account in Security Manager that MARS can use to perform queries. A separate account is recommended to provide a cleaner audit trail on the Security Manager server. You must create a user account with one of the following roles defined in Common Services 3.1 to be able to perform the policy table lookup query and modify the highlighted policy by starting Security Manager from the read-only popup window:
 - Approver
 - Network Operator
 - Network Administrator
 - System Administrator

**Note**

Any of the predefined Cisco Secure ACS roles with the exception of the Help Desk role can modify matching policies by starting Security Manager from the read-only policy lookup table. Users with the Help Desk security level can only view the read-only policy lookup table. An error message is displayed when a user with a Help Desk role attempts to start Security Manager to modify a policy from the read-only popup window in MARS.

When you add a Security Manager server to MARS, if you choose to use the option to prompt users for Security Manager credentials for the policy table lookup, you might not need to create a separate MARS user account in the Common Services 3.1 UI for authentication purposes.

For more information on adding users and associating roles with them from the Common Services 3.1 UI, see *User Guide for CiscoWorks Common Services 3.1*.

Adding a Security Manager Server to MARS GC

The Security Manager server is represented in MARS by defining a host with a software application residing on that host. The Security Manager server that you add to the Global Controller can be used to perform policy lookup only for those devices that it manages and that publish their events to MARS.

While a MARS LC can manage only a limited number of devices, Security Manager does not have any such limitation and can manage several multiples of the devices that an LC can. To enable complete coverage of MARS and CSM bidirectional linkage for all the devices in a network, Cisco supported multiple LC addition to Security Manager in earlier versions of the linkage. Now that you are able to add a GC to the CSM, so that all the devices managed by all the LCs monitored by the GC are automatically accessible to CSM.

Before You Begin

- Ensure that the Security Manager server is running version 3.2 or greater.
- You must be logged in to the MARS Global Controller as a user with an Admin role.

To identify a Security Manager server to use for policy lookups from within the web interface of MARS, follow these steps:

Step 1 Select **Admin > Security and Monitor Devices** and then click **Add**.

Figure 11-1 Add Device Selection Window

The screenshot shows the 'Add Device Selection Window' in the Cisco MARS web interface. The window has a header with the Cisco logo and a status bar showing the date and time (Aug 12, 2008 7:24:02 AM PDT) and the user login (Global: Administrator (pnadmin)). Below the header, there are two radio buttons: 'Add Device to Zone:' and 'Add Cisco Security Manager to Zone(s)'. The 'Add Cisco Security Manager to Zone(s)' option is selected. To the right of the radio buttons is a 'Select' dropdown menu. Below the radio buttons are 'Add' and 'Edit' buttons. A table is displayed with the following columns: 'CSM Device Name', 'Access IP', and 'Managing Zones'. The table contains two rows: one for '192.168.10.21' with 'zone99' and one for 'csm' with 'zone84'. Below the table, it says 'No active zones are available for adding CSM.' At the bottom, there is a copyright notice: 'Copyright © 2003-2008 Cisco Systems, Inc. All rights reserved.'

CSM Device Name	Access IP	Managing Zones
☐ 192.168.10.21	192.168.10.21	zone99
☐ csm	192.168.10.21	zone84

The window shown in [Figure 11-1](#) appears.

Step 2 Select **Add Cisco Security Manager to Zone(s)**. The existing Security Managers are displayed, together with the LCs or the zones in which each Security Manager is managed.

Step 3 Select a Security Manager and click **Edit**.

Figure 11-2 Cisco Security Manager Specification Page

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. System account is used by CS-MARS for testing connectivity to CSM, obtaining management information from CSM required for the linkage.
3. Cross-launch authentication settings applies to all CS-MARS users who cross-launch CSM.

3. * denotes a required field.

Cisco Security Manager

Host Details

* Device Name:

Access IP:

Reporting IP:

System Account

* User Name:

* Password:

* Access Type:

* Access Port: (Default: 443)

Cross-Launch Authentication Settings

☐ Use MARS Credentials

☒ Prompt User

☐ Allow Users to Save Credentials

Select Zones

- ☐ Zone11
- ☐ Zone12
- ☐ Zone13
- ☐ Zone14
- ☐ Zone15
- ☐ Zone16
- ☐ Zone17

Select All Deselect All

Submit

Copyright © 2003-2007 Cisco Systems, Inc.
All rights reserved.

Step 4 Specify Host Details in following fields:

- **Device Name**—Enter the name of the host (Security Manager server). This name is used for display purposes only in the MARS GUI and you can assign any meaningful name.
- **Access IP**—(Optional) This address is used to discover settings and pull query data from a Security Manager server using HTTPS. This address represents the physical IP address of the Security Manager server.
- **Reporting IP**—(Optional) Enter the same IP address of the Security Manager server interface as the one entered in the Access IP field. This address also represents the physical IP address of the Security Manager server.

Step 5 Specify System Account access credentials in following fields:

- User Name
- Password

Step 6 The Access Type identifies the protocol used to discover configuration information. Select HTTPS (default) from the list.**Step 7** Select the Access Port. The Access Port identifies the port that MARS uses to communicate with Security Manager. The default access port for HTTPS is port 443.**Step 8** Optionally, you can select the Cross-launch Authentication Setting to be applied to the Local Controller(s) to which the Security Manager is to be added. Select **Apply Settings** and choose between:

- **Use MARS Credentials**—Click this radio button if you want to use the MARS login credentials to contact Security Manager for the policy table lookup. The MARS user account must have been added to the Local User Setup page in the Common Services UI with a role other than Help Desk to navigate successfully to the Security Manager policy table and modify the matching rules. This option is useful when MARS and Security Manager use a common, external server for authentication and authorization such as Cisco Secure ACS.
- **Prompt User**—Click this radio button if you want to prompt the user to enter the credentials to log in to Security Manager to cross-launch the policy lookup table from MARS. The Security Manager login dialog box is displayed when you click the Security Manager icon to view the read-only policy lookup table.

When you select the Prompt User option, the **Allow Users to Save Credentials** check box, beneath it, is enabled. Select this check box if you want the Save Credentials check box in the Security Manager login dialog box to be enabled when you cross-launch the policy lookup table. Selecting the Save Credentials check box causes the Security Manager credentials to be saved in the MARS database and you are not prompted for access details during subsequent lookups.

If you deselect the **Allow Users to Save Credentials** check box, the Save Credentials check box is disabled in the login dialog box, prompting you to enter the login details each time you start the Security Manager policy table from MARS in a new session or after the timeout period. When the Allow Users to Save Credentials check box is deselected, the Security Manager credentials saved in the MARS database are deleted.

Step 9 (Optional) Click **Test Connectivity** to verify that the settings are correct and that MARS can communicate with this Security Manager server.

If the username and password are correct and MARS is configured as an administrative host for the device, a popup window appears with a “Connectivity successful.” message when the discovery operation is successfully completed. Otherwise, an error message appears asking you to click the View Error link for more information about the probable cause and its possible solution.

Step 10 The right panel lists all the LCs or zones monitored by the GC. Select the zones to which the CSM specified in the left section is to be added.

Step 11 Click **Submit**.

The Security Manager is added to the selected LCs, and the Status Summary page of the addition of CSM to MARS is displayed.

Global Controller: brn-te-g2-011 v5.3 Login: Global: Administrator (pnadmin) :: Close

Status Summary

Cisco Security Manager

Device Name: CSM_Zone11_12_21
Access IP: 192.168.10.216

Zone Name	Zone Address	Version	Description	Status
ZONE21	10.1.3.21	5.3.2	10.1.3.21	Successfully added CSM to zone. Test Connectivity is successful.
zone11	10.1.3.11	5.3.2	zone11	Successfully added CSM to zone. Test Connectivity failed.
zone12	10.1.3.21	5.3.2	10.1.3.21	Failed to add CSM to zone.

OK Retry

25128

The Status Summary page lists the details of the CSM and the status of addition to each LC. Legends of red, amber and green are used to highlight statuses:

- **Red**—failure in adding the Security Manager to the zone.
- **Amber**—failure to establish connectivity with the Security Manager.
- **Green**—successful addition and connectivity test.

In case of failure, a checkbox is provided for each of the failed LCs, to retry the addition.

Adding a Security Manager Server to MARS LC

The Security Manager server is represented in MARS by defining a host with a software application residing on that host. The Security Manager server that you add to the Local Controller can be used to perform policy lookup only for those devices that it manages and that publish their events to MARS.

Each Local Controller can query one Security Manager server only; you cannot define more than one Security Manager server per Local Controller. You can define the same Security Manager server on multiple Local Controllers. When planning the zones for Global Controller/multi-Local Controller deployments, ensure that each Local Controller maps to the Security Manager server that manages the reporting devices monitored by that Local Controller. For the procedure to add a Security Manager to a Global Controller, see [Adding a Security Manager Server to MARS GC, page 11-16](#).

If a Security Manager server is not added to MARS, the username and password fields in the Cisco Security Manager section of the User Configuration page are disabled. A message appears in the User Configuration page that the Security Manager credentials for policy table cross-launch cannot be saved in the MARS database because a Security Manager server is not yet added to MARS.

Before You Begin

- Make sure that the Security Manager server is running version 3.2 if you want to look up the policy table and modify matching rules or signatures. If you add a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance running 4.3.2 through 4.3.4 or 5.3.2 through 5.3.4, you can query for policies in view mode only; you must open a Security Manager client instance separately to modify the policies.

Adding a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance provides the same behavior that existed in versions of MARS earlier than 4.3.4 and 5.3.4 to perform policy lookup.

- You must be logged in to the MARS Local Controller as a user with an Admin role.

To identify a Security Manager server to use for policy lookups from within the web interface of MARS, follow these steps:

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](#). See [Figure 11-3](#).
- 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 6](#).

Figure 11-3 Device Discovery-Add SW Security Apps on New Host

You can select the Add SW Security apps on an existing host option 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 Specify values for the following fields:

- **Device Name**—Enter the name of the host (Security Manager server). This name is used for display purposes only in the MARS GUI and you can assign any meaningful name.
- **Access IP**—This address is used to discover settings and pull query data from a Security Manager server using HTTPS. This address represents the physical IP address of the Security Manager server.
- **Reporting IP**—(Optional) Enter the same IP address of the Security Manager server interface as the one entered in the Access IP field. This address also represents the physical IP address of the Security Manager server.
- **Operating System**—(Optional) Specify the operating system type by selecting **Windows** or **Generic** from the drop-down list.



Note

To pull event logs from Windows 2003 or Windows 2008, click **Logging Info**, select **Pull**, enter the account credentials, and then click **Submit**.

Step 4 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface in the Security Manager server from which configuration information will be queried.

Step 5 Click **Apply** to save these settings.

Step 6 Click **Next** to access the Reporting Applications tab.

- Step 7** Select the **Cisco Security Manager ANY** from the Select Application list, and click **Add**. See [Figure 11-4](#).

Figure 11-4 *Device Discovery-Cisco Security Manager ANY Page*

[bm-te-g1-014] Device Discovery-Cisco Security Manager ANY - Microsoft Internet Explorer provided by Cisco Systems, Inc.

CISCO

Feb 19, 2008 12:56:54 PM PST
Standalone: bm-te-g1-014 v4.3 Login: Administrator (pnadmin) :: Close

Cisco Security Manager ANY

Note:
1. System account is used by CS-MARS for testing connectivity to CSM, obtaining management information from CSM required for the linkage.
2. Cross-launch authentication settings applies to all CS-MARS users who cross-launch CSM.
3. * denotes a required field.

System Account

→ *User Name: admin

→ *Password: *****

→ *Access Type: HTTPS

→ *Access Port: 443 (Default: 443)

Cross-Launch Authentication Settings

☐ Use MARS Credentials

☒ Prompt User

☒ Allow Users to Save Credentials

Test Connectivity Cancel Submit

- Step 8** If you entered an address in the Access IP field on the host that represents this Security Manager server, specify values for the following fields:
- **User Name**—Identifies the Cisco Security Manager administrative account to be used to discover configuration settings.
 - **Password**—Identifies the password associated with the username account.
 - **Access Type**—Identifies the protocol used to discover configuration information. Select HTTPS from the drop-down list.
 - **Access Port**—Identifies the port that MARS uses to communicate with Security Manager. The default access port for HTTPS is port 443.
- Step 9** Under Cross-Launch Authentication Settings, do one of the following:
- Click the **Use MARS Credentials** radio button if you want to use the MARS login credentials to contact Security Manager for the policy table lookup. The MARS user account must have been previously added to the Local User Setup page in the Common Services UI with a role other than Help Desk to navigate successfully to the Security Manager policy table and modify the matching rules. This option is useful when MARS and Security Manager use a common, external server for authentication and authorization such as Cisco Secure ACS.

- Click the **Prompt User** radio button if you want to prompt the user to enter the credentials to log in to Security Manager to cross-launch the policy lookup table from MARS. The Security Manager login dialog box is displayed when you click the Security Manager icon to view the read-only policy lookup table. When you select the Prompt User option, you can choose to allow the Security Manager credentials to be saved or not.

When you click this radio button, the **Allow Users to Save Credentials** check box, beneath it, is enabled. Select this check box if you want the Save Credentials check box in the Security Manager login dialog box to be enabled when you cross-launch the policy lookup table. Selecting the Save Credentials check box causes the Security Manager credentials to be saved in the MARS database and you are not prompted for access details during subsequent lookups.

If you deselect the **Allow Users to Save Credentials** check box, the Save Credentials check box is disabled in the login dialog box, prompting you to enter the login details each time you start the Security Manager policy table from MARS in a new session or after the timeout period. When the Allow Users to Save Credentials check box is deselected, the Security Manager credentials saved in the MARS database are deleted.

**Note**

Login credentials are cached by MARS when you successfully log in to Security Manager. These credentials are discarded when you exit MARS or the idle session timeout period is exceeded.

If the Allow Users to Save Credentials check box is deselected, the username and password fields in the Cisco Security Manager section of the User Configuration page are disabled. A message appears in the User Configuration page that the Security Manager credentials to perform policy lookup cannot be saved in the MARS database because the Allow Users to Save Credentials check box is deselected. The message appears in the User Configuration page even when you choose to use MARS credentials for policy table lookup.

- Step 10** (Optional) Click **Test Connectivity** to verify that the settings are correct and that the MARS Appliance can communicate with this Security Manager server.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, a popup window appears with a “Connectivity successful.” message when the discovery operation is successfully completed. Otherwise, an error message appears asking you to click the View Error link for more information about the probable cause and its possible solution.

- 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**.

After the MARS Appliance is activated, it can query the Security Manager server to perform policy lookups.

Navigating to Access Rule Policy in Security Manager from MARS

Access rules filter network traffic by controlling whether routed packets are forwarded or blocked at the firewall's interfaces. Rules are processed by a device from first to last, or first-match basis, against each received packet. After you configure and deploy access rules from Security Manager to a device and enable logging on the device monitored by MARS, a log entry is created when an access rule matches the network traffic that the device is processing and the action defined in the rule is used to decide if traffic needs to be permitted. An incident is generated in MARS after the log associated with an access rule is received from the device.

In MARS, an incident is a chain of events that are correlated by a rule to signal an attack on your network. MARS simplifies and expedites the detection, mitigation, reporting, and analysis of the incident. The Network Summary dashboard, the Query Results pages, and the Incident pages help to detect recent incidents and show the rules and the events that compose them.

Using MARS, you can also navigate from messages that are generated during the establishment or tearing down of a TCP, UDP, or ICMP connection to the permit ACE in Security Manager for that specific syslog. You can then edit the access rule generating the MARS event or incident to update the action the device must take in response to a receiving packet.

Before You Begin

- Make sure you have performed all the tasks in the [Checklist for Policy Table Lookup from MARS, page 11-14](#).
- Make sure that Security Manager can be reached from MARS.
- In the Query Reports page, the following result formats are supported for access rule lookup:
 - All Matching Events.
 - All Matching Event Raw Messages.
 - All Matching Sessions.
 - All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).

To look up and modify the access rule in the policy table of Security Manager from an incident in MARS, follow these steps:

-
- Step 1** Log in to the MARS. The Dashboard page is displayed with the Summary tab selected.
- If you selected the authentication option to use MARS credentials for policy lookup, log in as an Administrator or Security Analyst to be able to modify the matched access rules. If you selected the option to use Security Manager credentials for policy lookup, the MARS login user role does not matter.
- Step 2** Identify the incident or event to investigate from the Query Results page or the Incident Details page.
- To navigate to the Query Results page, run a query to return events matching the specified query criteria. For example, if you run a query to return events ranked by time with the most current first from the Query/Reports tab, the Query Results page appears as shown in [Figure 11-8](#). Click the Security Manager icon in the Reporting Device column from the query results.
 - To navigate to the Incident Details page (see [Figure 11-9](#)), do one of the following:
 - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.

- From the Recent Incidents section of the Dashboard (see [Figure 11-10](#)), click the link in the Incident ID column.
- Click the Incidents tab to navigate to the Incidents page (see [Figure 11-11](#)), which displays recent incidents, and click the link in the Incident ID column.
- Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Step 3 Click the Security Manager icon in the Reporting Device field to invoke the Security Manager policy table lookup.

If you selected the option to be prompted for credentials to log in to Security Manager for policy table lookup, a login dialog box is displayed. Otherwise, [one of three popup windows](#) is displayed.

Step 4 Enter the Security Manager login credentials and click **OK**.

You are prompted for credentials the first time you start a new MARS session. These credentials are cached until the session expires or you open a fresh session.



Note

This dialog box is not displayed if you chose to use MARS credentials for logging in to Security Manager, or selected the check box to save Security Manager credentials when you performed the policy table lookup earlier.

If you access the MARS GUI using Internet Explorer, it is possible that the password is automatically entered in the login dialog box after you enter the username. This behavior occurs if you configured your browser to remember passwords. See the “Interoperation of MARS and Security Manager” chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2* for information on how cached passwords can be cleared or the caching feature can be disabled.

One of the following three popup windows may appear:

- Multiple Events window—Lists all reporting device events in the session, this window appears in this step when there are two or more events in the session. See [Figure 11-5](#). Go to [Step 5](#).
- Multiple Devices window—Lists all matching reporting devices that meet criteria available to MARS. This window appears when there are two or more matching devices. See [Figure 11-6](#). Go to [Step 6](#).
- Policy Table window—Lists the policy table of the reporting device. Access rules that match the MARS criteria are highlighted, this window appears in this step when there is one event and a unique reporting device identified. See [Figure 11-7](#). For a detailed description of how to work with the policy table popup window, see [Examining and Editing Highlighted Rules](#). For a description of the elements in the Policy Query window, see [Read-Only Security Manager Policy Lookup Page for Access Rules](#), page 11-35.

Figure 11-5 MARS Multiple Events Pop-up Window

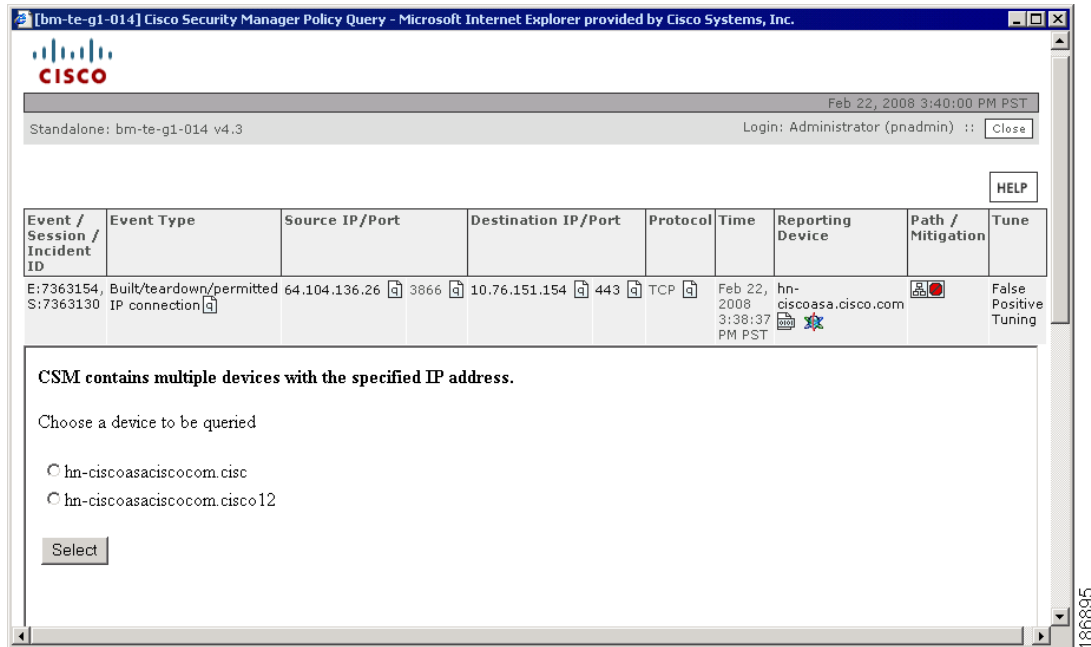


Figure 11-6 MARS Multiple Devices Pop-up Window

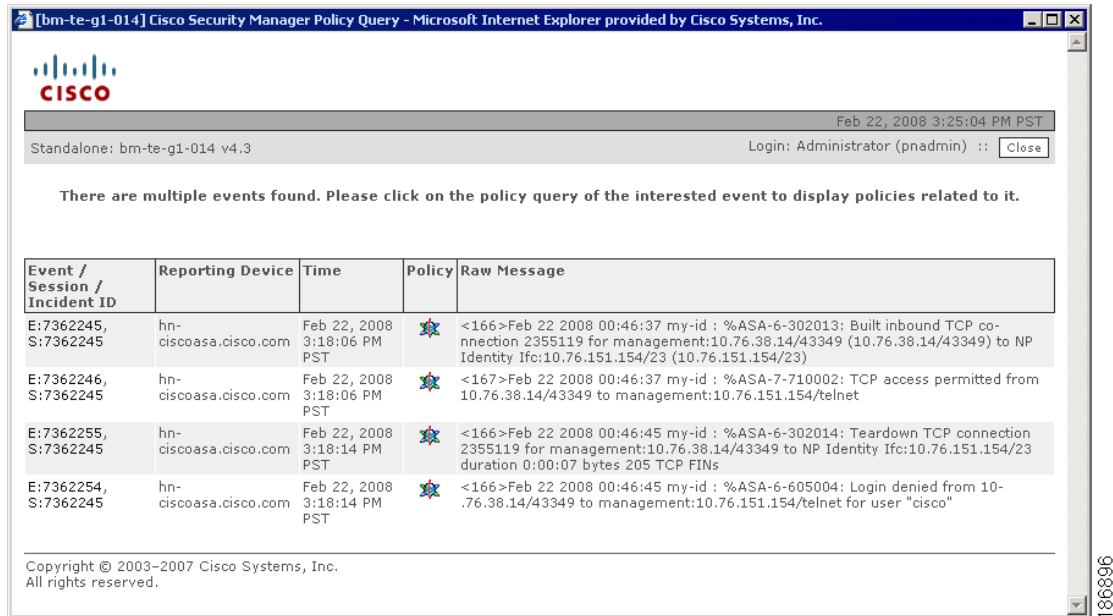


Figure 11-7 Read-Only Access Rule Table Pop-up Window

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:7362088, S:7362088	Built/Teardown ICMP connection	10.76.38.33 0	10.76.151.154 0	ICMP	Feb 22, 2008 3:16:37 PM PST	hn-ciscoasa.cisco.com		False Positive Tuning

Found 5 matches in about 4693 rules. Go to matched rule Local 1

Edit	Permit	Source	Destination	Service	Interface	Dir.	Option	Category	Description
Local (4692 Rules)									
1	✓	any	any	ICMP	outside	out	Alert/1	None	test
2	✓	bar	2.2.2.2	Telnet	outside	out	Warning/300	None	
3	✓	any	any	UDP	outside	out	Alert/1	None	
4	✓	any	any	TCP	outside	out	Alert/1	None	
5	✓	any	any	IP	outside	out	Informational/300	None	
6	✓	bar	200.200.200.200	IP	outside	in		None	
7	✓	1.1.1.2	200.200.200.200	IP	outside	in		None	
8	✓	1.1.1.3	200.200.200.200	IP	outside	in		None	
9	✓	1.1.1.4	200.200.200.200	IP	outside	in		None	
10	✓	1.1.1.5	200.200.200.200	IP	outside	in		None	
11	✓	1.1.1.6	200.200.200.200	IP	outside	in		None	
12	✓	1.1.1.7	200.200.200.200	IP	outside	in		None	
13	✓	1.1.1.8	200.200.200.200	IP	outside	in		None	

- Step 5** (Optional) If the Multiple Events window is displayed, click the Security Manager icon in the Policy field of the appropriate event. One of the following two popup windows may appear:
- Multiple Devices window. Go to [Step 6](#).
 - Policy Table window. For a detailed description of how to work with the policy table popup window, see [Examining and Editing Highlighted Rules](#). For a description of the elements in the Policy Query window, see [Read-Only Security Manager Policy Lookup Page for Access Rules, page 11-35](#).
- Step 6** (Optional) If the Multiple Devices popup window is displayed, click the radio button next to the appropriate reporting device. Click **Select**. The read-only access rule table popup window appears for the selected device.

The access rules that match the MARS query criteria are highlighted. The access rules displayed in the read-only policy table window depend on whether an instance of the Security Manager client is running and whether Workflow or non-Workflow mode is enabled. For more information, see Task 6 in the [Taskflow for Policy Table Query from MARS Events, page 11-2](#).

If there are more rules in the access rule table than can displayed in a single page, they are displayed across several pages and you can navigate back and forth. Pagination allows you to display a maximum number of items per page. Additional items carry over to the next page. You choose the number of items to display per page from the Rows per page drop-down list. Select a value from the Go to page drop-down list to navigate to the page number you desire, and click **Prev** or **Next** to navigate between pages.

To switch between matched rules, click **Prev** or **Next**, as required, beside the Go to matched policy drop-down list for each highlighted access rule. Select the first or last rule number from the Go to matched policy list to navigate to the first or last highlighted access rule. If multiple access rules match the query criteria, the first matching rule is highlighted, regardless of whether the page in which the match is found is the first page of the access rule table or not.

If an access rule contains network/host, interface, or service objects, you can click the object in the read-only policy lookup table to view the definitions of these objects in a popup window.

Step 7 Click the hyperlink in the rule number under the No. column for a highlighted access rule.



Note If an instance of the Security Manager client is running, the same instance is reused for the policy table lookup. If the Security Manager client session has timed out or is not open, a new client session is started. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.



Note When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box appears prompting you to confirm whether you want to download the CsmContentProvider file to your system. This dialog box appears because of security settings in Internet Explorer. To cause the Open button to be displayed in this dialog box during policy lookup, see the “Interoperation of MARS and Security Manager” chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2*.

The Security Manager client window is activated and the Access Rules page appears with the access rule that generated the event highlighted in the policy table. You can modify the access rule to control the flow of network packets and deploy the updated policy to the device to refine network protection.

If the highlighted access rule contains network/host, service, or interface objects, right-click the appropriate table cell of the rule in the Access Rules page and select **Show <object> Contents** from the shortcut menu to view the list of flattened values of the object.

Step 8 Click **Transcript Details** at the bottom of the read-only access rule table to open a popup window that displays information about the raw syslog for the event that you selected in MARS and the parsed format of the syslog after it is processed by Security Manager to find access rules that generated the syslog. These details enable you to understand the taskflow of the access rule lookup query and are informational messages, which can be used to troubleshoot errors.

Step 9 Click the **CS Manager Details** link at the bottom of the page to open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved. Click the Close icon to close the dialog box.

Navigating to IPS Signature Policy in Security Manager from MARS

Sensors scan network packets using signatures to detect attacks or other misuses of network resources. When the sensor finds a match for an incoming packet with the signature, it takes some action, such as logging the event. If the signatures are configured on the sensor using Security Manager and the sensor is monitored by MARS, the sensor publishes the logs to MARS. From the Query page, you can define

the query parameters and run a query to return events or incidents generated by signatures configured on the sensor. You can click the Security Manager icon from the returned events, or raw messages associated with events, to proceed to the policy in Security Manager. Alternatively, you can select a particular incident ID from the returned query results and view the details associated with the incident. From the Incident Details page, you can click the Security Manager icon () in the Reporting Device column for the event that you want to examine.

**Note**

In the Query Reports page, the following result formats are supported for access rule lookup:

All Matching Events.

All Matching Event Raw Messages.

All Matching Sessions.

All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).

A collection of events generated by sensors are also displayed in the Incidents page from which you can select an incident ID and navigate to the signature policy in Security Manager. You can then edit their parameters (tune them) to achieve optimal performance on your network, and particularly to minimize false positives and false negatives.

Before You Begin

- Ensure you have performed all the tasks in the [Checklist for Policy Table Lookup from MARS, page 11-14](#).
- Ensure that Security Manager can be reached from MARS.

To look up and modify an IPS signature in the signature summary table of Security Manager from an incident in MARS, follow these steps:

-
- Step 1** Log in to the MARS. The Dashboard page is displayed with the Summary tab selected.
- If you selected the authentication option to use MARS credentials for policy lookup, log in as an Administrator or Security Analyst to be able to modify the matched access rules. If you selected the option to use Security Manager credentials for policy lookup, the MARS login user role does not matter.
- Step 2** Identify the incident or event to investigate from the Query Results page or the Incident Details page in one of the following ways:
- To navigate to the Query Results page, run a query to return events matching the specified query criteria. For example, if you run a query to return events ranked by time with the most current first from the Query/Reports tab, the Query Results page appears as shown in [Figure 11-8](#). Click the Security Manager icon () in the Reporting Device column from the query results.
 - To navigate to the Incident Details page (see [Figure 11-9](#)), do one of the following:
 - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
 - From the Recent Incidents section of the Dashboard (see [Figure 11-10](#)), click the link in the Incident ID column.

- Click the Incidents tab to navigate to the Incidents page (see [Figure 11-11](#)), which displays recent incidents, and click the link in the Incident ID column.
- Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Figure 11-8 Query Results Page with Matching Events

The screenshot shows the Cisco Security Manager interface in a Microsoft Internet Explorer browser window. The page title is "[bm-te-g1-014] Query Results - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The browser's address bar shows the URL "http://172.20.10.43:8080/". The page has a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the navigation bar, there's a sub-header with "Query", "Batch Query", and "Report" tabs, and a date/time stamp "Feb 21, 2008 3:10:37 PM PST". The main content area shows the "QUERY / REPORTS" section with the text "CS-MARS Standalone: bm-te-g1-014 v4.3" and a login status "Login: Administrator (pnadmin) :: Logout :: Activate". A dropdown menu "Load Report as On-Demand Query..." is visible. Below this, the "Query Event Data" section allows users to click cells to change query criteria. The "Query type" is set to "Events ranked by Time, Real Time(raw events)". A table of query criteria is shown with columns: Source IP, Destination IP, Service, Events, Device, Reported User, Keyword, Operation, Rule, and Action. The table contains one row with values: ANY, ANY, ANY, ANY, ANY, ANY, ANY, None, ANY, ANY. Below the table are buttons: "Save As Report", "Save As Rule", and "Submit". The "Query Results" section displays a table of events with columns: Event ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, and Reporting Device. The table contains seven rows of event data.

Event ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device
6837907	Unknown Device Event Type	64.104.136.253	172.20.10.43	TCP	Feb 21, 2008 3:14:18 PM PST	IPS
6837908	Unknown Device Event Type	172.20.10.43	0.0.0.0	TCP	Feb 21, 2008 3:14:18 PM PST	IPS
6837909	Unknown Device Event Type	64.104.136.253	0.0.0.0	TCP	Feb 21, 2008 3:14:18 PM PST	IPS
6837910	Unknown Device Event Type	172.20.10.43	64.104.136.253	TCP	Feb 21, 2008 3:14:18 PM PST	IPS
6837911	Unknown Device Event Type	64.104.136.253	172.20.10.43	TCP	Feb 21, 2008 3:14:18 PM PST	IPS
6837912	Built/teardown/permitted IP connection	10.1.1.13	172.20.10.239	UDP	Feb 21, 2008 3:14:26 PM PST	MARS-CSM-ASA.cisco.com

Figure 11-9 Incident Details Page

Incident Details - Microsoft Internet Explorer provided by Cisco Systems, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

CISCO

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Incidents False Positives Cases Feb 22, 2008 2:18:32 PM PST

INCIDENTS | CS-MARS Standalone: bm-te-g1-014 v4.3 Login: Administrator (pnadmin) :: Logout :: Activate

Incident ID: 6077943 Show
Session ID: Show

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	(	ANY	SAME, \$TARGET01, ANY	ANY	Probe/HostInfo/All	ANY	None	ANY	ANY	1		FOLLOWED-BY
2		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/ArpPoisoning	ANY	None	ANY	ANY	1	)	OR
3		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/ArpPoisoning	ANY	None	ANY	ANY	1		

Rule Name: System Rule: Misc. Attacks: ARP Poisoning Status: Active
Action: None Time Range: 0h:30m
Description: This correlation rule detects ARP Poisoning attacks preceded by reconnaissance attempts to that host, if any.

Incident ID: 6077943 Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
Instance 1										
3	S:7356445, I:6077943	ARP Reply-to-Broadcast	10.76.151.65 0 0	10.76.151.65 0 0	N/A	Feb 22, 2008 1:58:41 PM PST	10.76.151.44			False Positive Tuning
Instance 2										
3	S:7356446, I:6077943	ARP Reply-to-Broadcast	10.76.151.67 0 0	10.76.151.67 0 0	N/A	Feb 22, 2008 1:58:41 PM PST	10.76.151.44			False Positive Tuning

186893

Figure 11-10 Recent Incidents on MARS Summary Page

The screenshot shows the Cisco MARS Summary Page in a Microsoft Internet Explorer browser window. The page title is "[bm-te-g1-014] Status Summary - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The browser's address bar shows the URL "http://186901:8080/mars/summary". The page has a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The SUMMARY tab is selected. Below the navigation bar, there is a "Page Refresh Rate" dropdown set to "15 minutes". The "Recent Incidents (Last Hour)" section displays a table of incidents. The table has columns: Incident ID, Event Type, Matched Rule, Action, Time, Path, and Cases. The incidents listed are:

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:1215097	ARP Reply-to-Broadcast	System Rule: Misc. Attacks: ARP Poisoning		Feb 19, 2008 12:21:06 PM PST		
I:1215095	Anomaly Detection - External UDP Scanner	System Rule: Scans: Stealth		Feb 19, 2008 12:16:05 PM PST - Feb 19, 2008 12:20:05 PM PST		
I:1215096	PIX user entered a command that modified the config	System Rule: Modify Network Config		Feb 19, 2008 12:15:46 PM PST		
I:1215094	PIX user entered a command that modified the config	System Rule: Modify Network Config		Feb 19, 2008 12:15:30 PM PST		
I:1215093	Anomaly Detection - External UDP Scanner	System Rule: Scans: Stealth		Feb 19, 2008 12:15:04 PM PST		

On the left side of the page, there are several summary statistics:

- Events:** 693,135
- Sessions:** 237,813
- Data Reduction:** 65%
- Incidents:**
 - High: 187 (29%)
 - Medium: 333 (51%)
 - Low: 130 (20%)
 - Total: 650 (100%)
- False Positives:**
 - To be confirmed: 0 (0%)
 - System determined: 0 (0%)
 - Logged: 0 (0%)
 - Dropped: 0 (0%)
 - User confirmed: 0 (0%)
 - Total: 0 (100%)
- To-do List:** No Open Cases
- My Reports:**

Figure 11-11 MARS Incidents Page

The screenshot shows the Cisco MARS Incidents Page in a Microsoft Internet Explorer browser window. The page title is "[bm-te-g1-014] Incidents - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The browser's address bar shows the URL "http://186901:8080/mars/incidents". The page has a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The INCIDENTS tab is selected. Below the navigation bar, there is a "Recent Incidents for Last" dropdown set to "One Hour". The "View" button is visible. The "Incidents" section displays a table of incidents. The table has columns: Incident ID, Event Type, Matched Rule, Action, Time, Path, and Cases. The incidents listed are:

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:1215106	Nachi Worm Spread and DoS via ICMP Ping	System Rule: Worm Propagation - Attempt		Feb 19, 2008 12:40:39 PM PST		
I:1215104	PIX user entered a command that modified the config	System Rule: Modify Network Config		Feb 19, 2008 12:30:10 PM PST - Feb 19, 2008 12:35:30 PM PST		
I:1215102	Nachi Worm Spread and DoS via ICMP Ping	System Rule: Worm Propagation - Attempt		Feb 19, 2008 12:35:24 PM PST		
I:1215103	Anomaly Detection - External UDP Scanner	System Rule: Scans: Stealth		Feb 19, 2008 12:26:07 PM PST - Feb 19, 2008 12:35:09 PM PST		
I:1215105	ARP Reply-to-Broadcast	System Rule: Misc. Attacks: ARP Poisoning		Feb 19, 2008 12:31:36 PM PST - Feb 19, 2008 12:32:08 PM PST		
I:1215099	Anomaly Detection - External UDP Scanner	System Rule: Scans: Stealth		Feb 19, 2008 12:21:06 PM PST - Feb 19, 2008 12:25:03 PM PST		

At the top of the incidents section, there are search filters: "All Severities" (dropdown), "All Rules" (dropdown), and "All Case Statuses" (dropdown). There are also input fields for "Incident ID:" and "Session ID:" with "Show" buttons.

Step 3 Click the Security Manager icon in the Reporting Device field to invoke the Security Manager policy table lookup. If you selected the option to be prompted for credentials to log in to Security Manager for policy table lookup, a login section is displayed in the Policy Query popup window. See [Figure 11-12](#). Go to [Step 4](#).

Otherwise, the Cisco Security Manager Policy Query popup window is displayed with the signature parameters in read-only mode. See [Figure 11-13](#). Go to [Step 5](#). For a description of the elements in the Policy Query window, see [Read-Only Security Manager Policy Lookup Page for an IPS Signature](#), page 11-39.

**Note**

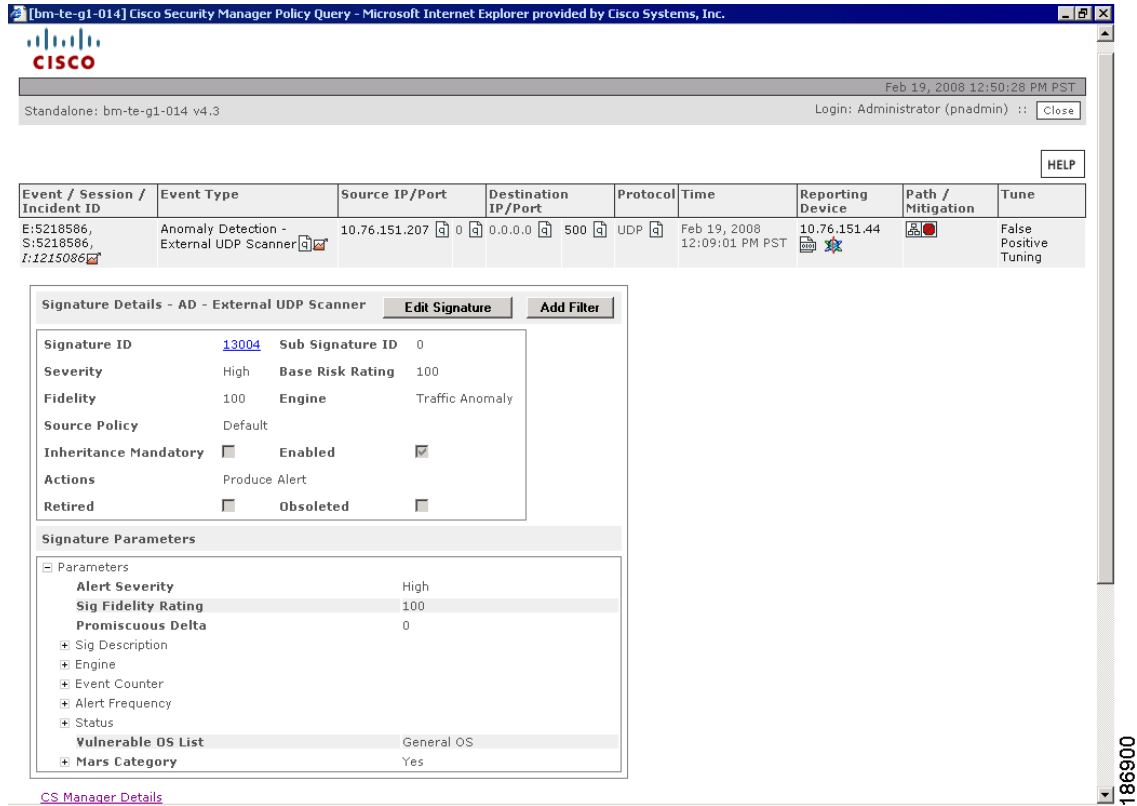
Events triggered by custom signature configured on a sensor are categorized as “Unknown Device Event Type” in the MARS GUI and the Security Manager icon is displayed for these events to enable policy lookup.

Figure 11-12 Read-Only Signature Policy Pop-up Window with Login Section

The screenshot shows the Cisco Security Manager Policy Query window. At the top, it displays the Cisco logo and the title "[bm-te-g1-014] Cisco Security Manager Policy Query - Microsoft Internet Explorer provided by Cisco Systems, Inc.". Below this, there is a status bar showing "Feb 19, 2008 12:43:39 PM PST" and "Standalone: bm-te-g1-014 v4.3". A login section on the right shows "Login: Administrator (pnadmin) :: [Close]". A "HELP" button is also present.

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:5218483, S:5218483, I:1215086	Anomaly Detection - External UDP Scanner	10.76.151.207 0	0.0.0.0 500	UDP	Feb 19, 2008 12:08:01 PM PST	10.76.151.44	[Icon]	False Positive Tuning

Below the table, there is a login section with fields for "*User Name:" and "*Password:", a "Submit" button, and a checkbox for "Save Credentials".

Figure 11-13 Read-Only Signature Policy Pop-up Window with Matching Signature Parameters

Step 4 Enter the Security Manager login credentials and click **OK**. The Cisco Security Manager Policy Query popup window is displayed with the signature parameters in read-only mode. For a description of the elements in the Policy Query window, see [Read-Only Security Manager Policy Lookup Page for an IPS Signature](#), page 11-39.

You are prompted for credentials the first time you start a new MARS session. These credentials are cached until the session expires or you open a fresh session.

**Note**

This dialog box is not displayed if you chose to use MARS credentials for logging in to Security Manager, or selected the check box to save Security Manager credentials when you performed the policy table lookup earlier.

If you access the MARS GUI using Internet Explorer, it is possible that the password is automatically entered in the login dialog box after you enter the username. This behavior occurs if you configured your browser to remember passwords. See the “Interoperation of MARS and Security Manager” chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2* for information on how cached passwords can be cleared or the caching feature can be disabled.

Step 5 Do one of the following:

- Click **Edit Signature** to open the Signatures page in Security Manager. The IPS signature that generated the event is highlighted in the policy table. You can tune the signature parameters to detect network intrusions.

**Note**

If an instance of the Security Manager client is running, the same instance is reused for the policy table lookup. If the Security Manager client session has timed out or is not open, a new client session is started. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.

- Click **Add Filter** to open the Add Event Action Filter dialog box in Security Manager to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. The fields that specify the actions that should be removed from the event, the percentage of packets to deny for deny attacker features, and the port and IP address used by the attacker host are populated with values derived from the event logged in MARS. The remaining fields in the Add Event Action Filter dialog box are displayed with default values. When you save the event action filter, it is stored as a local policy filter for that specific device.
- Click the **CS Manager Details** link at the bottom of the page to open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved. Click the Close icon to close the dialog box.

**Note**

When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box appears prompting you to confirm whether you want to download the CsmContentProvider file to your system. This dialog box appears because of security settings in Internet Explorer. To cause the Open button to be displayed in this dialog box during policy lookup, see the “Interoperation of MARS and Security Manager” chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2*.

Read-Only Security Manager Policy Lookup Page for Access Rules

Use the Cisco Security Manager Policy Query page in the MARS GUI to view the access rule that triggered the incident that you want to examine. This page takes one of the following forms, depending on the number of events and devices that match the incident you are investigating.

- A list of all reporting device events in the session when there are two or more events in the session. Click the Security Manager icon in the Reporting Device field for the event whose access rules you want to lookup. If multiple devices match the MARS query criteria, the page refreshes to display the information as described in the next bullet. If a unique device can be identified for the event, the page assumes the form as described in the third bullet.
- A list all matching reporting devices that meet criteria available to MARS when there are two or more matching devices. A radio button is displayed next to each device to select the device for which you want to lookup access rules. Selecting a device causes the page to display the information as described in the next bullet.
- Access rule table of the reporting device. Access rules that match the MARS criteria are highlighted, this window appears in this step when there is one event and a unique Security Manager device identified.

- An error message if no device matches the MARS query criteria.

Navigation Path

To access the read-only policy lookup page for access rules, do one of the following:

1. From the Query/Reports tab, run a query to return events or raw messages associated with events that meet the query criteria to display the Query Results page. Click the Security Manager icon in the Reporting Device column from the query results.
2. In the MARS GUI, navigate to the Incident Details page in one of the following ways:
 - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
 - From the Recent Incidents section of the Dashboard, click the link in the Incident ID column.
 - Click the Incidents tab to navigate to the Incidents page, which displays recent incidents, and click the link in the Incident ID column.
 - Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Click the Security Manager icon in the Reporting Device field of the Incident Details page for incidents generated by access rules.



Note

Although this page contains elements other than those listed in the field reference table, these elements are read-only or are used to navigate to other pages in MARS. Only the elements with which you can perform actions specific to access rule table lookup are listed in the table.



Note

Even though the Security Manager icon in the event displayed at the top of the page can be clicked, it only refreshes the page with the same contents. You need to click the hyperlink in the rule number of the read-only policy table to navigate to the Access Rules page in the Security Manager client; clicking this icon does not start the Security Manager client.

Field Reference

Table 11-2 Read-Only Access Rule Policy Lookup Page

Element	Description
Cisco Security Manager Login	Available only if you selected the option to prompt the user for Security Manager login credentials for access rule lookup and the Security Manager credentials are neither cached nor saved in the MARS database.
User Name	The username for logging in to Security Manager. Note The user must have administrative privileges to open the Security Manager client from the read-only access rule table. Otherwise, an error message is displayed when you click the hyperlinked rule number from the No. column of the access rule table.

Table 11-2 Read-Only Access Rule Policy Lookup Page (Continued)

Password	The password for logging in to Security Manager.
Submit	Sends the entered credentials to Security Manager and displays the read-only access table in the same page, if authentication is successful.
Save Credentials	Available only if the Allow Users to Save Credentials check box is selected in the Reporting Applications tab of MARS. When selected, Security Manager credentials are saved in the MARS database and reused during policy lookup. You are not prompted for credentials during subsequent policy lookup operations if you select this check box.
Access rule policy table	If the Security Manager Login section is displayed, this table appears after MARS is successfully authenticated with Security Manager. Also, if a unique device and a single event cannot be identified for an incident, this table is displayed after you select the required device and event from the list of multiple devices and multiple events.
Go to matched policy	Select the rule number to which you want to navigate in the table.
Prev	Click to move to the matching access rule previous to the one currently highlighted in the table.
Next	Click to move to the matching access rule next to the one currently highlighted in the table.
No.	Identifies the ordered rule number in the table. Click the hyperlink in the rule number to start the Security Manager client with the current row highlighted the access rule table and modify its settings. Hold your cursor over the rule number to view a tooltip. Note If an instance of the Security Manager client is already open, the same instance is activated.
Source	Identifies the source network object names or addresses of hosts and networks, for example, 10.1.1.1, 10.1.1.1/32, 10.1.1.1/255.255.255.255 and net10. Clickable only if it represents a network object. Clicking the object displays the contents of the object in a popup window. The source IP address or hostname contained in the object is highlighted in the popup window if it matches with the source IP address in the syslog that generated this rule.

Table 11-2 Read-Only Access Rule Policy Lookup Page (Continued)

Destination	Identifies the destination network/host object names or addresses of hosts or networks. Clickable only if it represents a network object. Clicking the object displays the contents of the object in a popup window. The destination IP address or hostname contained in the object is highlighted in the popup window if it matches with the destination IP address in the syslog that generated this rule.
Service	Identifies service objects that specify protocol and port information. Clickable only if it represents a service object. Clicking the object displays the contents of the object in a popup window. The protocol and port contained in the interface object are highlighted in the popup window if they match with the protocol in the syslog that generated this rule. However, this feature of highlighted entries is supported only for TCP-based and UDP-based rules.
Interface	Identifies the logical name of the interface (interface role) or physical interface to which a rule is assigned. Clickable only if it represents an interface object. Clicking the object displays the contents of the object in a popup window. Unlike network/host and service objects, the flattened-out interface objects that match with the interface value in the syslog that generated this rule are not highlighted in the popup window.
Go to page	Select the page number to which you want to navigate. Click Prev and Next on either side of the drop-down list to navigate between pages.
Rows per page	Select the number of rows that you want to be displayed in each page of the access rule table.
Transcript Details	Click to open a dialog box displaying information about the raw syslog for the event that you selected in MARS and the parsed format of the syslog after it is processed by Security Manager to find access rules that generated the syslog. These details enable you to understand the taskflow of the access rule lookup query and are informational messages, which can be used to troubleshoot errors.

Table 11-2 Read-Only Access Rule Policy Lookup Page (Continued)

CS Manager Details	Click open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved.

Read-Only Security Manager Policy Lookup Page for an IPS Signature

Use the Cisco Security Manager Policy Query page in the MARS GUI to view the signature that triggered the incident that you want to examine. From this page, you can open the Security Manager client to edit the signature parameters or define an event action filter to remove specific actions from an event.

Navigation Path

To access the read-only policy lookup page for IPS signatures, do one of the following:

1. From the Query/Reports tab, run a query to return events or raw messages associated with events that meet the query criteria to display the Query Results page. Click the Security Manager icon in the Reporting Device column from the query results.
2. In the MARS GUI, navigate to the Incident Details page in one of the following ways:
 - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
 - From the Recent Incidents section of the Dashboard, click the link in the Incident ID column.
 - Click the **Incidents** tab to navigate to the Incidents page, which displays recent incidents, and click the link in the Incident ID column.
 - Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Click the Security Manager icon in the Reporting Device field of the Incident Details page for incidents generated by signatures.



Note

Although this page contains elements other than those listed in the field reference table, these elements are either read-only or are used to navigate to other pages in MARS. Only the elements with which you can perform actions specific to signature policy lookup are listed in the table.

Even though the Security Manager icon in the event displayed at the top of the page can be clicked, it only refreshes the page with the same contents. You need to click Edit Signature to navigate to the Signatures page in the Security Manager client; clicking this icon does not start the Security Manager client.

Field Reference

Table 11-3 Read-Only Signature Policy Lookup Page

Element	Description
Cisco Security Manager Login	Available only if you selected the option to prompt the user for Security Manager login credentials for signature rule lookup in the Reporting Applications tab and the Security Manager credentials are neither cached nor saved in the MARS database.
User Name	The username for logging in to Security Manager. Note The user must have administrative privileges to open the Security Manager client from the read-only signature details page. Otherwise, an error message is displayed when you click Edit Signature or Add Filter.
Password	The password for logging in to Security Manager.
Submit	Sends the entered credentials to Security Manager and displays the read-only signature parameters in the same page, if authentication is successful.
Save Credentials	Available only if the Allow Users to Save Credentials check box is selected in the Reporting Applications tab of MARS. When selected, Security Manager credentials are saved in the MARS database and reused during policy lookup. You are not prompted for credentials during subsequent policy lookup operations if you select this check box.
Signature Details	If the Cisco Security Manager Login section is displayed, this section appears after MARS is successfully authenticated with Security Manager. Otherwise, these details are displayed immediately after the policy query lookup page is opened.
Edit Signature	Click to open the Signatures page in Security Manager. The IPS signature that generated the event is highlighted in the policy table. If an instance of the Security Manager client is already open, the same instance is activated. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.

Table 11-3 **Read-Only Signature Policy Lookup Page (Continued)**

Add Filter	Opens the Add Event Action Filter dialog box in Security Manager with the Actions to Subtract, % to Deny, Attacker Address, and Attacker Port fields populated with values derived from the MARS event. The remaining fields are displayed with default values.
Signature ID	Identifies the unique numerical value assigned to this signature. The signature ID contains hyperlinks to the Cisco Network Security Database (NSDB). Clicking on the link in the ID column will trigger the opening of an external browser window that opens to the entry in Security Center (MySDN) for that signature.
Signature Parameters	Displays the built-in micro-engine parameters for a particular signature. These parameters determine how the signature is configured and applied to an incoming packet. Click the + icon beside the Parameters option to expand the tree and display the available signature parameters. If a + icon appears beside any of the items in the expanded list, it indicates that more options are available for this parameter.
CS Manager Details	Click open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved.



CHAPTER 12

Botnet Traffic Filtering

Revised: September 16, 2010

This chapter describes the Botnet Traffic Filter support on the MARS Appliances and includes the following sections:

- [Information About Botnet Traffic Filtering, page 12-1](#)
- [Query Criteria, System Reports, and Rules Related to Botnet Traffic Filtering, page 12-3](#)
- [Site Management Page, page 12-14](#)

Information About Botnet Traffic Filtering

Table 12-1 *Feature History for Botnet Traffic Filtering on MARS Appliance*

Release	Modification
6.0.4	This feature was introduced.
6.1.1	Support for ASA 8.2.2 and 8.2.3 was introduced

Botnet in this context refers to a network of malicious software robots embedded on your network hosts that are activated by a distant botnet controller. See the following URL for further botnet information:

http://www.cisco.com/en/US/prod/vpndevc/ps6032/ps6094/ps6120/botnet_index.html

Table 12-2 defines abbreviations and terms used in this chapter.

Table 12-2 *Definitions of Terms*

Abbreviation or Term	Definition within the Context of this Documentation
BTF	Cisco ASA Botnet Traffic Filter
Botnet Site	A Black-, Gray-, or White-listed site as configured on the Cisco ASA Botnet Traffic Filter. A White-listed site is not technically a botnet site, but this term appears in the context of discussing the Cisco ASA Botnet Traffic Filter.
phone-home	Traffic from your network hosts to a Black- or Gray-listed sites.

Table 12-2 **Definitions of Terms (Continued)**

Abbreviation or Term	Definition within the Context of this Documentation
Reconnaissance	Traffic from Black- or Gray-listed hosts to “infected” hosts on your network.
Black-list	Known malware addresses—These addresses are on the blacklist identified by the Cisco ASA dynamic database and the static blacklist.
Gray-list	Ambiguous addresses—These addresses are associated with multiple domain names and some, but not all of these domain names are on the blacklist.
White-list	Known allowed addresses—These IP addresses are on the Cisco ASA white-list. They are typically Black-listed by the dynamic database, then identified as acceptable by the Cisco ASA administrator.

The Botnet Traffic Filter detects rogue traffic to or from Black-, Gray-, or White-listed hosts across all ports (botnet sites) and then forwards a syslog message to the Cisco Security MARS for detailed reporting and mitigation suggestions. Botnet Traffic Filtering is implemented on the Cisco Ironport Web Security Appliances and the Cisco ASA 5500 Adaptive Security Appliance, beginning with Version 8.2. With the introduction of ASA 8.2.2 in Cisco Security MARS 6.1.1, the Botnet Traffic Filter added Threat Level and Threat Category attributes to its detection and mitigation capabilities.

The Cisco ASA can download dynamically updated lists of botnet sites from a Cisco Ironport update server, as well as manually add botnet sites to the list on the Cisco ASA. To avoid false positives, whitelists can also be configured on the Cisco ASA to ignore known servers (for instance, the Yahoo or Google toolbar servers).

For further information on how to configure the Botnet Traffic Filter on the Cisco ASA 5500 Adaptive Security Appliance, Version 8.2, go to the following URL:

http://www.cisco.com/en/US/docs/security/asdm/6_2/user/guide/conns_botnet.html

MARS enhances the Cisco ASA botnet filter detection and mitigation capabilities because MARS, with its database correlation, query and reporting capabilities, can provide a global view across many firewalls while retaining the results over many separate time periods. An administrator can better prevent botnet activity by issuing mitigation commands to enforcement devices identified through MARS correlation, reporting and topology mapping.

MARS support for the Botnet Traffic Filter includes the following:

- Query result formats to display botnet sites ranked by session, or to display botnet events with site names (sessionized or in real-time)
- On-demand system reports to record suspected phone-home activity to Black-listed hosts and to record reconnaissance or attacks from Black-listed hosts to internal hosts
- Scheduled system reports to identify “Top botnet sites,” “Top infected hosts,” “Top botnet ports,” “Phone Home Traffic Events,” and “Malicious Site Traffic Events”
- System Rules to detect communication to and from Black- and Gray-listed botnet sites
- Activity charts of Top Botnet Ports, Top Botnet Sites, Top Botnet Hosts, Phone-Home Events, and Malicious Site Traffic Events on the Summary page
- Top 3 Botnet sites reported in email notifications

To gather and correlate Botnet Traffic Filter data on MARS, install the Cisco ASA, Version 8.2 as a MARS Security and Monitoring Device, as described in the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/device/configuration/guide/chAsa8x.html#wp1053948

Query Criteria, System Reports, and Rules Related to Botnet Traffic Filtering

This section discusses the following topics:

- [Botnet Site Query Criteria for Queries, Reports, and Rules](#)
- [Query Result Formats for Botnet Traffic Filter](#)
- [System Reports](#)
- [MARS Events for Botnet Traffic Filter](#)

For descriptions of all MARS reports and rules, see the “Systems Rule and Reports Reference” at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/appMars.html

Botnet Site Query Criteria for Queries, Reports, and Rules

Botnet site domain names and IP addresses that are known to MARS can be used as matching criteria in queries and rules as a Source IP or Destination IP parameter.

The **Management > Site Management** page lists all Botnet sites reported to MARS by the Cisco ASA Botnet Traffic Filter.

Botnet Traffic Filter event types can be used as matching criteria for Queries and Rules when setting the Events parameter. [Figure 12-1](#) shows how selecting **All Sites (ASA Botnet Traffic Filter)** displays all botnet sites available for the Source IP query parameter.

Figure 12-1 Botnet Traffic Filter Query Criteria

Query Event Data
Click the cells below to change query criteria:

Query type: *Destination Ports ranked by Sessions, Apr 1, 1970 9:15:00 AM PST - Apr 19, 2010 9:25:00 AM PDT* [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY

Filter by Source

Toggle Equal [Select All]

Pre-NAT source addresses: [Pre-NAT source addresses]

Remove (0)

Grouped As

IP: [IP] [IP]

Range: [Range] [Range]

Copyright © 2003–2010 Cisco Systems, Inc. All rights reserved.

236394

Clicking on a botnet site name or IP address launches a popup window with additional information on that site, as shown in Figure 12-2.

Figure 12-2 Botnet Site Information Popup Window

Static information includes host attributes such as MAC address, DNS name, operating system, open ports, applications and vulnerabilities. This information is assimilated from (a) topology discovery, (b) host fingerprinting during incident false positive analysis and (c) reports imported from Vulnerability Assessment tools to CS-MARS.

Static Info		Dynamic Info	
Device Name: 171.69.229.103/255.255.255.103			
IP Address: 171.69.229.12			
Interface Information			
Interface Name	MAC Address	MAC Update Time	
dummyInterface	00:30:48:88:e5:c2	Sep 15, 2010 4:17:37 AM PDT	
Site(ASA Botnet Traffic Filter) Information			
Site Name	Type of List(black/grey/white)	Threat Level	Threat Category
171.69.229.103/255.255.255.103	White	none	

Copyright © 2003–2010 Cisco Systems, Inc. All rights reserved.

236395

Query Result Formats for Botnet Traffic Filter

The Query Result formats related to Botnet Traffic Filter are as follows:

- Site Ranking (ASA Botnet Traffic Filter)
- All Matching Events (with site from ASA Botnet Traffic Filter)

Site Ranking Query Result Format

This result format ranks botnet sites by sessions. The total sessions count for a botnet site includes sessions where the black or gray site appears as a Cisco ASA syslog source site (suggesting a possible reconnaissance or attack) or as a Destination Site (suggesting possible phone-home activity).

The query results (or report results using this query format) shows the total count of sessions per botnet site with subtotals showing how many were Source Sites and how many were Destination Sites (See, [Figure 12-4](#)).

To filter on specific botnet sites, use the standard “Event Type Ranking” Result Format, specifying Source IP or Destination IP.

To view the Site Ranking query result format, navigate to **Query/Reports > Edit > Site Ranking (ASA Botnet Traffic Filter)**.

[Figure 12-3](#) shows the Site Ranking by Session query result format as it appears on the MARS GUI.

Figure 12-3 Site Ranking Query Result Format

The screenshot displays the Cisco MARS GUI interface for configuring a query. At the top, there is a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below this, a status bar shows the date and time: Sep 15, 2010 8:42:29 AM PDT, and the login information: Login: Local: Administrator (pnadmin) :: Logout :: Activate.

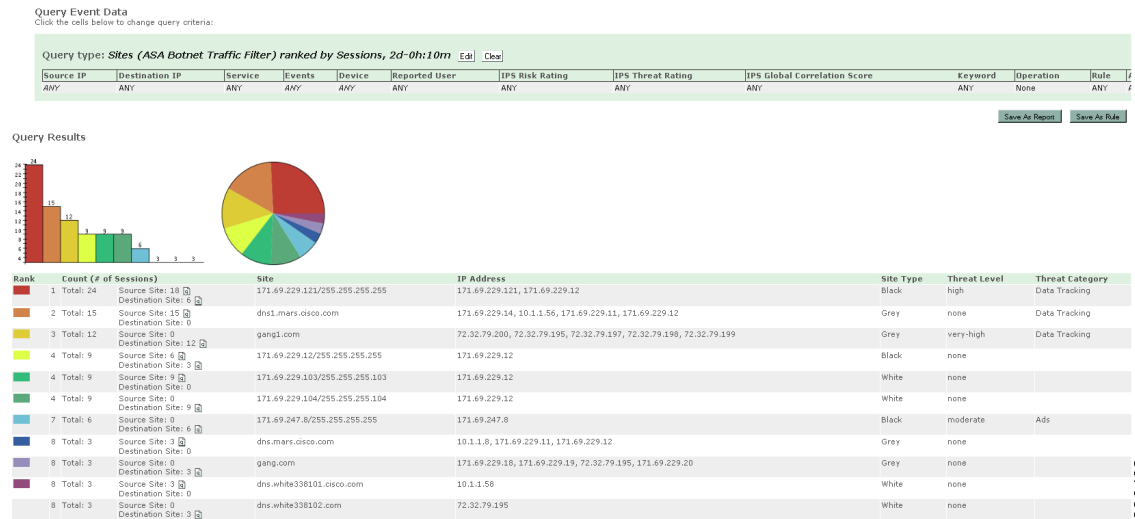
The main content area is titled "Query Event Data" and includes a sub-header "Click the cells below to change query criteria:". Below this, there is a section for "Query type: Event Types ranked by Sessions, 3d-0h:10m" with "Edit" and "Clear" buttons.

A table with the following columns is displayed: Source IP, Destination IP, Service, Events, Device, Reported User, IPS Risk Rating, IPS Threat Rating, IPS Global Correlation Score, Keyword, Operation, Rule, and Action. The table contains a single row with the value "ANY" for all columns.

Below the table, there is a section for "Result Format: Site Ranking (ASA Botnet Traffic Filter)" with a dropdown menu. Underneath, there are fields for "Order/Rank By: Session Count" and "Filter by Time:". The "Filter by Time:" section includes a "Last:" field set to 3 Days 0 Hrs 10 Mins, a "Start:" field set to 1970 April 1 9 Hrs 15 Mins, and an "End:" field set to 2010 April 19 9 Hrs 25 Mins. There is also a "Real Time: Sessionized events" dropdown and a "Use Only Firing Events:" checkbox with a dropdown set to "Any Status". At the bottom, there is a field for "Maximum number of rows returned: 5000".

At the bottom of the page, there is a copyright notice: "Copyright © 2003–2010 Cisco Systems, Inc." and a summary bar: "Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help".

[Figure 12-4](#) displays the output of the Botnet Site Ranking by Session query.

Figure 12-4 Botnet Site Ranking Query Output

All Matching Events With Botnet Sites Result Format

The query result format, “All Matching Events (with sites with ASA Botnet Traffic Filter),” is equivalent to the “All Events” result format except that the botnet result format displays botnet site names in the query results (Source Site or Destination Site) where the “All Matching Events” output does not. For events that do not contain botnet site information, “N/A” is displayed as the site information. Because a non-botnet event does not have site information, no query icon appears next to the “N/A.”

The “All Matching Events (with sites with ASA Botnet Traffic Filter)” query can display results as sessionized events, or it can display events in real time.

Figure 12-5 shows the All Matching Events query format as it appears on the MARS GUI.

Figure 12-5 All Matching Events (with Sites from ASA Botnet Traffic Filter) Result Format

CISCO [SUMMARY](#) [INCIDENTS](#) [QUERY / REPORTS](#) [RULES](#) [MANAGEMENT](#) [ADMIN](#) [HELP](#)

Query | Batch Query | Report | Sep 15, 2010 9:02:23 AM PDT

[QUERY / REPORTS](#) | CS-MARS Local Controller: pmars/LC1 v6.1.1 | Login: Local: Administrator (pnadmin) :: [Logout](#) :: [Activate](#)

Query Event Data
Click the cells below to change query criteria:

Query type: **Event Types ranked by Sessions, 3d-0h:10m** [Edit](#) [Clear](#)

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Operation	Rule
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY

Result Format: **All Matching Events**

Order/Rank By: **Time**

Filter by Time:

☒ Last: Days Hrs Mins

☐ Start: Hrs Mins

End: Hrs Mins

☐ Real Time: **Raw events**

Use Only Firing Events: ☐ **Any Status**

Maximum number of rows returned:

Figure 12-6 displays the real-time output of the All Matching Events query result format.

Figure 12-6 All Matching Events (with Sites from ASA Botnet Traffic Filter) Real-time Raw Events

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY
419878625	64.101.182.234	N/A	1702	N/A	1188	TCP	Sep 15, 2010 12:18:38 PM PDT	fake0.2				
419878626	10.89.130.28	N/A	1188	N/A	1702	TCP	Sep 15, 2010 12:18:38 PM PDT	fake0.2				
419878627	N/A	N/A	N/A	N/A	N/A	TCP	Sep 15, 2010 12:18:38 PM PDT	fake0.2				
419878628	64.101.182.16	N/A	34346	N/A	7778	TCP	Sep 15, 2010 12:18:40 PM PDT	fake0.5				
419878629	64.101.182.228	N/A	N/A	N/A	N/A	TCP	Sep 15, 2010 12:18:40 PM PDT	fake0.5				
419878630	10.2.2.1.3	N/A	6080	N/A	54788	TCP	Sep 15, 2010 12:18:40 PM PDT	fake0.5				
419878631	10.89.130.30	N/A	47912	N/A	5000	TCP	Sep 15, 2010 12:18:40 PM PDT	fake0.5				
419878632	N/A	N/A	N/A	N/A	N/A	TCP	Sep 15, 2010	fake0.5				

Figure 12-7 displays the sessionized output of the All Matching Events (with Sites from ASA Botnet Traffic Filter) query result format.

Figure 12-7 All Matching Events (with Sites from ASA Botnet Traffic Filter) Sessionized Events Output

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY
E:418408707, S:418408707, I:416909035	N/A	10.200.5.1	66537	255.255.255.255	69	UDP	Sep 14, 2010 1:11:54 PM PDT	igod71admin.mars.cisco.com				
E:418408704, S:418408704	N/A	N/A	N/A	N/A	N/A	ICMP	Sep 14, 2010 1:11:53 PM PDT	fake0.1				
E:418408703, S:418408703	N/A	10.89.130.28	33008	64.101.182.69	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9				
E:418408702, S:418408422	N/A	N/A	N/A	N/A	N/A	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9				
E:418408701, S:418408430	64.101.182.147	32795	64.101.176.33	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408700, S:418408424	64.101.182.220	1091	128.107.250.141	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408699, S:418408427	10.89.130.30	42551	171.71.177.254	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408698, S:418408424	64.101.182.168	1104	128.107.250.141	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408697, S:418408424	N/A	N/A	N/A	N/A	N/A	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9				
E:418408696, S:418408426	10.89.130.30	42551	171.71.177.254	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408695, S:418408425	N/A	10.89.130.28	33008	64.101.182.69	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9				
E:418408694, S:418408422	64.101.182.44	39922	64.101.176.33	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408693, S:418408423	N/A	N/A	N/A	N/A	N/A	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9				
E:418408692, S:418408692	64.101.182.147	32795	64.101.176.33	25	TCP	Sep 14, 2010 1:11:53 PM PDT	fake0.9					
E:418408687, S:418408687	N/A	N/A	N/A	N/A	N/A	N/A	Sep 14, 2010 1:11:51 PM PDT	pmnars				
E:418408686, S:418408686	N/A	N/A	N/A	N/A	N/A	ICMP	Sep 14, 2010 1:11:49 PM PDT	fake0.10				
E:418408685, S:418408685	10.200.5.1	66537	255.255.255.255	69	UDP	Sep 14, 2010 1:11:48 PM PDT	igod71admin.mars.cisco.com					
E:418408684, S:418408684	N/A	N/A	N/A	N/A	N/A	UDP	Sep 14, 2010 1:11:43 PM PDT	igod71admin.mars.cisco.com				

To display results showing only Botnet Traffic Filter Events, do the following:

Step 1 Navigate to the **Query/Reports > Query** page and click **Edit**.

The Result Format dialog screen appears

Step 2 Select the Result Format, **All Matching Events (with sites with ASA Botnet Traffic Filter)**.

- Step 3** Set the **Filter by Time** parameters. Click **Apply**.
The Submit Query page appears.
- Step 4** Click the **Events** parameter, then select the **Group:ASA Traffic Filter** criterion. Click **Apply**.
The Submit Query page appears.
- Step 5** Click **Submit**.
-

System Reports

The following six System Reports support Botnet Traffic Filtering:

- **Activity: ASA Botnet Traffic Filter - Top Botnet Ports**
This report ranks top destination ports for traffic originating from infected hosts to Black or Grey-listed sites, for all sessions as seen by MARS.
- **Activity: ASA Botnet Traffic Filter - Top Botnet Sites**
This report ranks top botnet sites (Black- or Gray-listed sites) for all inbound and outbound sessions as reported by the Cisco ASA Botnet Traffic Filter. This report uses the “Site Ranking (ASA Traffic Filter)” query result format and shows the total count of sessions per botnet site with subtotals showing how many were Source Sites and how many were Destination Sites (See, [Figure 12-9](#)).
- **Activity: ASA Botnet Traffic Filter - Top Botnet Sites Blocked**
This report ranks top botnet sites (Black- or Gray-listed sites) blocked for all inbound and outbound sessions as reported by the Cisco ASA Botnet Traffic Filter. This report uses the “Site Ranking (ASA Traffic Filter)” query result format and shows the total count of sessions per botnet site with subtotals showing how many were Source Sites and how many were Destination Sites (See, [Figure 12-9](#)).
- **Activity: ASA Botnet Traffic Filter - Top Infected Hosts**
This report ranks top infected hosts for traffic originating from infected hosts to Black- or Gray-listed sites, for all sessions as seen by MARS.
- **Activity: ASA Botnet Traffic Filter: Phone Home - All Events**
This report details all suspicious events related to phone home activity, as reported by ASA Botnet Traffic Filter.
- **Attacks: ASA Botnet Traffic Filter: Malicious Site Traffic - All Events**
This report details all events related to traffic originating from black/gray sites/IPs, as reported by ASA Botnet Traffic Filter.

To view Reports, navigate to the MARS **Query/Reports > Report > ASA Botnet Traffic Filter**. [Figure 12-8](#) shows the Botnet Traffic Filter report definitions from the MARS GUI.

Figure 12-8 MARS Reports Related to Botnet Traffic Filter

CISCO

Query | Batch Query | Report

QUERY / REPORTS | CS-MARS Local Controller: pnmars/LC1 v6.1.1

Login: Local: Administrator (pna)

Report Selection

Group: GCSystem: ASA Botnet Traffic Filter

Schedule: All

Name	Provider	Schedule	Format	Recipients	Query	Description	Status	Submitted
Activity: ASA Botnet Traffic Filter - Top Botnet Ports	Cisco	Every hour	Total View	None	Event type: ASATrafficFilter/PhoneHomeTrafficLogged Query Type: Destination Ports ranked by Sessions Time: 0d-1h:00m	This report ranks top destination ports for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.	Finished: Sep 14, 2010 1:02:03 PM PDT	Sep 14, 2010 1:02:03 PM PDT
Activity: ASA Botnet Traffic Filter - Top Botnet Sites	Cisco	Every hour	Total View	None	Event type: ASATrafficFilter/PhoneHomeTrafficLogged, ASATrafficFilter/TrafficLoggedFromMaliciousSite Query Type: Sites (ASA Botnet Traffic Filter) ranked by Sessions Time: 0d-1h:00m	This report ranks top botnet sites (black/grey listed sites) for all inbound/outbound sessions as reported by ASA Botnet Traffic Filter.	Finished: Sep 14, 2010 1:02:04 PM PDT	Sep 14, 2010 1:02:04 PM PDT
Activity: ASA Botnet Traffic Filter - Top Botnet Sites Blocked	Cisco	Every hour	Total View	None	Event type: ASATrafficFilter/PhoneHomeTrafficBlocked, ASATrafficFilter/TrafficBlockedFromMaliciousSite Query Type: Sites (ASA Botnet Traffic Filter) ranked by Sessions Time: 0d-1h:00m	This report ranks top botnet sites (black/grey listed sites) blocked for all inbound/outbound sessions as reported by ASA Botnet Traffic Filter.	Finished: Sep 14, 2010 1:02:03 PM PDT	Sep 14, 2010 1:02:03 PM PDT
Activity: ASA Botnet Traffic Filter - Top Infected Hosts	Cisco	Every hour	Total View	None	Event type: ASATrafficFilter/PhoneHomeTrafficLogged Query Type: Source IPs ranked by Sessions Time: 0d-1h:00m	This report ranks top infected hosts for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.	Finished: Sep 14, 2010 1:02:04 PM PDT	Sep 14, 2010 1:02:04 PM PDT
Activity: ASA Botnet Traffic Filter: Phone Home - All Events	Cisco	Run on demand only	Total View	None	Event type: ASATrafficFilter/PhoneHomeTrafficLogged Query Type: Events (with sites from ASA Botnet Traffic Filter) ranked by Time Time: 0d-1h:00m	This report details all suspicious events related to phone home activity, as reported by ASA Botnet Traffic Filter.	Finished: Sep 9, 2010 2:51:35 PM PDT	Sep 9, 2010 2:51:33 PM PDT
Attacks: ASA Botnet Traffic Filter: Malic Site Traf - All Events	Cisco	Run on demand only	Total View	None	Event type: ASATrafficFilter/TrafficLoggedFromMaliciousSite Query Type: Events (with sites from ASA Botnet Traffic Filter) ranked by Time Time: 0d-1h:00m	This report details all events related to traffic originating from black/grey sites/IPs, as reported by ASA Botnet Traffic Filter.	Finished: Sep 9, 2010 2:51:53 PM PDT	Sep 9, 2010 2:51:51 PM PDT

236403

Figure 12-9 shows the output of the Top Botnet Sites report.

Figure 12-9 MARS Reports Results—Top Botnet Sites

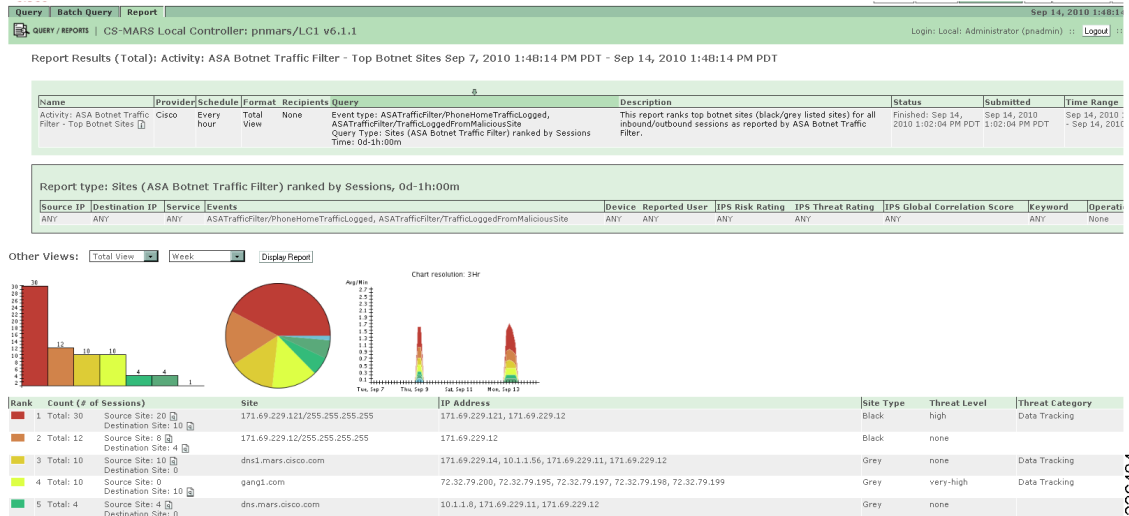
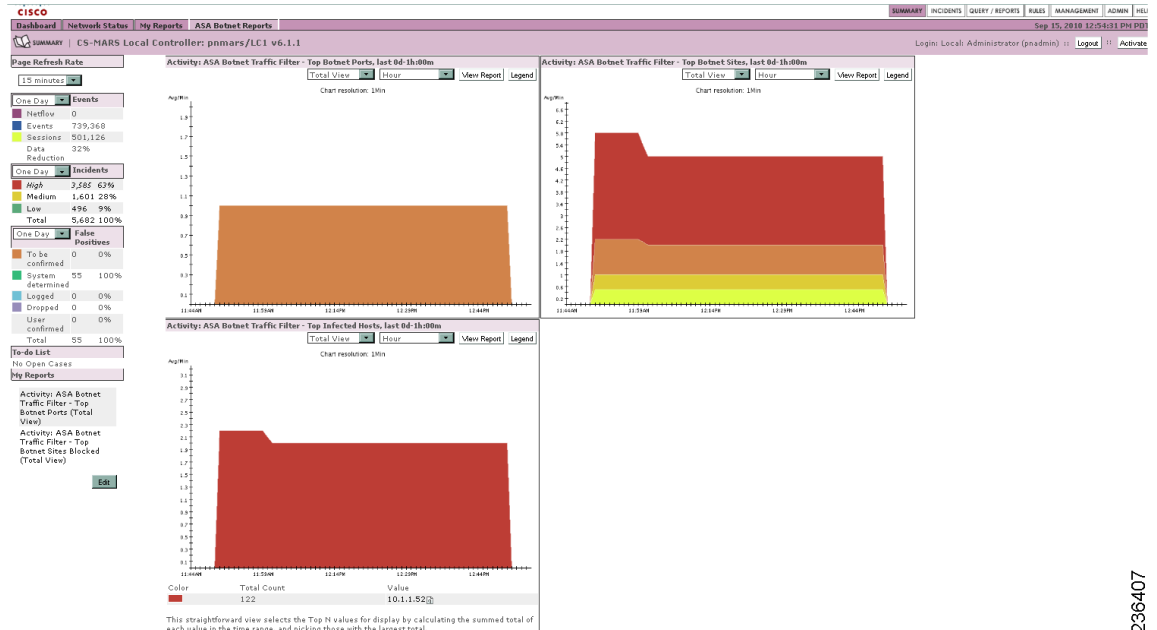


Figure 12-10 shows the continually updated charts for the Botnet Traffic Filter reports—Top Botnet sites, Top Botnet Ports, and Top Botnet Infected Hosts—available on the **Summary > ASA Botnet Reports** page.

Figure 12-10 Summary Page—ASA Botnet Reports (Top Ports, Top Sites, Top Infected Hosts)



MARS System Rules and Notifications for Botnet Traffic Filtering

The following two System Rules support Botnet Traffic Filtering:

- **System Rule: Blocked Phone Home Activity: ASA Botnet Traffic Filter**
This rule detects phone home activity to Black- and Gray-listed sites and IP addresses that was blocked, as reported by the Cisco ASA Botnet Traffic Filter.
- **System Rule: Blocked Traffic from site: ASA Botnet Traffic Filter**
This rule detects blocked traffic activity originating from Black and Gray-listed sites and IP addresses, as reported by the Cisco ASA Botnet Traffic Filter.
- **System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter**
This rule detects phone home activity to Black- and Gray-listed sites and IP addresses, as reported by the Cisco ASA Botnet Traffic Filter.
- **System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter**
This rule detects traffic activity originating from Black and Gray-listed sites and IP addresses, as reported by the Cisco ASA Botnet Traffic Filter.

To view Rules, navigate to the **MARS Rules > Inspection Rules** page.

Figure 12-11 shows the Botnet Traffic Filter rule definitions from the MARS GUI.

Figure 12-11 MARS System Rules for Cisco ASA Botnet Traffic Filter

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	IPS Risk Rating	IPS Threat Rating	IPS Global Correlation Score	Keyword	Severity Count	Close Operation
1		ANY	ANY	ANY	ASATrafficFilter/PhoneHomeTrafficBlocked	ANY	None	ANY	ANY	ANY	ANY	ANY	1
1		ANY	ANY	ANY	ASATrafficFilter/TrafficBlockedFromMaliciousSite	ANY	None	ANY	ANY	ANY	ANY	ANY	1
1		ANY	ANY	ANY	ASATrafficFilter/PhoneHomeTrafficLogged	ANY	None	ANY	ANY	ANY	ANY	ANY	1
1		ANY	ANY	ANY	ASATrafficFilter/TrafficLoggedFromMaliciousSite	ANY	None	ANY	ANY	ANY	ANY	ANY	1

Botnet Traffic Filter Notifications

The Botnet Traffic Filter rules can be configured to send notifications. Because of space limitations, the syslog and SNMP incident notifications do not explicitly label botnet site information. The email notification includes a “Top 3 sites sorted by count” listing, as shown in Example 12-1.

Example 12-1 Email Notification With Botnet Site Information

```
From: notifier.pnmars@cisco.com [mailto:notifier.pnmars@cisco.com]
Sent: Friday, June 19, 2009 2:49 PM
```

To: Lavim Busa (labusa)
 Subject: CS-MARS Incident Notification (yellow, Rule Name: labusa-notif)

The following incident occurred on "pnmars"

Start time: Fri Jun 19 14:46:22 2009
 End time: Fri Jun 19 14:46:29 2009
 Fired Rule Id: 328056
 Fired Rule: labusa-notif
 Incident Id: 607632
 Incident Severity: yellow

Top 3 src-dest address pairs sorted by severity and count (showing 3 of 9):

1. N/A	-> N/A	Severity: yellow	Count: 54
2. 1.2.3.4	-> 4.5.6.7	Severity: yellow	Count: 6
3. 11.22.33.44	-> 41.52.63.74	Severity: yellow	Count: 3

Top 3 src ip's address sorted by severity and count (showing 3 of 6):

1. N/A	-> Severity: yellow	Count: 54
2. 1.2.3.4	-> Severity: yellow	Count: 6
3. 11.22.33.44	-> Severity: yellow	Count: 5

Top 3 dest ip's address sorted by severity and count (showing 3 of 9):

1. N/A	-> Severity: yellow	Count: 54
2. 4.5.6.7	-> Severity: yellow	Count: 6
3. 41.52.63.74	-> Severity: yellow	Count: 3

Top 3 dest TCP/UDP ports sorted by severity and count (showing 2 of 2):

1. 80	Severity: yellow	Count: 11
2. 80	Severity: green	Count: 8

Top 3 event types sorted by severity and count (showing 3 of 16):

1. Download failed for dynamic filter data file from updater server	Severity: yellow	Count: 9
2. Authentication failure with dynamic filter updater server	Severity: yellow	Count: 9
3. Decryption of downloaded dynamic filter data file failed	Severity: yellow	Count: 9

Top 3 reporting devices sorted by count (showing 1 of 1):

1. asa82	Count: 100

Top 3 sites sorted by count (showing 3 of 3):

1. cisco.com	(Type: black)	Count: 6
2. whitecisco.com	(Type: white)	Count: 6
3. altavista.com	(Type: grey)	Count: 5

For more details about this incident please go to:

https://pnmars/Incidents/IncidentDetails.jsp?Incident_Id=607632
https://pnmars.mars.cisco.com/cisco.com/Incidents/IncidentDetails.jsp?Incident_Id=607632
https://192.168.1.10/Incidents/IncidentDetails.jsp?Incident_Id=607632
https://10.2.4.1/Incidents/IncidentDetails.jsp?Incident_Id=607632

For all incidents occurred recently please go to:

<https://pnmars/Incidents/>
<https://pnmars.mars.cisco.com/cisco.com/Incidents/>
<https://192.168.1.10/Incidents/>
<https://10.2.4.1/Incidents/>

MARS Events for Botnet Traffic Filter

The following event groups comprise the Botnet Traffic Filter related events.

- ASATrafficFilter/All

- ASATrafficFilter/TrafficLoggedFromMaliciousSite
- ASATrafficFilter/TrafficBlockedFromMaliciousSite
- ASA TrafficFilter/Misc
- ASATrafficFilter/OperationalError
- ASATrafficFilter/PhoneHomeTrafficLogged
- ASATrafficFilter/PhoneHomeTrafficBlocked
- Info/UncommonTraffic/Suspicious

To view Events and Event Groups, navigate to the MARS **Management > Event Management** page.

[Table 12-3](#) lists the Events related to the Cisco ASA Botnet Traffic Filter

Table 12-3 MARS Botnet Traffic Filter Events

MARS Normalized Event Number	Event Name
1734142	Traffic originating from Black-listed site
1734143	Phone home traffic to Black-listed site
1734144	Traffic originating from Black-listed IP
1734145	Phone home traffic to Black-listed IP
1734146	Traffic originating from White-listed site
1734147	Traffic destined to White-listed site
1734148	Traffic originating from White-listed IP
1734149	Traffic destined to White-listed IP
1734150	Traffic originating from Gray-listed site
1734151	Phone home traffic to Gray-listed site
1734152	Intercepted DNS reply for listed site
1734153	Adding an IP address to the dynamic filter rule
1734154	Removal of an IP address from the dynamic filter rule
1734155	Download dynamic filter data file from updater server succeeded
1734156	Download failed for dynamic filter data file from updater server
1734157	Authentication failure with dynamic
1734158	Decryption of downloaded dynamic filter data file failed
1734160	Current license does not support dynamic filter updater feature
1734161	Failed to receive an update from dynamic filter updater server
1734228	Traffic originating from blacklisted site was blocked.
1734229	Traffic to blacklisted site was blocked.
1734230	Traffic originating from blacklisted IP is blocked
1734231	Traffic to blacklisted IP was blocked.
1734232	Traffic originating from greylisted site was blocked.
1734233	Traffic to greylisted site was blocked.

Site Management Page

The site management page, shown in [Figure 12-12](#), lists all Black-, Gray-, and White-listed botnet sites parsed from Cisco ASA syslogs. Sites can be deleted from this page, but cannot be edited or manually added.

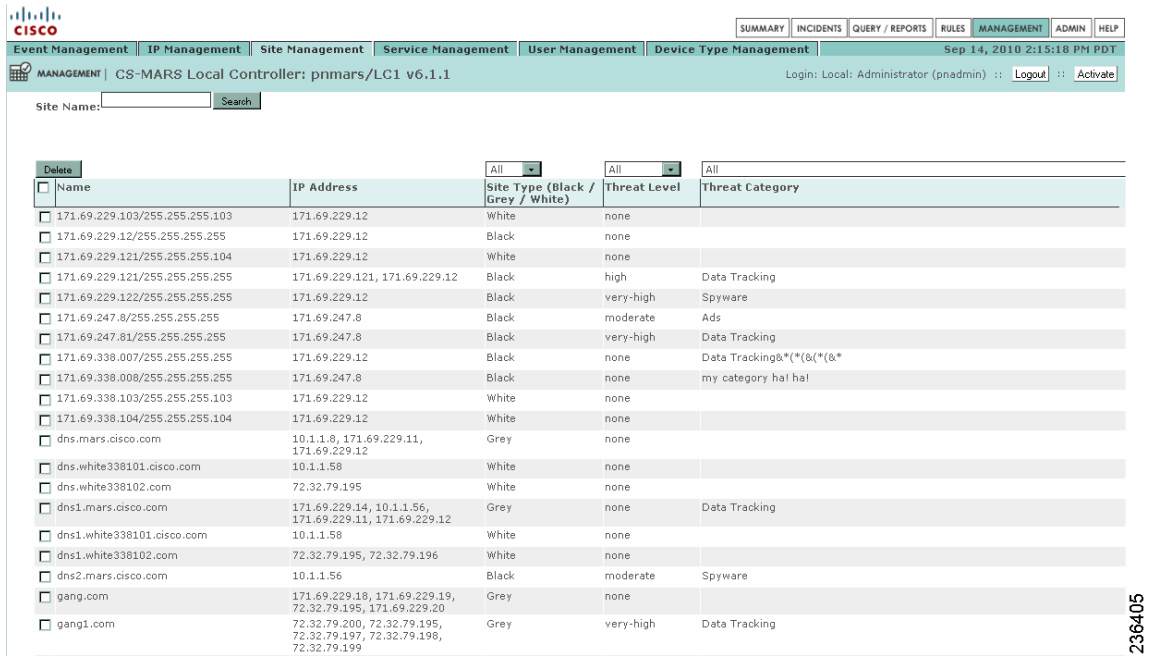
All sites reported in Cisco ASA syslogs as Black-lists and Gray-lists are malware sites. Sites reported as whitelists are not considered malware. Each time MARS parses a botnet address and sitename from a Cisco ASA syslog, the site is appended to the MARS Site Management list. Over time, the list may become obsolete and long, making it a practical necessity to delete sites. The Cisco ASA configuration is not affected by any site delete action performed in MARS.



Note

White-listed sites are technically not “botnet sites” but they may be referred to as botnet sites in this documentation because the Cisco ASA Botnet Traffic Filter is the only context in which the term “White-list” appears in MARS.

Figure 12-12 MARS Site Management Page

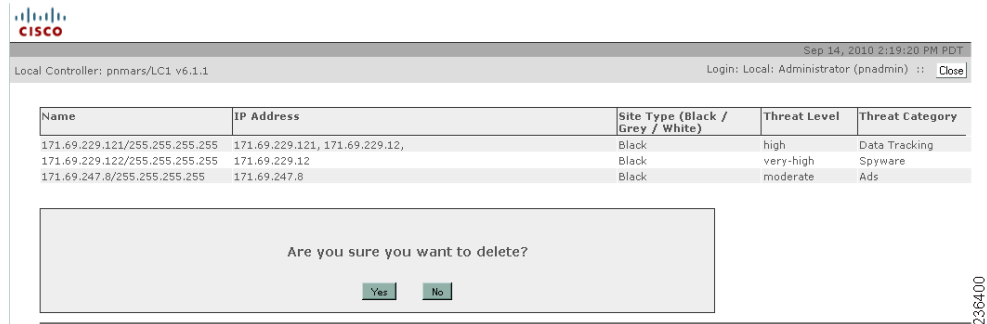


Use the **Site Type** pull-down filter to display, All, Black-, Gray-, or White-listed sites. Use **Threat Level** or **Threat Category** pulldown filter to display sites with selected threat levels or threat categories.

To search for a specific site name, enter the name or fragment of the name into the **Site Name** field and click **Search**. A site name can have multiple IP addresses.

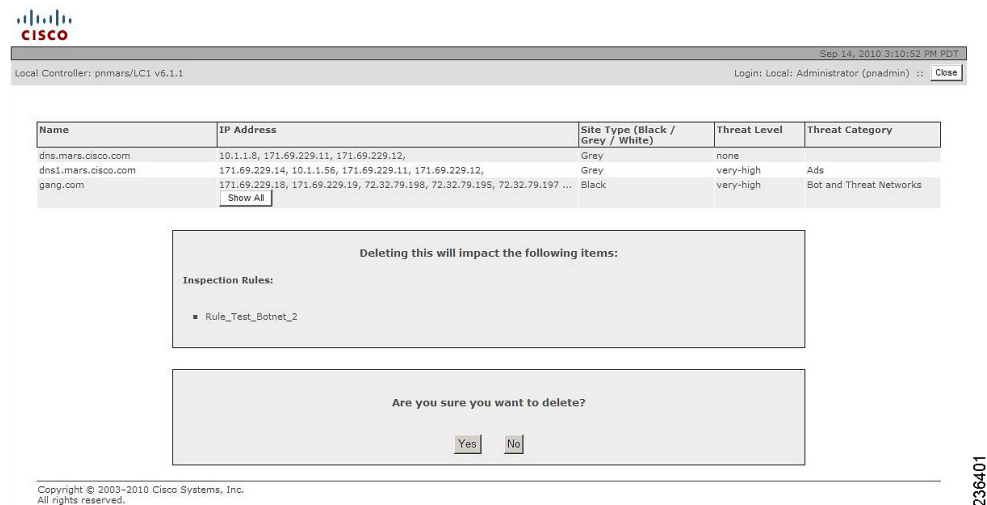
Deleting Sites

To delete sites, check the box of the site and click **Delete**. A popup window appears as shown in [Figure 12-13](#).

Figure 12-13 Delete Confirm Popup Window—Delete Sites

Deleting a Site Referenced in a Rule or Report

If a user-created rule or report includes a botnet site as a criterion, and an attempt is made to delete that site from the Site page, a delete confirmation popup window appears that lists the affected rules and reports, as shown in Figure 12-14.

Figure 12-14 Delete Confirmation Popup Window—Delete Site Referenced by a Rule

A rule that references a deleted site is made inactive.

If the site that is referenced by a report is deleted, that report is deleted and a new report with all the same parameters is created but with the deleted botnet site information removed.

When a large number of sites are selected for deletion, MARS checks all the rules and reports for botnet references before deleting the sites. This may cause a delay in displaying the delete confirmation page.



CHAPTER 13

System Maintenance

Much of the system maintenance information for the MARS Appliance is provided exclusively in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

The MARS Appliance requires little maintenance. To perform maintenance tasks, you can use the CLI or the web interface, as needed. Some hardware maintenance tasks require physical access to the MARS Appliance.



Note

For information on upgrading, backing up, and restoring data on the MARS Appliance, see the [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#) and [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#).

This chapter contains the following topics:

- [Setting Runtime Logging Levels, page 13-1](#)
- [Viewing the MARS Backend Log Files, page 13-2](#)
- [Viewing the Audit Trail, page 13-2](#)
- [Retrieving Raw Messages, page 13-3](#)
- [Change the Default Password of the Administrator Account, page 13-7](#)
- [Understanding Certificate and Fingerprint Validation and Management, page 13-7](#)
- [Database Tuning and Query Optimization, page 13-11](#)

Setting Runtime Logging Levels

To set the appliance's runtime logging levels, navigate to **Admin > System Maintenance > Set Runtime Logging Levels**. For typical use, it is best to leave this page set to its defaults.

When you have made your selections, click the **Change Logging Levels** button.

The following log levels are available:

- **Fatal**—Enables fatal logging messages. Fatal messages record very severe error events that will likely lead the application to abort.
- **Error**—Enables error and fatal logging messages. Error messages record error events that might still allow the application to continue running.
- **Warn**—Enables warning, error, and fatal logging messages. Warning messages record potentially harmful situations.

- **Info**—Enables informational, warning, error, and fatal logging messages. Informational messages highlight the progress of the application at coarse-grained level.
- **Debug**—Enables debug, informational, warning, error, and fatal logging messages. Debug messages record fine-grained informational events that are most useful to debug an application.
- **Trace**—Enables trace, debug, information, warning, error, and fatal logging messages. Trace messages record finer-grained informational events than debug messages.

Viewing the MARS Backend Log Files

To view the appliance's log files or to change their levels or source, navigate to **Admin > System Maintenance > View Log Files**.

Figure 13-1 Backend log viewing options

View Backend Log

☒ Last: 0 Days 1 Hrs 0 Mins
 ☐ Start: 2003 September 11 14 Hrs 4 Mins
 End: 2003 September 11 15 Hrs 4 Mins

Select Level: All Select Source: Backend Submit

143387

You can view the appliance's backend logs either by selecting a number of days, hours, and minutes or you can view logs by selecting a start and ending date and time.

You can select the levels of logs that you want. Your choices are: All, Fatal, Error, Warn, Info, and Debug.

You can also choose the source of the files that you want to view. Select either Backend or GUI.

To view the backend log files, follow these steps:

-
- Step 1** Click the appropriate radio button:
- **Last**—The present time minus the number of days, hours, and minutes entered.
 - **Start/End**—Absolute literal time ranges defined by the date to the minute.
- Step 2** Select user, group, and so on.
- Step 3** Select the source.
- Step 4** Click **Submit**.
-

Viewing the Audit Trail

You can track the activities of the appliance's users by analyzing the appliance's log files. To set the appliance's audit trail logs, navigate to **Admin > System Maintenance > View Audit Trail**. For typical use, it is best to leave this page set to its defaults.

You can view the user audit trails either by selecting a number of days, hours, and minutes, or you can view a specific interval by selecting a start and ending date and time.

To view the audit trail, follow these steps:

-
Step 1	Click the appropriate radio button: • Last: DD-HH-MM • Start/End: YY-MM-DD-HH-MM
Step 2	From the list, select the user or user group.
Step 3	Click Submit .
-

Retrieving Raw Messages

You can retrieve raw messages from either an archive server (see [Configuring and Performing Appliance Data Backups](#)) or from the local files running on the Local Controller. These two methods offer different advantages:

- **Archive server.** Retrieving raw messages, or event data, from an archive server is much faster than retrieving from the database. Therefore, it is the recommended option if it is available and it covers the time period you are investigating. However, this option is only available if you have enabled data archiving and waited the requisite time for the initial archival operation to occur; it is a scheduled operation that runs nightly around 2:00 a.m. After the initial archive is performed, the event data is written to the archive server frequently, often within 5 to 8 minutes after the MARS Appliance receives the message. That the data is not archived in real-time identifies another limitation to this option, and that is the historical period that can be studied. If you need to view data that is more current than an hour old, you should select the Database option to ensure that correct data is retrieved. For all other periods, the archive server option is recommended. To enable archiving, see [Configuring and Performing Appliance Data Backups](#).
- **Local Files.** Retrieving event data from the local files provides slower performance than the archive server. However, it provides access to the most current data received. Local Files have the five tuples, whereas archived raw messages do not have the five tuples.

This section contains the following topics:

- [About Raw Message Size Limitations and Storage Location, page 13-3](#)
- [Retrieve Raw Messages, page 13-4](#)

About Raw Message Size Limitations and Storage Location

Before the 5.2.4 release, the storage of raw message data in the local database was restricted to 500 KB per message. Beginning with 5.2.4, the raw message size is stored in local files that can be up to 1.5 MB without being truncated. Each MARS Appliance model has dedicated disk space reserved for arbitrary-sized raw message files. When the upper limit of this storage size is reached, the pnarchiver process moves the raw messages and associated index files to the remote NFS server, if configured. If no NFS server is configured, then the raw message files are purged, oldest data first (first in, first out). When the database is purged, the corresponding raw message files are also purged.

The raw message files are archived under `/pnarchive/DATA_POOL`. The `DATA_POOL` directory contains a dated directories under which the raw message files created on that date are compressed and saved. An example `/pnarchive/DATA_POOL/<date>` directory listing follows:

2007-02-10
2007-02-11

The file names use the following format:

```
[dbversion]-[productversion]-[serialno]_[StartTime]_[EndTime].gz
```

For example, the `./pnarchive/DATA_POOL/2007-02-12/ES` listing reveals:

```
ix-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
rm-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
```


Note

Those files beginning with “ix” are index files, and those beginning with “rm” are the raw message files.

Retrieve Raw Messages

You can retrieve Raw Messages in any of four different modes, depending on the settings you configure on the Retrieve Raw Messages page for source and destination of the files. You can:

- Retrieve data from archived files to a local MARS cache.
- Retrieve data from archived files to a remote network file server (NFS).
- Retrieve data from the database to a local MARS cache.
- Retrieve data from archived files to a remote network file server (NFS).

You can also filter the output according to time range, reporting device, and file size.

To retrieve raw message event data, follow these steps:

Step 1 Click **Admin > System Maintenance > Retrieve Raw Messages**.

The Raw Message Files page appears.

Figure 13-2 Retrieve Raw Messages Page

The screenshot displays the 'Retrieve Raw Messages' configuration page, organized into five sections:

- Data Source:** Contains two radio buttons: 'Archived Files (If Archiving is Turned On)' and 'From DataBase'. The 'From DataBase' option is selected.
- Filter:** Includes a 'Specify Time Range:' section with 'Start' and 'End' time pickers. The 'Start' is set to 2009 January 6 12 Hrs 59 Mins 38 Secs, and the 'End' is set to 2009 January 6 13 Hrs 9 Mins 38 Secs. Below this is a 'Select Reporting Device:' dropdown menu currently set to 'All Devices'.
- File Size:** Features a checkbox 'Specify Uncompressed File Size (Compression Ratio 10:1)'. When checked, a text box shows '100 MB (1 MB - 1024 MB)'.
- Output Settings:** Contains two radio buttons: 'Local MARS Cache' (selected) and 'Remote NFS Server'. Under 'Local MARS Cache', there is a checked checkbox 'Force Generation of Files', a 'Maximum Number of Files:' text box set to '10', and a 'View Local Cache' button. Under 'Remote NFS Server', there are text boxes for 'Remote Host IP:' and 'Remote Path:'.
- Output Raw Message Time Format:** Contains two radio buttons: 'Local Time' (selected) and 'UTC Time'.

251187

Step 2 In the Data Source area, click to select the source as either: **Archived Files** or **From Database**.



Note Archiving must be turned on for you to select Archived Files as the data source.

Step 3 In the Filter area, specify the time range by specifying values in the Start and End fields.



Note The default specifies the last 10 minutes.

Step 4 In the File Size area, to specify a file size limit, select **Specify Uncompressed File Size (Compression Ratio 10:1)** and then type in the box the size limit you want. (The range is from 1 to 1024 MB.) The default size is 100 MB.

If you have specified *Archived Files*, and you do not specify a file size limit, links to all the files within the specified time limit are displayed.

Step 5 In the Output Settings area, select *one* of the following:

- **Local MARS Cache**—You are given the following options:

- Deselect the **Force Generation of Files** option to negate forced generation of the files.
- Click **View Local Cache** to view the cache.
- Enter a number in the Maximum Number of Files field to increase or limit the number of files.
- **Remote NFS Server**—If you choose this option for output destination, you *must* specify the Remote Host IP and the Remote Path.

Step 6 Select the Output Raw Message Time Format as *one* of the following:

- Local Time (the output raw messages will be displayed in local time)
- UTC Time (the output raw messages will be displayed in UTC time)

Step 7 Click **Submit**.



Note While MARS is generating your files, you can still use the system for other tasks.

The *Retrieving Progress 0%* screen appears. When the operation is complete, the Raw Message Files screen appears, identifying a new Gzip archive file with a filename based on specified time range. The files are copied from the source (archive or database) to either the local cache in MARS or to the NFS specified, and links are displayed on the GUI to download files.

Get More Files

Raw Message Files

Download

2005-10-07-06-14-28_2005-10-08-06-24-28.gz Click Here to Download

143797

Step 8 To download and view the generated raw message file, click **Click Here to Download** next to the filename.

The filename adheres to the following syntax:

YYYY-MM-DD-HH-MM-SS_YYYY-MM-DD-HH-MM-SS.gz.

Step 9 Use WinZip or another archive expansion program to extract the contents of the Gzip archive file.

Step 10 After the textfile is extracted from the GNU Zip archive format, its contents resemble the following:

```
33750>Wed Jul 27 16:16:06 PDT 2005>BR-FW-1>10.1.2.4>9000>10.1.5.20>80>6><134>Jan 06 2003
11:03:53: %PIX-6-302001: Built inbound TCP connection 21000 for faddr 10.1.2.4/9000 gaddr
10.1.5.20/80 laddr 10.1.5.20/80
```

where it reads: *Event ID >>date >>device name >>src IP >>src port >>dst IP >>dst port >>protocol number >>raw message.*



Note If you see Chinese or other unfamiliar characters in the resulting text file, please use Microsoft Internet Explorer to view the file and verify that the Western European ISO or Western European Windows encoding value is selected (View > Encoding). The “»” sign appears correctly as a separator when a compatible encoding is selected.

Change the Default Password of the Administrator Account

Good security practices require that you change the default password. We recommend using strong passwords for the MARS Appliance appliances.

Login names and passwords:

- Can be alphanumeric characters
- Are case sensitive
- Can contain special characters (!, @, #, etc.)
- *Cannot* contain single or double quotes ('or “)

Login names can contain up to 20 characters. Passwords can contain up to 64 characters.

To change the default password and setup administrator notification, follow these steps:

-
Step 1	Click the Management > User Management tab.
Step 2	Check the box next to Administrator, and click Edit .
Step 3	Enter the new Administrator password and the Administrator e-mail address.
Step 4	Click Submit .
-

Understanding Certificate and Fingerprint Validation and Management

Many reporting devices use certificates or fingerprints to enable secure communications over SSL or SSH respectively. MARS performs a strict check of the certificate or fingerprint of the device or server to which it is attempting to connect.



Note

Certificate validation does not follow the convention of presenting the client with a list of certificate authorities and using the selected one to validate individual certificates. Instead, the MARS Appliance compares the certificate presented by the reporting device with a previously stored instance of the certificate. If the two match, the presented certificate is considered valid. This approach allows MARS to validate certificates without knowledge of revocation lists and to operate in a network without an Internet connection.

Three options exist for specifying how MARS should respond during attempts to establish a secure connection. The three options are as follows:

- **Automatically always accept.** This option, which is compatible with previous releases, allows a MARS Appliance to connect to reporting devices regardless of how frequently the certificate or fingerprint changes because MARS automatically accepts and stores the replacement certificate or fingerprint for all devices. However, this option does not provide an opportunity to inspect and authorize the changes to the certificates or fingerprints. When a conflict is detected or when a new certificate or fingerprint is accepted, the event is logged to the internal log. The internal log entry includes the name of the process that detected the conflict and the IP address of the reporting device. The logs can be retrieved by queries and reports. See [Monitoring Certificate Status and Changes](#), page 13-10 for more information on studying these events.

- **Accept first time and prompt on change (default).** This option accepts and stores a new certificate or fingerprint the first time MARS Appliance connects to a device. For subsequent connection attempts, the appliance checks the presented certificate or fingerprint against the stored value. If a conflict is detected, the session is refused unless the new certificate or fingerprint is manually accepted by the administrator. This option enables initial topology discovery to proceed without administrator intervention. Internal system logs of the initial acceptance, conflict detection, and acceptance of new change are created. The internal logs include the name of the process that detected the conflict, the IP address of the reporting device, and the username of the account used to accept the change.

If, when a change is detected by a web interface process, the session times out before administrative intervention, the communication fails but no internal system log is generated to record the failure to accept the changed certificate or fingerprint. Also, if a back-end process initiates the request, such as auto discovery, then the session attempt always fails and no attempt to obtain administrative acceptance is initiated. In such cases, any data the MARS Appliance would normally ascertain from the device during such a session is not collected. This delay of data retrieval does not apply to syslogs forward to the MARS Appliance by the reporting device and it resumes once the new certificate is accept. The recommended method for manually kicking off the change detections is to use the Test Connectivity or Discover button on the reporting device.

- **Always prompt on new and changed.** This option requires an administrator to manually accept the certificate or fingerprint before MARS can establish the desired communications each time the certificate or fingerprint changes. During changes, the internal log includes the username of the account used to accept the change. If the communication times out before administrative intervention, the communication fails and an internal system log records the failure to accept the changed certificate or fingerprint.

The implication of each option varies based on which MARS service is attempting the connection, not in the enforcement of the option, but in the ability of the service to prompt for immediate administrative intervention. In other words, if the service is a GUI-based services, you will be prompted to accept the changed certificate or fingerprint. If the service is a backend service, the communications with the target device will fail and the event will be logged.

The following services and operations are affected by the global certificate/fingerprint response setting:

- Upgrade (SSL). When MARS uses the HTTPS option to download the upgrade package from the remote server specified on the Admin > System Maintenance > Upgrade page.
- Discovery operation. (SSH)
- Test Connectivity operation. (SSL)
- Cisco IDS, IPS, and IOS IPS router Event Processing (RDEP or SDEE over SSH)
- CSM Policy Query Integration (SSL)
- Qualys Report Discovery. (SSL)
- Graphgen process for mitigation operation (SSH and SSL)
- Device Monitor process for resource monitoring feature (SSH)

Setting the Global Certificate and Fingerprint Response

The default response is to accept the certificate or fingerprint the first time MARS attempts to connect to the device, after which if a conflict is detected, then administrative intervention is required to update to the new certificate or fingerprint.

If this option is not the one that you wish to use, you can select from three options. The global setting for the conflict detection responses is located on the Admin > System Parameters > SSL/SSH Settings page.

To change the default certificate and fingerprint response, follow these steps:

-
- Step 1** Log in to the web interface using an account with Administrative privilege.
- Step 2** Click the **Admin > System Parameters > SSL/SSH Settings** tab.
- Step 3** Select one of the following options to define the global behavior that you require:
- Automatically always accept
 - Accept first time and prompt when changed
 - Always prompt on new and changed
- For details on these options, see [Understanding Certificate and Fingerprint Validation and Management, page 13-7](#).
- Step 4** Click **Submit**.
-

Upgrading from an Expired Certificate or Fingerprint

If you have selected a global response option other than Automatically always accept (see [Setting the Global Certificate and Fingerprint Response, page 13-8](#)), you will at some time be required to update an expired certificate or fingerprint.

Two options exist for upgrading from an expired certificate or fingerprint. If you are logged in to the web interface when a GUI process detects a certificate or fingerprint conflict, you will be prompted to accept or reject the new value. Otherwise, if you are not logged in or a backend process detects the conflict, you must manually initiate a communication with the device. To determine the list of devices for which you must manually update the certificates or fingerprints, review the Activity: CS-MARS Detected Conflicting Certificates/Fingerprints report (see [Monitoring Certificate Status and Changes, page 13-10](#)).

The following procedures explain how to upgrade under the specific circumstances:

- [Upgrade a Certificate or Fingerprint Interactively, page 13-9](#)
- [Upgrade a Certificate Manually, page 13-9](#)
- [Upgrade a Fingerprint Manually, page 13-10](#)

Upgrade a Certificate or Fingerprint Interactively

An interactive upgrade refers to responding to a web interface prompt to update the certificate. This type of upgrade is available when you are logged into the GUI and a process, such as graphgen, prompts you to upgrade a certificate or fingerprint that conflicts with the previously accepted value. Click **Yes** to accept the new fingerprint or certificate.

Upgrade a Certificate Manually

A manual upgrade allows you to upgrade any certificate at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade to a new certificate, follow these steps:

-
- Step 1** Log in to the web interface using an account with Administrative privilege.
- Step 2** Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a certificate conflict. and click **Edit**.
- Step 3** Click **Test Connectivity**.
The dialog box displays stating “Do you want to accept following certificate for the device named: <device_name>?”.
- Step 4** Verify the certificate value.
- Step 5** If the value is correct. click **Yes**.
-

Upgrade a Fingerprint Manually

A manual upgrade allows you to upgrade any fingerprint at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade a fingerprint, follow these steps:

-
- Step 1** Log in to the web interface using an account with Administrative privilege.
- Step 2** Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a fingerprint conflict and click **Edit**.
- Step 3** Click **Discover**.
The dialog box displays stating “Do you want to accept following fingerprint for the device named: <device_name>?”.
- Step 4** Verify the fingerprint value.
- Step 5** If the value is correct, click **Yes**.
-

Monitoring Certificate Status and Changes

To support the certificate management features in MARS, the following system inspection rule exists:

- **System Rule: CS-MARS Failure Saving Certificates/Fingerprints.** This inspection rule indicates that MARS has failed to save a new or changed device SSL certificate or SSH key fingerprint based on either explicit user action or automatic accept as specified on the SSL/SSH Settings page.

In addition, the following reports appear under the System: CS-MARS Issue category.

- Activity: CS-MARS Accepted New Certificates/Fingerprints
- Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints
- Activity: CS-MARS Detected Conflicting Certificates/Fingerprints
- Activity: CS-MARS Accepted New Certificates/Fingerprints'
- Activity: CS-MARS Failure Saving Certificates/Fingerprints
- Activity: CS-MARS Device Connectivity Errors

Database Tuning and Query Optimization

When you run a query from the MARS GUI and specify a large time range, it may take a long time to complete the query even though the returned results may include only a few entries. Such long-term queries require the database to perform a full table scan, even when you employ query filters.

To vastly improve the speed of query execution, we recommend that you create and employ database indexes of the filtering columns. Database query performance, of course, still depends on the amount of data that must be returned, and a query that returns thousands of rows of data will still take significantly longer than a query that returns only dozens of rows.

The performance improvement achieved is not subject to the number of indexes created, rather, the degree of performance improvement is subject to the following three conditions:

- The query has at least one filter
- All the filters are indexed (the number of filters do not matter, one filter may be as good as many filters)
- The query returns a small amount of data after the filtering.

About Database Indexing

Although a series of database indexes can significantly improve response time, creating additional indexes can also, depending on the particular circumstances, have the reverse effect. To effectively optimize query operations, MARS helps to determine the nature and scope of database indexing you should perform.

MARS stores security events in 10 database tables, *pn_event_session_0*, ..., *pn_event_session_9*. Each of the tables is about the same size, and the size is predefined based on the CS-MARS model. A MARS-25, for example, has approximately 70 percent fewer rows in each table than a MARS-55. When the current table is full of data, the system truncates the table that contains the oldest data and starts storing data there.

An index is a special database table that stores the location of particular data in a database table. Looking up an entry in the index table is usually faster because it is organized, while looking up an entry directly from the data table is sequential and usually much slower.

MARS employs both bitmap and B-tree indexes. Bitmap indexes are preferred when the cardinality of a database table column is low. Cardinality expresses the number of distinct values in a column. For example, a column that held only *true/false* values would have a cardinality of 2 and would be a prime candidate for a bitmap index. For this reason, proper database indexing begins with determining the cardinality of all database columns.



Note

B-tree indexes use many more system resources and may severely impact system performance. Use B-tree indexing prudently when the index is not recommended, and drop the index if you find it impacts your system performance.

Keep the following considerations for database optimization in mind:

- Calculating the cardinality is best done on a full table.
- You should only have to calculate cardinality once or twice a year.
- Calculate cardinality before creating indexes.

- Create indexes on columns that best reduce the scope of the data returned.
- Monitor system performance and test queries using the indexed columns as filters.
- Drop an index if you find it degrades system performance. (A dropped index can always be reactivated.)
- Keep an index, even if it is rated as “Not Recommended,” if you determine it works well.

Understanding the Data Indexing/Query Optimization Page

The Data Indexing/Query Optimization page, which you can view by selecting **Admin > System Maintenance > Database Tuning / Query Optimization**, enables you to view index configuration information and to perform index-related functions.

Figure 13-3 shows the Data Indexing/Query Optimization page of the System Maintenance tab.



Note

The table on the Data Indexing/Query Optimization page presents each database table column that can be indexed on a separate row.

The screenshot shows the Data Indexing/Query Optimization page for a Cisco Security MARS Local Controller. The page includes a navigation bar at the top with tabs like System Setup, System Maintenance, User Management, System Parameters, and Custom Setup. Below the navigation bar, there's a section for 'Index Configuration Information' with a 'Page Refresh Rate' dropdown set to 5 minutes. A table lists various index columns with their status, schedule tasks, cardinality, last sampling date, and recommendations. The table has columns: Index Column, Status, Schedule Task, Index Cardinality, Last Sampling Date, and Recommendation. The rows include Source IP, Source Port, Destination IP, Destination Port, Protocol, Event Type, Reporting Device, and Reported User. The 'Recommendation' column shows 'Recommended' for most, but 'Not Recommended' for Destination Port. At the bottom, there are buttons for 'Calculate Cardinality', 'Create Index', 'Drop Index', and 'Cancel Task'.

Index Column	Status	Schedule Task	Index Cardinality	Last Sampling Date	Recommendation
Source IP	Index Active	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:07:49 PDT 2009	Recommended
Source Port	Index Active	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:07:49 PDT 2009	Recommended
Destination IP	Index Inactive	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:07:49 PDT 2009	Recommended
Destination Port	Index Active	Schedule 5/5/2009 6:25 AM Run Now	50K (sample base: 270005686 row(s))	Fri Mar 27 23:11:46 PDT 2009	Not Recommended
Protocol	Index Active	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:11:48 PDT 2009	Recommended
Event Type	Index Inactive	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:15:38 PDT 2009	Recommended
Reporting Device	Index Active	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:19:29 PDT 2009	Recommended
Reported User	Index Inactive	Schedule 5/5/2009 6:25 AM Run Now	OK (sample base: 270005686 row(s))	Fri Mar 27 23:23:31 PDT 2009	Recommended

Figure 13-3 Data Indexing/Query Optimization Page

1	Index Column: Lists which database columns can have indexes created.	2	Status: For a each index column, indicates index status. Displays a green, square, check icon for active indexes or a black, round, X icon for inactive indexes.
3	Schedule Task: For a each index column, two radio buttons enable you to determine whether an operation on an index is scheduled or run immediately. Four date and time fields enable you to specify schedule time.	4	Index Cardinality: For a each index column, displays the size of the last sampled cardinality in thousands and, in parentheses, displays the sample base size.
5	Last Sampling Date: For a each index column, displays the date of the most recent cardinality calculation sampling.	6	Recommendation: For a each index column, indicates recommendations for whether a particular index: • <i>should be</i> activated (green, thumb up icon with text reading “Recommended”), or • <i>may be</i> activated (green, thumb up icon with the text "Not Ideal"), or • <i>should not be</i> activated (red, thumb down icon).
7	Calculate Cardinality Button: Clicking this button requests that cardinality calculations be performed on the selected database columns, either immediately, or by the specified schedule.	8	Create Index Button: Clicking this button requests that the selected database columns be indexed (or re-indexed), either immediately, or by the specified schedule.
9	Drop Index Button: Deletes selected index.	10	Cancel Task Button: Cancels requested actions on the selected database columns.

The performance of an indexed database to a query depends on three factors:

- At least one filter is employed
- The filter(s) used is indexed
- The query returns a small of amount of data after the filtering

Data Indexing/Query Optimization Procedures

Procedures that you perform from the Data Indexing/Query Optimization page include the following:

- [Calculate Cardinality, page 13-14](#)
- [Create Database Index, page 13-14](#)
- [Schedule Database Optimization, page 13-15](#)
- [Drop Index, page 13-15](#)

Calculate Cardinality

You can calculate the cardinality of any database table column to better understand whether that column is suitable for bitmap indexing. This calculation also helps the system determine the best type of index to create (cardinality values less than a few thousand typically employ a bitmap index and larger cardinality values dictate the use of a B-tree index.) This operation can be scheduled to run during off-peak hours to minimize system impact.

Keep the following considerations in mind:

- Calculating the cardinality is best done on a full table.
- You should only have to calculate cardinality once or twice a year.



Warning

To prevent overwhelming system resources, you should always calculate a database column's cardinality prior to creating its index.

To calculate a database column's cardinality, follow these steps:

- Step 1** Log in to the web interface using an account with Administrative privilege.
- Step 2** Click the **Admin > System Maintenance > Database Tuning / Query Optimization**
The Index Configuration Information page appears.
- Step 3** Select the database columns for which you want to calculate cardinality by clicking to select their corresponding checkbox on the left of the table.



Tip

Typically you will want to calculate cardinality for all your indexes close to the same time. However, to lessen system impact, you may want to run a few calculations one night and the rest on the next night.

- Step 4** Select when to run the calculation by doing one of the following:
 - To run the calculation immediately, select the default, Run Now.
 - To schedule the calculation to run later, specify the time by selecting values for the date, hour, minute and AM/PM fields.



Tip

Clicking the blue calendar icon next to the date field simplifies selecting a date. Alternatively you can enter a date in mm/dd/yyyy format.

- Step 5** Click Calculate Cardinality.

Create Database Index

Any database column that you use to perform queries should be indexed.

- Step 1** Log in to the web interface using an account with Administrative privilege.
- Step 2** Click the **Admin > System Maintenance > Database Tuning / Query Optimization**
The Index Configuration Information page appears.
- Step 3** Select the database columns for which you want to create an index by clicking to select their corresponding checkbox on the left of the table.

**Tip**

Typically you will want to create your indexes at close to the same time. However, to lessen system impact, you may want to create your indexes one at a time and on weekends.

Step 4 Select when to create the index by doing one of the following:

- To create the index immediately, select the default, Run Now.
- To schedule the index creation to run later, specify the time by selecting values for the date, hour, minute and AM/PM fields.

**Tip**

Clicking the blue calendar icon next to the date field simplifies selecting a date. Alternatively you can enter a date in mm/dd/yyyy format.

Step 5 Click Create Index.

Schedule Database Optimization

This procedure enables you to schedule the update of one or more database tables. To lessen system impact, you may want to optimize your indexes one at a time and on weekends.

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select a database column for which you want to schedule an update.

**Tip**

If you previously scheduled a particular index for optimization, eliminate that task request by selecting that index and clicking Cancel Task.

Step 4 Specify a time by selecting values for the date, hour, minute and AM/PM fields.

Step 5 Click Create Index.

Step 6 Repeat [Step 3](#) through [Step 5](#) for each database column to be updated.

Drop Index

Too many active indexes can cause system performance issues and impact the event rate. The system warns you of this when you have compiled three database indexes or more. When you find an index affects your system's performance, you should drop it.

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select the checkbox of any database column whose index status is listed as Index Active.

Step 4 Select when to drop the index by doing one of the following:

- To drop the index immediately, select the default, Run Now.
- To schedule the index to be dropped later, specify the time by selecting values for the date, hour, minute and AM/PM fields.

Step 5 Click Drop Index.



CHAPTER 14

Authenticating MARS Accounts with External AAA Servers

Revised: April 5, 2007

External Authentication, Authorization, and Auditing (AAA) servers can act as the authentication mechanism for MARS Appliance GUI logins (username and password). This permits authentication and centralized password management for all MARS Appliances.

Table 14-1 *Feature History for MARS Appliance AAA Authentication Method*

Release	Modification
4.3.1 and 5.3.1	This feature was introduced.

This chapter describes the Authentication, Authorization and Accounting (AAA) feature for the MARS Appliances and includes the following sections:

This chapter contains the following topics:

- [Information About Authenticating MARS User Accounts with External AAA Servers, page 14-1](#)
- [Procedure for First-time Configuration of MARS AAA Feature, page 14-9](#)
- [Edit an External AAA Server, page 14-15](#)
- [Delete an External AAA Server, page 14-16](#)
- [Unlock an Account after Login Failure, page 14-16](#)

Information About Authenticating MARS User Accounts with External AAA Servers

The administrator can configure MARS to authenticate GUI login attempts with an external AAA server, or with the default method of authenticating to the appliance's local database.

This section contains the following topics:

- [Supported AAA Protocols and Servers, page 14-2](#)
- [Configuration Overview, page 14-2](#)
- [Global Controller Considerations with External AAA Servers, page 14-3](#)
- [Failed Authentication Lockout \(Login Failure\), page 14-4](#)

- [System Events related to Authentication and Login Attempts, page 14-4](#)
- [System Reports and Rules Related to Authentication Method, page 14-8](#)

Supported AAA Protocols and Servers

The AAA protocol used by MARS is a basic Remote Authentication Dial In User Service (RADIUS) protocol. The supported external RADIUS servers are as follows:

- [Cisco Secure Access Control Server \(ACS\) for UNIX](#)
- [Cisco Secure Access Control Server \(ACS\) for Windows](#)
- [Microsoft Internet Authentication Service \(IAS\) Server](#)
- [Juniper Steel belted RADIUS](#)

Configuration Overview

The following overview describes the Local Controller. Global Controller differences are discussed in the section [“Global Controller Considerations with External AAA Servers”](#) section on page 14-3.

Summary of MARS Appliance AAA Configuration Tasks

1. Create user accounts on the MARS Appliances.

On each MARS Appliance to which a user must have access, the MARS administrator must create a user account for that user (contact information, group permissions and role). The account can be created on the Local Controller or on a Global Controller and pushed to the Local Controller.

2. Configure all MARS Appliances to use AAA authentication method.

Each MARS Appliance must be individually configured to run the AAA authentication method. From the AAA Configuration page (**Admin > System Setup > Authentication Configuration**), manually add external AAA servers in a procedure similar to that of adding a software security application on a new host.

Up to three AAA servers can be selected for AAA server authentication. They are named the primary, secondary, and tertiary servers, which signifies their rank in the AAA server failover sequence.



Note

When the administrator changes the MARS authentication method from Local to AAA, all passwords from accounts other than administrator, are deleted from the local user profiles. When changing from AAA to Local, the MARS administrator must recreate passwords for each local account.

When the MARS Appliance operates with the AAA authentication method, every login except the administrator accounts are authenticated by the external AAA server.

All authentication method changes, successful logins, and failed logins are captured as event messages.

Summary of AAA Server Configuration Tasks

1. Configure the MARS Appliance as an AAA client of the AAA server.
2. The AAA server administrator must create the MARS user accounts in the external AAA servers to provide only login name/password authentication for each MARS user.

See the user guide of your AAA server for details.

Global Controller Considerations with External AAA Servers

The following constraints and recommendations pertain to using the AAA authentication method with a Global Controller:

- **Global and Local Accounts for the Same User**

Using the Local authentication method, a user can have two accounts with the same login name and different passwords on a single appliance, for example, global:person1 created on the Global Controller and pushed to the Local Controller and local:person1 created on the Local Controller. Because the AAA server has only one password per login name, do the following to maintain the Local method functionality with the AAA method:

- Use the same password for both the global and local accounts.
- Use different AAA servers to authenticate the global and local login names.

- **Changing Global Controller to AAA Authentication Method**

Configuring AAA Authentication Method on a Global Controller is similar to configuring AAA on a Local Controller, except that AAA servers cannot be added, edited or deleted on a Global Controller. The list of available AAA server names in the GUI is populated from the Local Controllers reporting to the Global Controller. The hostname of the reporting Local Controller is prepended to the AAA server name. The Global Controller should use an AAA server from the closest Local Controller on the network.

- **Use the same Authentication Method for all Global and Local Controllers**

To avoid login problems, the optimal scenario is to have all Local Controller and Global Controllers use the same authentication method, either all Local or all AAA. For example, when a Global Controller uses AAA method, and a Local Controller uses Local method, any global user accounts pushed to the Local Controller will not have passwords. Any login attempt by the global user to that Local Controller fails until the administrator configures a password for the global account.

- **Setup accounts for Global Controller Users in all AAA servers used by Local Controllers**

When a Global Controller and a Local Controller use different AAA servers for authentication the Global Controller login name and password must be configured in one of the Local Controller's AAA servers or the Global Controller user cannot log in to the Local Controller.

- **Deleting AAA servers on Local Controllers**

If a Local Controller deletes the AAA server in use by a Global Controller, the Global Controller is automatically switched to Local authentication. To reestablish AAA authentication for the Global Controller, the administrator must reconfigure the Global Controller to AAA authentication method and select another AAA server.

Just before a Local Controller being deleted from a Global Controller, a warning message appears if it is the Local Controller with the AAA server to which the Global Controller authenticates.

- **Unlocking Accounts**

Unlocking is not replicated through Global Controller-Local Controller communications, it applies only to the local appliance. An account locked on a Global Controller does not replicate the locked status to global accounts on Local Controllers. A global account locked on two different appliances must be unlocked manually on each appliance.

Failed Authentication Lockout (Login Failure)

For both Local or AAA authentication methods, GUI access is prevented (locked) for an account upon login failure, which occurs when a specified number of incorrect password entries are made for a single login name.

The maximum number of password attempts before locking is set by the Maximum Login Failures parameter in the Account Lockout Policy box of the AAA configuration page (**Admin > System Setup > Authentication Configuration**). The default setting is 5 attempts. By setting the Account Lockout Policy to **Never Lock**, the administrator can disable GUI locking for all accounts, but not specific accounts.

The count of incorrect attempts before login failure clears only when a successful login occurs, it does not age out. For example, if a user performs two incorrect password attempts then quits for the day, they must succeed on the first attempt the next morning or the account will be locked. A running session does not terminate if a login failure occurs for the same user account attempting to open another session, but the account will be locked to all future login attempts.

Once locked, an account must be unlocked by the MARS administrator. The **Admin > User Management** page of the GUI displays locked accounts. The Status column indicates if the account is **active**, **locked** or **password expired**. An administrator can unlock accounts from the User Management page by selecting the accounts and clicking **Unlock**.



Note

An account password expires when the authentication method is changed from Local to AAA then back to Local, because the initial change from Local to AAA erased all the passwords of the non-administrative local accounts. The passwords must be reset by editing each account from the User Management page.

The CLI access through the console or through SSH is never locked. The **unlock** CLI command can unlock GUI access for some or all accounts. This is the recourse when the administrator is locked out from the GUI. For information on the **unlock** command, see the [Cisco Security MARS Command Reference](#).

System Events related to Authentication and Login Attempts

[Table 14-2](#) lists events triggered by Local and AAA authentication method actions.

Table 14-2 **MARS AAA-related Events**

Event	Raw Messages
CS-MARS admin user login success	GUI Raw message: % MARS-3-400001 CS-MARS GUI login successful for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication GUI Raw message: % MARS-3-400001 CS-MARS GUI login successful for admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>
CS-MARS admin user login failure	GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using AAA, reason: user information is not verified in local DB GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>, reason: invalid user or password
CS-MARS non-admin user login success	GUI Raw message: %MARS-3-400003 CS-MARS GUI login successful for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication" GUI Raw message: %MARS-3-400003 CS-MARS GUI login successful for non-admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>

Table 14-2 MARS AAA-related Events (Continued)

CS-MARS non-admin user login failure	GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using AAA authentication, reason: user information is not verified in local DB GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>, reason: invalid user or password
CS-MARS failed to connect to AAA server	GUI Raw message: %MARS-2-400005 CS-MARS GUI failed to connect to AAA server at: <aaa-ip> for authenticating admin user 'username(CS_MARS_LC)@LC42', reason: <reason-string> GUI Raw message: %MARS-2-400005 CS-MARS GUI failed to connect to AAA server at: <aaa-ip> for authenticating non-admin user 'username(CS_MARS_LC)@LC42', reason: <reason-string>
CS-MARS pndadmin user password changed	GUI raw message: %MARS-2-401001 CS-MARS 'pndadmin(CS_MARS_LC)@LC42' user password has changed from GUI at <src-ip> CLI raw message: %MARS-2-401001 CS-MARS 'pndadmin(CS_MARS_LC)@LC42' user password has changed from CLI at <src-ip>
CS-MARS pndadmin user password remains default	raw message: '%MARS-2-401002 CS-MARS 'pndadmin(CS_MARS_LC)@LC42' user password remains default for the past 24 hours

Table 14-2 **MARS AAA-related Events (Continued)**

CS-MARS admin user account locked	Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with local authentication Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication at server: <aaa-ip> Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication but failed in local user verification
CS-MARS admin user account unlocked	GUI Raw message: %MARS-3-402003 CS-MARS unlocked admin user account 'username(CS_MARS_LC)@LC42' from GUI by admin user 'adminuser(CS_MARS_LC)@LC42' while logged in from: <src-ip> CLI Raw message: %MARS-3-402003 CS-MARS unlocked admin user account 'username(CS_MARS_LC)@LC42' from CLI by admin user 'padmin(CS_MARS_LC)@LC42' while logged in from: <src-ip>
CS-MARS non-admin user account unlocked	Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with local authentication Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication at server: <aaa-ip> Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication but failed in local user verification

Table 14-2 MARS AAA-related Events (Continued)

CS-MARS unlocked all accounts	CLI raw message: %MARS-3-402005 CS-MARS unlocked all accounts while logged in from: <src-ip>
CS-MARS Authentication method changed from Local to AAA	GUI raw message: %MARS-2-403001 CS-MARS Authentication method was changed from Local to AAA by admin user 'username(CS_MARS_LC)@LC42' while logged in from: <src-ip>
CS-MARS Authentication method changed from AAA to Local	GUI raw message: %MARS-2-403002 CS-MARS Authentication method was changed from AAA to Local by admin user 'username(CS_MARS_LC)@LC42' while logged in from: <src-ip>

System Reports and Rules Related to Authentication Method

For descriptions of MARS reports and rules, please see [Appendix E, “System Rules and Reports.”](#)

System Reports

The following six reports disclose authentication events. All the reports are custom column, run on-demand only, with a time range of 1 day.

- Activity: CS-MARS Login Failures
- Activity: CS-MARS Successful Logins
- Activity: CS-MARS Accounts Locked
- Activity: CS-MARS Accounts Unlocked
- Activity: CS-MARS Authentication Method Modifications
- Activity: CS-MARS padmin User Password Status

System Rules

The following three rules capture authentication method configuration actions:

- System Rule: CS-MARS Authentication Method Modified - AAA to Local
- System Rule: CS-MARS Login Failures - Admin User
- System Rule: CS-MARS Login Failures - Non-Admin User

The following system rule is triggered depending on how events are grouped:

- System Rule: Vulnerable Host Found (Event: CS-MARS padmin user password remains default)

Because MARS login successes and failures are grouped into event groups the following rules could fire if a MARS Local Controller is also the target of attacks described in each of the following rules:

- System Rule: Local Attack - Attempt
- System Rule: Local Attack - Success Likely
- System Rule: Password Attack: System - Attempt

- System Rule: Password Attack: System - Success Likely
- System Rule: Password Attack: System - Success Likely

Login events groups—Info/SuccessfulLogin/System/Root, Info/SuccessfulLogin/System/Non-root, Penetrate/GuessPassword/System/Root and Penetrate/GuessPassword/System/Non-root

Procedure for First-time Configuration of MARS AAA Feature

This procedure demonstrates a first-time configuration of AAA Authentication method for a MARS Appliance.

Summary of steps:

1. Add a new external AAA Server
2. Select AAA Authentication
3. Configure Account Lockout Policy (optional)

Before You Begin

The following prerequisites are required to configure the AAA authentication method:

- User profiles created in each MARS Appliance (role and contact involver each intended user)
- MARS configured as an AAA client on the external AAA server



Tip

For the Cisco Secure ACS, MARS must be configured as an AAA client. You may choose any vendor-specific attribute (VSA) configuration that uses port 1812 as an authentication port and port 1813 as an accounting port. We recommend the Cisco VPN3000/ASA/PIX 7.x+ VSA. For further information see the [User Guide for Cisco Secure Access Control Server 4.1](#).

- MARS user accounts created in the external AAA server to provide only login name/password authentication



Note

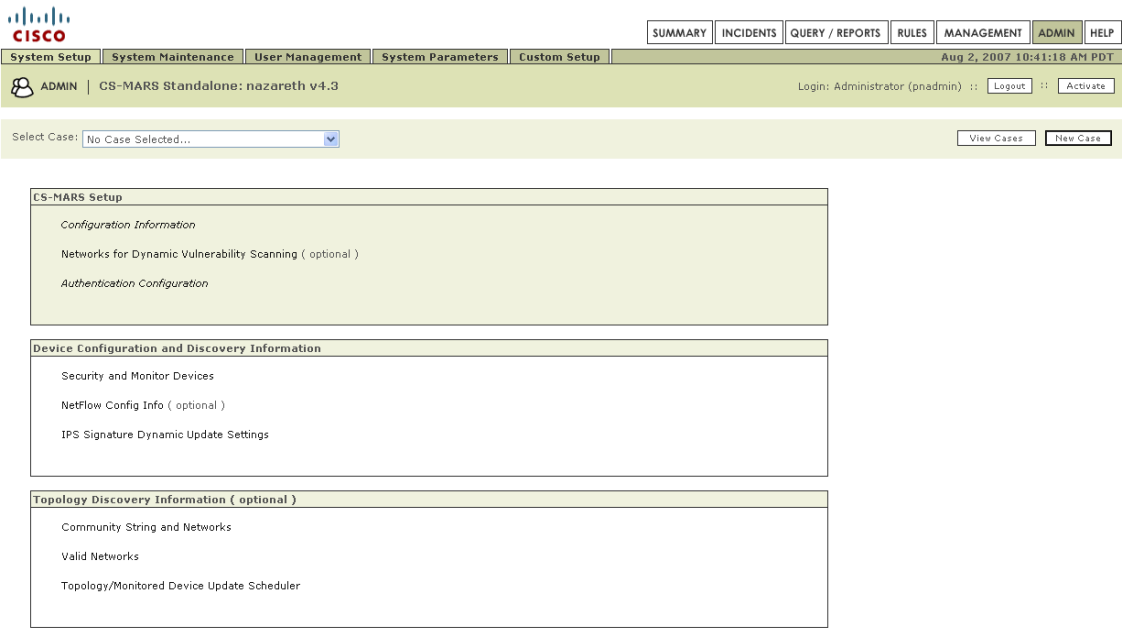
The MARS Appliance login name is case-sensitive, the Cisco Secure ACS User Setup username is not. For example, the MARS login names Victor, victor, and VICTOR will match the Cisco Secure ACS username “victor.” Thus, three MARS users could share the same password. We recommend that there be a one-to-one correspondence of MARS login names to Cisco Secure ACS usernames.

- (Local Controller only) AAA server configuration information required by MARS as follows:
 - Access and Reporting IP addresses
 - Interface addresses
 - Shared secret string
 - Authentication port (default is 1812)
 - Accounting port (default is 1813)

To configure the MARS AAA Feature, follow these steps:

- Step 1** Click the **Admin** tab to navigate to System Setup page.

Figure 14-1 Admin > System Setup Page



Step 2 Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 14-2](#). If you are configuring a Global Controller, please skip to [Step 10](#).

Figure 14-2 AAA Configuration Page

The screenshot displays the AAA Configuration page within the Cisco MARS web interface. The top navigation bar includes links for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The breadcrumb trail shows System Setup > System Maintenance > User Management > System Parameters > Custom Setup. The user is logged in as ADMIN, and the system is identified as CS-MARS Standalone: nazareth v4.3. The date and time are Aug 2, 2007 11:09:15 AM PDT. A 'Select Case' dropdown is set to 'No Case Selected...'. The 'Authentication Method' section has 'Local' selected, with 'AAA Server' as an alternative. The 'AAA Server Configuration' section features a dropdown menu and buttons for 'Edit', 'Delete', and 'Add'. The 'Account Lockout Policy' section shows 'Maximum Login Failures' set to 5. At the bottom, there are 'Back' and 'Submit' buttons.

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

250321

Add an external AAA Server

Step 3 Click **Add** in the AAA Server Configuration box.

The Add Reporting Device page appears, as shown in [Figure 14-3](#).

Figure 14-3 Add Reporting Device Page

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Add AAA server on new host

General Reporting Applications

→ *Device Name:

→ *Access IP:

→ Reporting IP:

→ Operating System: Generic

→ NetBIOS Name:

→ Monitor Resource Usage: NO

Enter interface information:

Name: IP Address: Network Mask:

☐ ether0

Step 4 Type in the configuration information and click **Next**.

The reporting application dialog appears as shown in [Figure 14-4](#).

The usage guidelines for the configuration fields are equivalent to those for adding a monitoring device.



Note The Done and Apply buttons are used when editing a configuration, not in a first-time configuration. Clicking Done returns you to the AAA Configuration page.

Figure 14-4 Reporting Application Dialog

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Edit host with security applications

General Reporting Applications

Enter reporting application:

→ Device Name: ACS Server

→ Select application: Generic AAA Server

Step 5 Select **Generic AAA Server** and then click **Add**.

The AAA Server Configuration pop-up window appears, as shown in [Figure 14-5](#).

Figure 14-5 AAA Server Configuration Pop-up Window


Aug 2, 2007 1:36:58 PM PDT

Standalone: nazareth v4.3 Login: Administrator (pnadmin) :: [Close](#)

AAA Server Configuration:

Name:	
Shared Secret:	
Authentication Port:	
Accounting Port:	

[Test Connectivity](#) [Cancel](#) [Submit](#)

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

250324

Step 6 Enter AAA Server configuration information.

The default authentication and authorization port is 1812.

The default accounting port is 1813.

Step 7 Click **Test Connectivity**.

A pop-up window appears for success or failure, as shown in [Figure 14-6](#) and [Figure 14-7](#).



Note The AAA Server Configuration field values are provided by the AAA server administrator.

Figure 14-6 Connectivity Succeeds Pop-up Window

Feb 8, 2007 4:45:31 PM PST

Standalone: erebus v0.0 Login: Administrator (pnadmin) :: [Close](#)

Connection to AAA server succeeded!

Input user name and password to check authentication:

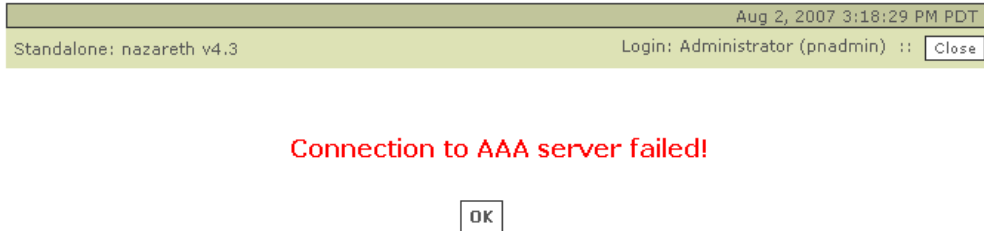
User Name:	
Password:	

[Cancel](#) [Submit](#)

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

[Feedback](#)

250325

Figure 14-7 Connectivity Fails Pop-up Window

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

250326

- Step 8** If the connectivity test succeeds, enter any User Name and Password configured for MARS on the AAA server and click **Submit** to verify that the added external AAA server correctly authenticates you to the MARS account.

You are returned to the AAA Configuration Page, as shown in [Figure 14-2](#).

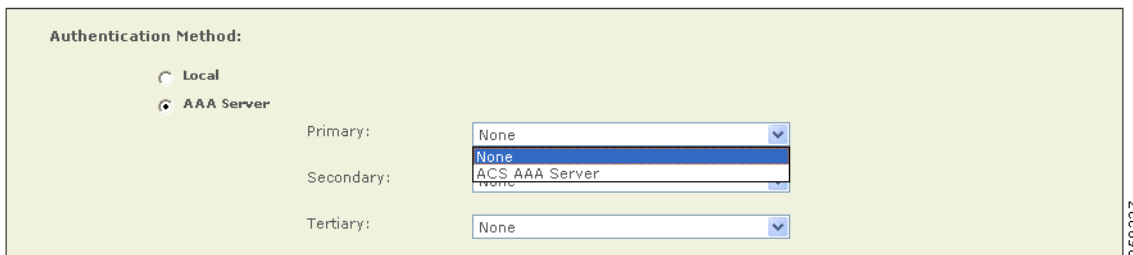
If the connectivity fails, you are returned to the AAA Server Configuration Pop-up Window, as shown in [Figure 14-5](#). Troubleshoot the AAA server connection until connectivity succeeds.

- Step 9** Add Secondary or Tertiary AAA servers per your administrative requirements.

Select AAA Authentication

- Step 10** In the Authentication Method box of the AAA Configuration Page, click the **AAA Server** radio button, and select your primary AAA server from the drop-down list. Select secondary and tertiary servers as appropriate to your network.

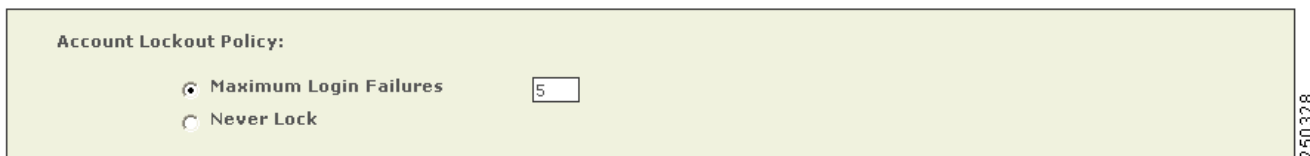
If you are configuring a Global Controller, select the AAA server closest to the Global Controller.

Figure 14-8 Select Newly-added AAA Server From Drop-down List

250327

Configure Account Lockout Policy (optional)

In the Account Lockout Policy box, configure the maximum login failures threshold, or click the Never Lock radio button.

Figure 14-9 Maximum Login Failure Parameter

250328

Step 11 Click **Submit**.

When the authentication method is changed from Local to AAA Server, all user passwords are removed from the MARS local database (except administrators). If you change the authentication method back to Local from AAA Server, you must reconfigure all the user passwords with the MARS GUI (Management > User Management).

When the MARS authentication is set to AAA server mode, user passwords can not be added or edited on the MARS User Management page.

End of [Procedure for First-time Configuration of MARS AAA Feature, page 14-9](#).

Edit an External AAA Server

Step 1 Click the **Admin** tab to navigate to System Setup page.

Step 2 Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 14-2](#).

Step 3 In the AAA Server Configuration box, select the external AAA Server to edit.

Step 4 Click **Edit**. The Edit Server page appears, as shown in [Figure 14-10](#).

Figure 14-10 *Edit Server Page*

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Edit host with security applications

Step 5 Click the checkbox of the Device Type to change then click **Edit**. The Server Configuration pop-up window appears, as shown in [Figure 14-5](#).

Step 6 Make changes, click **Test Connectivity**.

Step 7 If the connectivity test succeeds, enter your User Name and Password and click **Submit** to verify that the added external AAA server correctly authenticates you to your MARS account.

You are returned to the AAA Configuration Page, as shown in [Figure 14-2](#).

If the connectivity fails, you are returned to the AAA Server Configuration Pop-up Window, as shown in [Figure 14-5](#). Troubleshoot the AAA server connection until connectivity succeeds.

Step 8 Click **Submit**. You are returned to AAA configuration page.

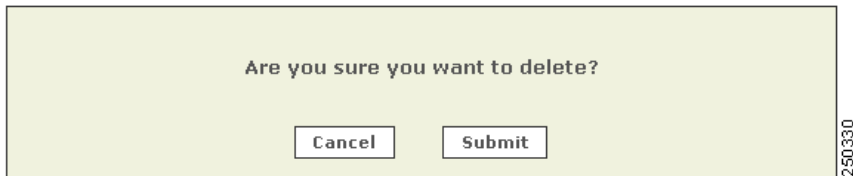
End of [Edit an External AAA Server, page 14-15](#).

Delete an External AAA Server

- Step 1** Click the **Admin** tab to navigate to System Setup page.
- Step 2** Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 14-2](#).
- Step 3** In the AAA Server Configuration box, select the external AAA Server to delete.
- Step 4** Click **Delete**. A delete confirmation pop-up window appears, as shown in [Figure 14-11](#).

Figure 14-11 Server Delete Confirmation

Application: Generic AAA Server



- Step 5** Click **Submit**. You are returned to AAA configuration page.
If the AAA server deleted is a primary server used by a Global Controller, The Global Controller automatically switches to the Local authentication method and the administrator must reconfigure the Global Controller to AAA method and select another AAA server as required.

End of [Delete an External AAA Server, page 14-16](#).

Unlock an Account after Login Failure

The following procedure details the steps required to unlock a non-administrative Local Controller or Global Controller account. To unlock an administrative account, use the **unlock** CLI command, as described in the [Cisco Security MARS Command Reference](#).

A login failure to the MARS GUI is signaled by the Login Failure message, as shown in [Figure 14-12](#).

Figure 14-12 Login Failure Message


Login Failure
(less info)

Potential Login Failure Reasons:

1. Incorrect Login or Password
2. Connection to AAA server failed
3. Account Locked due to too many failed login attempts
4. Account Locked due to switching authentication methods

Please try again or contact system administrator

Login Name:

Password:

Type: Local ▼

Login

Step 1 Log in to an administrator account.

Step 2 Navigate to the User Management subtab (**Management > User Management**), as shown in [Figure 14-2](#).

The status column indicates which accounts are locked.

Click the check box of the user accounts to unlock.

Figure 14-13 Unlocking a Locked User Account


[SUMMARY](#)
[INCIDENTS](#)
[QUERY / REPORTS](#)
[RULES](#)
[MANAGEMENT](#)
[ADMIN](#)
[HELP](#)

Aug 2, 2007 5:32:50 PM PDT

[Event Management](#)
[IP Management](#)
[Service Management](#)
[User Management](#)

CS-MARS Standalone: nazareth v4.3

Login: Administrator (pnadmin) :: [Logout](#) :: [Activate](#)

Select Case: No Case Selected... ▼

[View Cases](#) [New Case](#)

[Search](#)

[Edit](#) [Delete](#) [Add](#) [Unlock](#)

Select Group: All ▼

[Edit Group](#) [Delete Group](#) [Add Group](#)

User Name	Status	Login	Email	Role	Organization	Groups
☐ Administrator (pnadmin)	Active	pnadmin	admin@cisco.com	Admin	Cisco Systems, Inc.	Admin
☐ Analyst, Test (bink)	Active	bink		Security Analyst		Security Analyst
☒ Blauer, Fortz (fblauer)	Locked	fblauer	fblauer@capu.com	Operator	none	Operator, UserGroup Test
☐ Documentation, Guest (pndocs)	Active	pndocs		Admin		Admin
☐ Quick, Deletus	Active		bamm@gone.com		None	Notification
☐ Wu, xiaoli	Active		howl@rantor.com			Notification

[Edit](#) [Delete](#) [Add](#) [Unlock](#)

1 to 6 of 6 25 per page ▼

Step 3 Click **Unlock**. The status of the user account changes from Locked to Active.

User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x

OL-16777-02

14-17

End of [Unlock an Account after Login Failure, page 14-16](#).



CHAPTER 15

Monitoring Events from Custom and Unsupported Devices or Versions

Cisco Security Monitoring, Analysis, and Response System (MARS) provides native support for many Cisco and 3rd-party reporting devices and versions of software running on those devices. However, you may need to monitor the events generated by a home-grown application or an unsupported device. To support this ability, MARS allows you to define custom parsers, which represent reporting devices, and to define event types for parsing the SNMP TRAP or SYSLOG events received from those devices.

Beginning with MARS 6.0, these new custom parsing features are referred to as the Device Support Framework (DSF). With DSF you can quickly add support for new device types, improve support for existing device types, and replicate accomplished work from one CS-MARS appliance to another.

The following terms are used throughout this chapter:

- **audit event**—A predictable event that can be detected by a system and about which enough details exist to define a record about the event's occurrence. In this usage, *audit* simply indicates that the event is worthy of inclusion in an audit trail. Events are typically categorized as security, authorization, system, or network events.
- **audit record**—A record, such as a syslog message, SDEE event, or SNMP trap, generated by a system to detail the occurrence of a specific audit event.
- **device type** —A collection of device event types, event types, and event grouping definitions that represents a type of device or application (such as Cisco PIX 7.0) and parsing functions to parse events received from that type of device/application.
- **custom parser**—A feature that employs a user-provided definition of device event type, event type, event grouping and patterns, as well as pattern matching, to parse events from a device/application of the type defined. Currently, custom parsers are supported only for SNMP trap and syslog.
- **device event type**—A description of a specific event type generated by a device type. These event descriptions instruct the MARS parser on how to process the received events to extract the useful information. A device event type includes an event type mapping, match patterns, severity level settings, and a log ID. A device event type maps between the *audit record* and an existing or a newly created *event type*, and then to an event type group, which allows the device event type to be used in inspection rules, queries, and reports. Also known as *parser templates*.
- **event type**—The MARS-specific construct that collects similar device event types from all supported device types as well as similar common vulnerabilities and exposures (CVE) definitions. This normalized view shows the relationship among reported device type events and allows MARS to understand that a single activity has occurred although it could be reported as different device event types by multiple devices across the network.

Multiple device event types are normalized to an event type, as seen under Management > Event Management. On this page, you can select a group to see the normalized event type in the Event ID column, its name in the Description column, and the list of device event types that normalize to it under the Device Event ID column.

- **device support package**—A single package file that contains one or more device types, custom parsers, rules, and report data definitions.

When you define a custom parser, you must define a custom device type and event types. When you define an instance of a custom device type, you are defining a reporting device of that type under Admin > System Setup > Security and Monitoring Devices. You are required to specify the reporting method as either SNMP TRAP or SYSLOG. This designation determines the protocol MARS uses to listen for events from the reporting device.

To receive events from an unsupported reporting device, you must perform the following tasks:

1. Add a custom device or application type. See [Create a Device Type, page 15-7](#).
2. Add one or more device event type templates (log parser template). See [Create Device Event Types for a Custom Device Type, page 15-8](#).
3. Add a reporting device that is based on the custom device or application type definition. See [Add a Reporting Device based on a Custom Appliance Device Type, page 15-18](#) or [Add a Reporting Device based on a Custom Software Device Type, page 15-19](#).

This chapter contains the following topics:

- [Overview of the Device Support Framework, page 15-3](#)
 - [Specify the Provider Configuration, page 15-4](#)
 - [Checklist for Defining and Exporting a Device Support Package, page 15-5](#)
 - [Create a Device Type, page 15-7](#)
 - [Create Device Event Types for a Custom Device Type, page 15-8](#)
 - [Editing a Device Type, page 15-17](#)
 - [Overriding Existing Parsers, page 15-17](#)
 - [Extending Existing Device Types, page 15-18](#)
 - [Add a Reporting Device based on a Custom Appliance Device Type, page 15-18](#)
 - [Add a Reporting Device based on a Custom Software Device Type, page 15-19](#)
 - [Import a Device Support Package, page 15-20](#)
 - [Export a Device Support Package, page 15-24](#)
 - [Remove an Installed Device Support Package, page 15-28](#)
- [Events and Reports About Device Support Package Activities, page 15-28](#)
- [MARS Forum on NetPro: An Overview, page 15-31](#)
 - [Uploading a Device Support Package to the MARS Forum, page 15-31](#)
 - [Download a Device Support Package from the MARS Forum on NetPro, page 15-32](#)
 - [Subscribe to Package Sharing Page of the MARS Forum, page 15-33](#)
- [Example Custom Device Type: Custom Software Application, page 15-34](#)

Overview of the Device Support Framework

Beginning in release 6.0, MARS extends the custom parser feature support found in earlier versions, which allowed you to parse and inspect SNMP TRAP and SYSLOG events. Specifically, it enables the following new features:

- Extend existing device type parsers by adding new device event types and patterns for those new types.
- Support new event and signature data for existing device types by adding new device event types that use existing native parsers.
- Define new patterns that override native parsing functions of an existing device event type.
- Create a device type that inherits its device event types and parsers from an existing device type. The derived device type retains the Appliance or Software type property from its parent, which cannot be overridden.
- Assign custom event types to a system event type group so any rule, report, or query using that group will include the new custom event types.
- Import and export of custom parsers, rules, and reports as device type-specific packages from a Global Controller or a standalone Local Controller.

**Note**

An internal syslog message summarizes the provider and device data information about each import or export operation.

**Warning**

Import and export from a Local Controller is only allowed in standalone mode. Once the Local Controller is managed by a Global Controller, you can only import and export from the Global Controller.

Using these features, collectively called the *Device Support Framework*, you can quickly add support for new device types, improve support for existing device types, and replicate accomplished work on different MARS of one customer's MARS appliances, or share work among customers, partners, and vendors.

The device support framework extends the custom log parser feature to enable the following features:

- Add a device/application type
- Add device event type to a device/application type definition
- Derive a device/application type from an existing device/application type

**Note**

The child inherits any changes made to the parent, even after the child is defined.

- Add a device event type with or without pattern definitions for existing device types
- Assign custom event types to system or custom event type groups
- Add a reporting device based on the custom device type
- Edit an existing parser
- Import and export of custom parser
- Import and export of rules and reports

- Download and import customer parser, rules, and reports as device support packages from MARS forum on NetPro website.
- Protect exported device support packages with passwords to prevent unauthorized downloading and decryption.
- Remove custom device support packages

Specify the Provider Configuration

A *provider* attribute identifies the developer of any particular MARS support for a device type, including such elements as device type, device event type, event type, event type group, inspection rule, rule group, report, report group, and pattern type. This metadata is attached to any exported device support package, and it is rendered in the web interface when you review or import a device support package, or when provider information is available, such as when viewing device type, event type, or other provided element.

When defining a new provider, you can specify more meaningful values for the provider named *Local CS-MARS box*. When you export a custom device package from a MARS Appliance, it is the *Local CS-MARS box* provider information that is applied to that package, even if that package is derived from a device that was developed by Cisco.

To define a new provider, follow these steps:

Step 1 Click **ADMIN > Custom Setup > Provider Configuration**.

Step 2 Select the check box next to **Local CS-MARS box** entry, and click **Edit**.

Step 3 Specify values for the following required fields:

- **Provider Identifier**—A string value that, when combined with the Provider Name, uniquely identifies the provider.
- **Provider Name**—The name of the provider.

It is the combination of Provider Name and Provider Identifier that uniquely identify a provider.



Note

Before you can remove a provider, you must first delete all dependencies manually.

- **Display Name**—This name is the name used throughout the web interface. For example, it appears in the Provider column of pages that list device support packages.

Step 4 (Optional) Specify values for any of the following optional fields:

- **Address**—Identifies the postal address of the provider.
- **Phone Number**—Identifies the phone number of the provider.
- **Fax Number**—Identifies the fax number of the provider.
- **Email**—Identifies the e-mail address of the provider.
- **URL**—Identifies the company URL address of the provider.
- **Description**—Provides a description of the provider.

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

Checklist for Defining and Exporting a Device Support Package

When developing a new device support package, consider the following:

- **Prioritize events and effort**—Develop full custom device types for those event logs that are high severity and critical to be understood by MARS. The events in this subset require detailed regular expression parsing of the event. With non-critical events, you may be able to define keyword searches that identify the events clearly enough to be included in rules and reports.
- **Group to simplify maintenance**—Groups can simplify the definition of device types, such as IPS devices, that have a significant number of signatures or require periodic maintenance due to signature updates. Grouping is largely an abstract concept realized by mapping a device event type to a single event type or event type group. Based on the content of events, you can create groups of signatures that map to a smaller number of event types in MARS, where the event type represents the group of signatures. When the inspection rule or report fires in MARS, you can review the raw message for signature details. For example, you can create custom event types for each protocol or attack type as determined by the message data provided by the specific vendor.
- **Reuse existing event types**—Map to predefined event types in MARS so that existing reports and rules support the new device event types. If you cannot find a good match among the event types that are already in the system, you can create your own event type and event type groups. Then you can either put the new event types in system event type groups (so system rules and reports using the groups can automatically use the event type), or define new rules and reports to use the new event type or event type group.

Step 1 Verify that the device support package does not already exist

Log on to the MARS NetPro Forum site and conduct a survey to determine whether the device support package you require has been previously developed and posted.

For more information, see

Step 2 Determine which similar device support packages already exist

Even when the MARS NetPro Forum site (or local resources) do not have the *exact* device support package you require, locating a similar package can be advantageous. You can typically alter an existing device support package file for the required device or version more easily than you could build one from scratch.

For more information, see

Step 3 Verify the Provider Definition.

You can define a custom device support package on either a Global Controller or a stand-alone Local Controller; however, the appliance on which you are defining it has a local provider definition, which is the profile included in the export package. You should customize this profile so you can more easily distinguish your packages from others that you might install.

The local provider definition presents information that is unique to your organization.

For more information, see [Specify the Provider Configuration, page 15-4](#)

Step 4 Define a custom device type.

The custom *device type* is an object defined in MARS that represents an unsupported application or device. It organizes the following information about the device: vendor, model, version, and type (whether it is a hardware device or a software application running on a host). This last distinction is used to determine how a reporting device of that type is added in the web interface.

- **Vendor**—Identifies the vendor of the appliance or software.

- **Model**—Identifies the appliance model or software package name.
- **Version**—Identifies the version of the software, whether standalone or running on an appliance.
- **Type**—Specifies whether it is an appliance or software running on a host. This value is required because it determines how you define a reporting device of this device type under Admin > Security and Monitoring Devices.

You can define a custom device type for any device that generates SYSLOG or SNMP events and that can forward those events to the MARS Appliance. Once you have defined a custom device type, you can define device event types for that device type.

You can define a custom device type in two different ways.

1. Define a custom device type under the Management > Device Type Management.
2. Define a custom log parser under ADMIN > Custom Setup > Custom Log Parser.

For more information, see [Create a Device Type, page 15-7](#)

Step 5 Define one or more custom event types, and ensure defined patterns work if patterns are defined.

A custom event type represents a definition of a specific SYSLOG or SNMP trap event so that MARS can parse and extract the relevant session information from the event. It also maps the event to a custom or existing event type, which in turn is mapped to one or more existing event type groups. The event type groups are already mapped to existing inspection rules, reports, and queries. Once you have defined the device type and described the structure of the events, you need to configure devices of that type into the network topology, configure them to report data to the MARS Appliance, and query the event data using a free-form or predefined query to ensure the defined patterns work as expected.

To define a device event type, you must identify the format of the raw message and define multiple regular expressions that match against the key and value patterns within the message. These patterns are typically mapped to predefined value types, which tell MARS how to store the values extracted so they can be used in inspection rules, queries, and reports.

For more information, see [Create Device Event Types for a Custom Device Type, page 15-8](#)

Step 6 Determine the Device Support Package Level of Protection

You determine whether, and how, a device support package is protected. Password protection can permit or deny import of the package as well as determining whether encryption can be unlocked.

For more information, see

Step 7 Export the Device Support Package to an Off-Appliance Location.

After the custom device type and all event types are defined, you can export them to a single file format, which can be used as a backup or to import into other devices that receive events from the same device type. Exported packages are not restricted to a single device type; and therefore, you may have one that includes multiple custom devices types.

A single file is exported. The file contains the device type, event type, rules, and report information. You can import the file into a MARS Appliance to enable event parsing support of the device types contained in the file, as well as to enable rules and reports support if rules and reports are also contained.

For more information, see [Export a Device Support Package, page 15-24](#)

Step 8 Verify export/import works, and that parsing works with the imported data.

You can verify that the custom definition works with the logs and reporting. If you're importing or exporting a device type definition, review the report Activity: CS-MARS importing/exporting DSF packages logs to verify that the import succeeded.

For more information, see

Create a Device Type

You can create a device or application type in either of two places in the MARS web interface:

- Click **MANAGEMENT > Device Type Management** and then click **Add**.
- Click **ADMIN > Security and Monitor Devices**, and then click **Add** next to the Device/Application Type list.

The device or application type organizes the custom event types that you define. MARS uses this logical group to select which custom event types to apply to events received from a reporting device of this type. You must define a device type before you can define a custom parser.

To create a device type, follow these steps:

Step 1 Click **MANAGEMENT > Device Type Management**.

The Device Type Management list appears.

Step 2 Click **Add**.

The Device Type Definition page appears.

Device/Application Type Definition

→ *Type: ☐ Appliance ☐ Software

→ *Vendor:

→ *Model:

→ *Version:

→ Description:

251122

Step 3 Select the type of custom parser to define:

- **Appliance**—Represents a hardware device that sends logs to the MARS Appliance.
- **Software**—Represents an application running on a host. The host can be configured to send logs to the MARS Appliance.

Step 4 Enter values for the following fields:

- **Vendor**—Unique name to identify the vendor of the custom parser. *Example:* Cisco.
- **Model**—Unique name to identify the model that the custom parser represents. *Example:* PIX.

- **Version**—Unique name to identify the software image version running on the appliance or host for which the custom parser is being defined. *Example:* 7.0.

**Tip**

The **Description** field is optional and may be used to expand the device/application type definition as desired.

Step 5 Click **Submit**.

The Device Event Types For page displays. While it appears empty during the initial definition, this page will list the custom event type definitions grouped by this custom device.

Figure 15-1 Device Event Types For: <page_name>

Device Event Types For : Test Test 1.0

Device Event ID / Description:

Select Provider: All

Device Event ID	Device Event Type Description	Mapped to Event Type	Severity	Provider Name	Last Updated By	Last Updated Time

0 to 0 of 0
25 per page

251124

Create Device Event Types for a Custom Device Type

The definition of a device event type includes two parts:

- **data work**—which instructs MARS what event type it will be mapped to
- **regular expression pattern definition (optional)**—which, if defined, instructs MARS how to extract relevant data from a raw message.

A device event type maps the event to a predefined or custom event type, which specifies the event priority and identifies the event type groups with which it is associated.

**Note**

Device event types were referred to as *log templates* in previous releases of MARS.

Before You Begin

This procedure assumes that you have defined a custom device type, as described in [Create a Device Type](#), page 15-7.

Be familiar with the Perl Compatible Regular Expressions (PCRE) syntax. For more information, see [Appendix B, “Regular Expression Reference”](#).

Step 1 Click **Management > Device Type Management**.

Step 2 Select the custom device type for which you want to define a new device event type, and then click **Add Device Event Type**.

A log template ties directly to the particular message that you want to parse. A log template is composed of one or more patterns that describe the contents of the message. Using the patterns, MARS parses the message when it is received.

The Device Event Type For: <device_type_name> pages appears.

Step 3 Enter a value in the Device Event ID field.

The Device Event ID allows you to map this message number—or another moniker used by the device—to the custom event type definition. Use the Device Event ID to clarify the relationship with the device trap or message ID. This value is a unique string value among all Device Event IDs associated with the selected device type.

Step 4 Enter a description of the device event type in the Description field.

This value is the one that is used throughout the web interface when displaying lists of custom device event types. If you leave this field blank, distinguishing among device event types is made more difficult.

Step 5 Do *one* of the following:

- Map the log to an existing event type. MARS includes tens of thousands of predefined event types. Select the event type and click the << button to add the event type to the Selected Event Type field.



Tip To display this list, select **System** from the Choose Event Type From filters and click **Get**). Alternatively, you can filter on severity level or enter keywords in the search field and click **Search**. To see additional event types, select a different page number under the Event Type list.

- Define a custom event type and map the log to it by performing the following steps:

- a. To define a new event type, click **Add** below the Event Type list.

The Event Type Definition page appears.

Event Type Definition

→ *Event ID:

→ *Description:

→ Severity: RED

→ CVE Name:

→ *Event Type Group:

Choose Event Type Groups From:

Select Provider: All

☐	ApplPolicyViolation/Misc
☐	ApplPolicyViolation/Web
☐	AttacksProtected
☐	ConfigError/CS-MARS
☐	ConfigError/CiscoCatOS
☐	ConfigError/CiscoIOS
☐	ConfigError/CiscoPix
☐	ConfigError/CiscoVPNConc
☐	ConfigError/Host
☐	ConfigError/NetScreenFirewall

251123

b. Enter values for the following fields and then click **Submit**:

- **Event ID**—A unique string that identifies the event relative to all other events defined in MARS. This value appears in the Event ID column on the Management > Event Management page. It is this ID to which the device event IDs are matched.
- **Description**—Provide a description of this event. It is this description that appears under the event list when selecting an event type.
- **Severity**—Identifies the severity level of this event type. Select from RED, YELLOW, or GREEN.
- **CVE Name**—Identifies the name of the Common Vulnerabilities and Exposures Name, if any.
- **Event Type Group**—Identifies the event type groups to which this event type definition belongs. An event type can belong to one or more event type groups. If you want to define a custom event type group, click **Add Group** on the Management > Event Management page. It is also on this page that you can click on an event type group in the Groups column to see a description of the group and a list of the other events mapped to this group.

**Note**

For a list of the event type groups that can be used when defining an event type in a device support framework package see [DSF Event Type Group Descriptions, page C-1](#).

Step 6 Once the Selected Event Type field contains a value, click **Apply**.

The Patterns link is enabled.

Step 7 Click the **Patterns** link.

Patterns For Device Event ID : Log1



Definition	Patterns

Position	Key Pattern	Parsed Field	Value Type	Value Format	Value Pattern
0 to 0 of 0 25 per page					

Developing a custom device event type requires a bit of work. The first step is to identify a complete raw message example. Next, identify which values in the raw message to parse and store. To obtain each value, MARS parses the raw message looking for a defined pattern known as a *value pattern*. A *value pattern* is a mask used to extract the values. It is bounded by another type of pattern called *key patterns*. After the key pattern, or beginning delimiter, is matched, a value pattern is matched and is stored as the value assigned to that key. The value pattern can be considered the ending delimiter. Then the next key pattern is sought, and so on. Each value is stored as a predefined value type, which include:

- source address
- source port
- destination address
- destination port
- protocol
- NAT source address
- NAT source port
- NAT destination address
- NAT destination port
- NAT protocol
- device time stamp
- received time
- session duration
- transmitted bytes
- reported user
- workstation name
- domain name

As described earlier, the parsing format is a pair of value strings: a *Key pattern* followed by a *Value pattern*. The Key and Value patterns are regular expressions based on the Perl Compatible Regular Expressions (PCRE) library, see [Appendix B, “Regular Expression Reference”](#) for syntax details. A device event contains multiple *Key-Value sub-pattern pairs*, which together describe the event in the common value types understood by MARS. The series of *Key-Value sub-pattern pairs* are concatenated in the order of their positions and used to match against the raw message in an event.



Note If the protocol is ICMP (a portless protocol), the source and destination ports are stored as 0 (zero.)

Step 8 Define a device event type.



Timesaver

To show how to define a device even type, the following *example* presents the 12 patterns required to parse the example raw message below:

Example 15-1 Example Raw Message

```
Teardown TCP connection 1000 faddr 67.126.151.132/80 gaddr 198.133.219.28/43246 laddr
10.1.1.30/890 (sudha) duration 01:00:02 bytes 1000000 (TCP FINs)
```

a. First we click **Add** to input patterns.

In [Example 15-1](#), we see, reading left to right, 12 keys and expected values for which patterns and value types can be defined:

Key	Expected Value	Common Value Type
Teardown	TCP	protocol
connection 1000 faddr	67.126.151.132	source address
/	80	source port
gaddr	198.133.219.28	destination address
/	43246	destination port
laddr	10.1.1.30	NAT destination address
/	890	NAT destination port
(	sudha	reported user
duration	01	session duration/hours
:	00	session duration/minutes
:	02	session duration/seconds
bytes	10000	transmitted bytes



Note A Key can be an empty string.

The Pattern Definition for Device Event Type: Log 1 page (shown below [g.](#)) appears.

**Tip**

Steps [b.](#) through [j.](#) present an example of how to complete a Pattern Definition for the Device Event Type page.

- b. The *Position* field identifies the order of the specified Key-Value sub-pattern when parsing the raw message from left to right, top to bottom. The parser allows arbitrary whitespace between Key and Value patterns and between Key-Value sub-patterns.
- c. In [Example 15-1](#), the first Key pattern on which to match is the string "Teardown". To match on this string, use a simple regular expression with no wildcards or repetitions.

**Note**

The Key pattern is "Teardown", which means that when this pattern is found, the parser evaluates the next sequence to find the value to associate with this key.

- d. Looking at the value to be paired with the Teardown key, we see "TCP", which identifies the protocol. This field type matches the common value type Protocol, which we select as the Parsed Field value.
- e. The *Value Type* tells the parser what data type to expect, enabling suitable parsing action on the matching sub-pattern string. Selecting Protocol (String) as the value type indicates the protocol field is a string as defined in the file `/etc/protocols` in a UNIX system. In [Example 15-1](#), "TCP" is the string captured by the Value pattern. In this example, the Value Type indicates that TCP is to be converted into its equivalent protocol number, 6.
- f. The *Pattern Name* field lists the predefined regular expression patterns you can use to extract the value. Several common predefined patterns are defined for each common value type. In [Figure 15-2](#), the value pattern captures all word-character strings that may also include the characters '-', '/', and '+.
- g. When defining an event type, we do one of the following:
 - To use a predefined pattern, we select a predefined pattern from the **Pattern Name** list, and click **Submit**.
 - To define a custom pattern we perform the following steps:
 - a. Enter a name in the **Or enter new** field.
This name allows you to reuse this pattern when defining other device event types. Once it is defined, it will be associated with the value type selected in the Value Type field. You can select this pattern whenever that value type is selected.
 - b. Enter a description in the **Description** field.
 - c. Specify the regular expression pattern used to extract the value from the raw message in the **Value Pattern** field.
 - d. Click **Submit** to complete the Key-Value sub-pattern definition.

The key and value patterns are specified for the protocol.

Figure 15-2 Pattern Definition for Device Event Type (First Position)

Pattern Definition For Device Event Type : Log1

→ Position: 1

→ Key Pattern: Teardown

→ Parsed Field: Protocol

→ Value Type: Protocol (String)

→ Pattern Name: PROTOCOL STRING

Or enter new:

→ Description: Protocol, as a protocol string as defined in /etc/protocols

→ Value Pattern: [\w-/+\,]+

Cancel Submit

Figure 15-3 Patterns for Device Event ID (First Position)

Patterns For Device Event ID : Log1

	Position	Key Pattern	Parsed Field	Value Type	Value Format	Value Pattern
1	1	Teardown	Protocol	Protocol String		[\w-/+\,]+

1 to 1 of 1 25 per page

Add Edit Delete Test

Back Submit

- h. To define the Key-Value pair for the second position, we must define a more complicated regular expression. We click **Add** to begin defining the second pattern. The key pattern is not a simple string. In the example, we want to match on "connection 1000 faddr". To do this, we match first on the string *connection* and then match on any sequence of digits using the expression *\d+*. This expression is followed by the string *faddr*, which rounds out our key pattern match *connection \d+ faddr*.

**Note**

The example includes the match for an optional plus or minus, *[+/-]?*, in case the digits are signed. The plus or minus sign would have to appear in front of the digits for this pattern to be matched. The *?* indicates that this pattern is optional.

The expected value is a source IP address, which we designate by selecting **Source Address** as the Parsed Field value. The example value is specified using standard dot notation and the address is IP version 4 so we can select **IPV4 (Dotted Quad)** as the pattern name and **IPV4_DOTQUAD** as the predefined pattern.

The key and value patterns are defined for the source IP address.

Figure 15-4 Pattern Definition for Device Event Type: Log1 (Second Position)

Pattern Definition For Device Event Type : Log1

→ Position:

→ Key Pattern:

→ Parsed Field:

→ Value Type:

→ Pattern Name:

Or enter new:

→ Description:

→ Value Pattern:

251112

- i. For the third position, we want to match the source port. The unique pattern we can use to match for the key is the forward slash that precedes the port number. The Value Type is **Port (Number)**, which allows us to select the predefined Pattern Name of **PORT_NUMBER**.

The key and value patterns are defined for the source port.

Figure 15-5 Pattern Definition for Device Event Type: Log1 (Third Position)

Pattern Definition For Device Event Type : Log1

→ Position:

→ Key Pattern:

→ Parsed Field:

→ Value Type:

→ Pattern Name:

Or enter new:

→ Description:

→ Value Pattern:

251113

- j. For each key position in the raw message, we add a new pattern definition until we have defined all 12 key and value patterns.

Patterns for Log Template : Log1

Definition					Patterns																																																																																												
Add Edit Delete Test <table border="1"> <thead> <tr> <th></th> <th>Position</th> <th>Key Pattern</th> <th>Parsed Field</th> <th>Value Type</th> <th>Value Format</th> <th>Value Pattern</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td>1</td> <td>Teardown</td> <td>Protocol</td> <td>Protocol String</td> <td></td> <td>[w-/+]+</td> </tr> <tr> <td>☐</td> <td>2</td> <td>connection [+]? d+ faddr</td> <td>Source Address</td> <td>IPv4 Dotted Quad</td> <td></td> <td>((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])</td> </tr> <tr> <td>☐</td> <td>3</td> <td>/</td> <td>Source Port</td> <td>Port Number</td> <td></td> <td>((0x[a-fA-F\d]{1,4}) (\d{1,5}))</td> </tr> <tr> <td>☐</td> <td>4</td> <td>gaddr</td> <td>Destination Address</td> <td>IPv4 Dotted Quad</td> <td></td> <td>((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])</td> </tr> <tr> <td>☐</td> <td>5</td> <td>/</td> <td>Destination Port</td> <td>Port Number</td> <td></td> <td>((0x[a-fA-F\d]{1,4}) (\d{1,5}))</td> </tr> <tr> <td>☐</td> <td>6</td> <td>laddr</td> <td>NAT Dest Address</td> <td>IPv4 Dotted Quad</td> <td></td> <td>((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])</td> </tr> <tr> <td>☐</td> <td>7</td> <td>/</td> <td>NAT Dest Port</td> <td>Port Number</td> <td></td> <td>((0x[a-fA-F\d]{1,4}) (\d{1,5}))</td> </tr> <tr> <td>☐</td> <td>8</td> <td>\Q\E</td> <td>Reported User</td> <td>String</td> <td></td> <td>\w+</td> </tr> <tr> <td>☐</td> <td>9</td> <td>\Qduration\E</td> <td>Session Duration</td> <td>Duration-Hours</td> <td></td> <td>(0x)?[a-fA-F\d]+</td> </tr> <tr> <td>☐</td> <td>10</td> <td>:</td> <td>Session Duration</td> <td>Duration-Minutes</td> <td></td> <td>(0x)?[a-fA-F\d]+</td> </tr> <tr> <td>☐</td> <td>11</td> <td>:</td> <td>Session Duration</td> <td>Duration-Seconds</td> <td></td> <td>(0x)?[a-fA-F\d]+</td> </tr> <tr> <td>☐</td> <td>12</td> <td>bytes</td> <td>Transmitted Bytes</td> <td>Number</td> <td></td> <td>(0x)?[a-fA-F\d]+</td> </tr> </tbody> </table> 1 to 12 of 12 25 per page Add Edit Delete Test								Position	Key Pattern	Parsed Field	Value Type	Value Format	Value Pattern	☐	1	Teardown	Protocol	Protocol String		[w-/+]+	☐	2	connection [+]? d+ faddr	Source Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])	☐	3	/	Source Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))	☐	4	gaddr	Destination Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])	☐	5	/	Destination Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))	☐	6	laddr	NAT Dest Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])	☐	7	/	NAT Dest Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))	☐	8	\Q\E	Reported User	String		\w+	☐	9	\Qduration\E	Session Duration	Duration-Hours		(0x)?[a-fA-F\d]+	☐	10	:	Session Duration	Duration-Minutes		(0x)?[a-fA-F\d]+	☐	11	:	Session Duration	Duration-Seconds		(0x)?[a-fA-F\d]+	☐	12	bytes	Transmitted Bytes	Number		(0x)?[a-fA-F\d]+
	Position	Key Pattern	Parsed Field	Value Type	Value Format	Value Pattern																																																																																											
☐	1	Teardown	Protocol	Protocol String		[w-/+]+																																																																																											
☐	2	connection [+]? d+ faddr	Source Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])																																																																																											
☐	3	/	Source Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))																																																																																											
☐	4	gaddr	Destination Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])																																																																																											
☐	5	/	Destination Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))																																																																																											
☐	6	laddr	NAT Dest Address	IPv4 Dotted Quad		((([01]?d\d? 2[0-4]d 25[0-5])\,){3}([01]?d\d? 2[0-4]d 25[0-5])																																																																																											
☐	7	/	NAT Dest Port	Port Number		((0x[a-fA-F\d]{1,4}) (\d{1,5}))																																																																																											
☐	8	\Q\E	Reported User	String		\w+																																																																																											
☐	9	\Qduration\E	Session Duration	Duration-Hours		(0x)?[a-fA-F\d]+																																																																																											
☐	10	:	Session Duration	Duration-Minutes		(0x)?[a-fA-F\d]+																																																																																											
☐	11	:	Session Duration	Duration-Seconds		(0x)?[a-fA-F\d]+																																																																																											
☐	12	bytes	Transmitted Bytes	Number		(0x)?[a-fA-F\d]+																																																																																											

143234

Step 9 To complete a definition, click **Submit**.

Once the log template is defined and submitted, you must define a reporting device based on the custom device.

The new event type definition appears.

User Defined Log Parser Templates

Device/Application Type:

Log Templates for : Vendor1 Model1 1.2

Add Edit Delete			
Log ID	Log Description	Mapped to Event Type	Severity
☐ Log1	The first example log message to parse	Teardown Connection[3]	

1 to 1 of 1

143236

Editing a Device Type

You can edit a custom device type that is defined on MARS. To do so, select a custom device type under **MANAGEMENT > Device Type Management**, and then click **Edit**. This feature allows you to edit the following fields:

- type
- vendor
- model
- version
- description
- any device event type definitions (same as Edit Parser)

Overriding Existing Parsers

You can override existing parsers by navigating to **MANAGEMENT > Device Type Management**. A list of all device event types will appear.

Figure 15-6 Device Event Types

Vendor	Model	Version	Provider	Last Updated By	Last Updated Time	Update Revision	Derived From Parent / Ancestor
☐ ANY	Generic Device	ANY	Cisco			0	
☐ CheckPoint	Opsec	NG AI	Cisco			0	
☐ CheckPoint	Opsec	NG FP3	Cisco			0	
☐ CheckPoint	Opsec	NGX	Cisco			0	
☐ Cisco	ASA	7.0	Cisco			0	
☐ Cisco	ASA	7.2	Cisco			0	
☐ Cisco	ASA	8.0	Cisco			0	
☐ Cisco	ASA	8.1	Cisco			0	
☐ Cisco	CSA	4.x	Cisco			0	
☐ Cisco	CSA	5.x	Cisco			0	
☐ Cisco	CSC SSM	6.1	Cisco			0	
☐ Cisco	CSC SSM	6.2	Cisco			0	
☐ Cisco	FWASM	1.1	Cisco			0	
☐ Cisco	FWASM	2.2	Cisco			0	
☐ Cisco	FWASM	3.3	Cisco			0	

Select an existing device type and then click **Edit Parser**. A list of all device events will appear.

Figure 15-7 Device Events List

Device Event ID	Device Event Type Description	Mapped to Event Type	Severity	Provider Name	Last Updated By	Last Updated Time
☐ ASA-1-101001		Failover cable OK	Info	Cisco		
☐ ASA-1-101002		bad failover cable	Warning	Cisco		
☐ ASA-1-101003		Failover cable not connected	Warning	Cisco		
☐ ASA-1-101004		Failover cable not connected	Warning	Cisco		
☐ ASA-1-101005		Error reading failover cable status	Warning	Cisco		
☐ ASA-1-102001		Failover: power failure/System reload other side	Warning	Cisco		
☐ ASA-1-103001		Unable to communicate with the other unit over the failover cable	Warning	Cisco		
☐ ASA-1-103002		Failover: other firewall network interface OK	Info	Cisco		
☐ ASA-1-103003		Failover: other firewall network interface failed	Warning	Cisco		
☐ ASA-1-103004		Failover: other firewall reports this firewall failed	Warning	Cisco		

Select the device event to override, and then click **Edit**.

Figure 15-8 **Device Event Types**

You can walk through the pattern definitions to modify them as desired.



Tip

Alternatively, you can override existing parsers by selecting an existing device type under **MANAGEMENT > Device Type Management** and then clicking **Edit**. The Device/Application Type Definition page appears, click **Next**. Select from the list of Device Event Types and click **Edit**.

Extending Existing Device Types

You can extend existing device types (or parsers) using one of the following methods on the **MANAGEMENT > Device Type Management** page:

- **Derive From**—You can select an existing device type and click **Derive From** to define a new device type/parser based on an existing definition. This method allows you to support incremental version updates or to classify the device type as a custom device type, which is distinguishable from the base device type.
- **Add Device Event Type**—You can select an existing device type and click **Add Device Event Type** to extend the current definition with additional device event type definitions. This method is useful when you want to support additional message types that were not supported by the original device type definition.



Note

The benefit of extending an existing device type is that there is only one device type, so it is simple to manage. However, if there are different event formats for the same device event type to be parsed between an existing device type and a new device type, and you have both device types reporting to MARS, then we recommend that you derive from existing device type to create a new device type, and configure on the MARS GUI different device types for each of the reporting devices.

Add a Reporting Device based on a Custom Appliance Device Type

Adding custom appliance as a reporting device is similar to adding a predefined device type. You can select the appliance type directly from the Device Type list.

To add a reporting device based on a custom appliance device type, follow these steps:

- Step 1** Click **Admin > Security and Monitor Devices**.
- Step 2** Click **Add** to add a new device.
- Step 3** Select the custom appliance type from the Device Type list.
- Step 4** Complete the following fields and click **Submit**:

**Tip**

The fields may vary depending on the appliance device type.

- **Device Name**—The name of the device.
- **Reporting IP**—The IP address that the reporting device will use to publish its event stream.
- **Reporting Method**—Select either **SNMP TRAP** or **SYSLOG** so as to match the event type generated by the reporting device. This option determines what type of traffic is processed by the custom device type parser.

Step 5 Click **Done**.

Add a Reporting Device based on a Custom Software Device Type

Adding a custom application as a reporting device is similar to adding a predefined application. You must first define a host and then add the custom application as a reporting application.

The following example adds an instance of the newly defined Apache Webserver1.1 software application.

To add a reporting device based on a custom software device type, follow these steps:

- Step 1** Click **Admin > Security and Monitor Devices**.
- Step 2** Click **Add** to add a new device.
- Step 3** Select **Add SW security apps on a new host** from the Device Type list.
- Step 4** Fill in name and other host details and click **Apply**.
- Step 5** Click on **Reporting Applications**.
- Step 6** Select Application (such as Apache Webserver.1.1) from the list and click **Add**.

Figure 15-9 Adding the Custom Application to MARS

Device Type: Edit host with security applications

General Reporting Applications Vulnerability Assessment Info

Enter reporting application:

→ Device Name: Host1

→ Select application: Apache Webserver 1.1 Add

Edit Remove

Device Type

☐ Apache Webserver 1.1

Done

- Step 7** Select either **SNMP TRAP** or **SYSLOG** as the Reporting Method in the resulting window, and click **Submit**.

This option determines what type of traffic will be processed by the custom log parser.

- Step 8** Click **Done**.
-

Import a Device Support Package

MARS is designed to share device support packages with standalone Local Controllers as well as with a Global Controller, which in turn pushes packages down to its managed Local Controllers. You can share device support by importing one or more device support packages that have been developed either within your organization or downloaded from the MARS forum on NetPro.

When you import a device support package, you import the settings that represent a custom device type, including the device type definition and the device event types and their associations with event type groups, rules, and reports.

To import a device support package, follow these steps:

- Step 1** Click **ADMIN > Custom Setup > Device Support Packages**.

The Device Support Packages page appears.

CISCO

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

System Setup System Maintenance User Management System Parameters Custom Setup Sep 10, 2008 10:20:10 AM PDT

ADMIN | CS-MARS Global Controller: GC181-DSF v6.0 Login: Global: Administrator (pnadmin) :: Logout :: Activate

Device Support Packages

Export Import Unlock Lock Back Delete

☐	Name	Version	Provider	File Name	Summary	Description	Time	Type	Protected
☐	test et group in rule filter	1.0	marsGC181-local	test-etgroup-in-rule-filter.zip	test et group in rule filter (View)	user/system et group in filter	Aug 6, 2008 3:34:05 PM PDT	Exported	No
☐	test et group in rule filter	1.0	mars181	test-etgroup-in-rule-filter.zip	test et group in rule filter (View)	user/system et group in filter	Aug 12, 2008 10:30:55 AM PDT	Imported	No
☐	liz pkg cd4 for filter in report	1.0	mars96-edit	liz-pkg-CD4-for-filter-in-report.zip	liz pkg cd4 for filter in report (View)	1 report	Aug 12, 2008 10:33:49 AM PDT	Imported	No
☐	liz pkg CD4 SNMP test devices	5.0	Local	liz-pkg-CD4-SNMP-test-devices.zip	liz pkg CD4 SNMP test devices (View)	3 device types	Aug 19, 2008 4:10:46 PM PDT	Imported	No
☐	device-type-only-for-Agata-pkgname	10.0	dsf<i>team</i> local	device-type-only-for-Agata-pkgname Test1.zip	device-type-only-for-Agata-pkgname (View)	This package contains device types only: 1 local	Sep 10, 2008 9:19:12 AM PDT	Imported	No

251118

Step 2 Click Import.

CISCO

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

System Setup System Maintenance User Management System Parameters Custom Setup Sep 10, 2008 9:28:29 AM PDT

ADMIN | CS-MARS Global Controller: GC181-DSF v6.0 Login: Global: Administrator (pnadmin) :: Logout :: Activate

Input or browse the name of the package to be imported

Launch Package Sharing on MARS forum

Back Next

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

194626

The input file name page appears.

- Step 3** Specify the file to import either by typing the path and filename or by clicking **Browse** and navigating to the file. Then click **Next**.



Tip

Alternatively, you can click *Launch Package Sharing on Mars forum* to launch a browser and explore the MARS Forum. There, you can select and download a device support package file. The file you download can then be imported. For more information on the forum, see [Download a Device Support Package from the MARS Forum on NetPro, page 15-32](#).

- Step 4** If the file is protected, a dialog box appears.

The screenshot shows the Cisco MARS web interface. At the top left is the Cisco logo. A status bar at the top right displays 'May 12, 2008 12:52:26 PM PDT'. Below the status bar, a login bar shows 'Standalone: pnmars v0.0' and 'Login: Administrator (pnadmin) :: Close'. The main content area displays 'Package is protected' in a yellow box. Inside this box, there are two password prompts: 'Password for importing package' with a field labeled '*Password:' and 'Unlock password for protected package data' with a field labeled 'Password:'. At the bottom of the yellow box are 'Cancel' and 'Submit' buttons. At the bottom of the page, there is a copyright notice: 'Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved.' and a small number '261117' on the right side.

Enter the password for importing the package and then click **Submit**.



Tip

At this time you can also enter the password for unlocking protected package data. This allows you to view the parser pattern data.

- Step 5** The Import Summary page appears.

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

If you intend to import a subset of the device types defined in this package file, deselect any of the items that you do not want to import, and then click **Import**.



Tip

You must select any device type from which a device type is derived. MARS checks for dependencies and does not allow you to deselect a device type if it is a parent or ancestor of a selected device type.

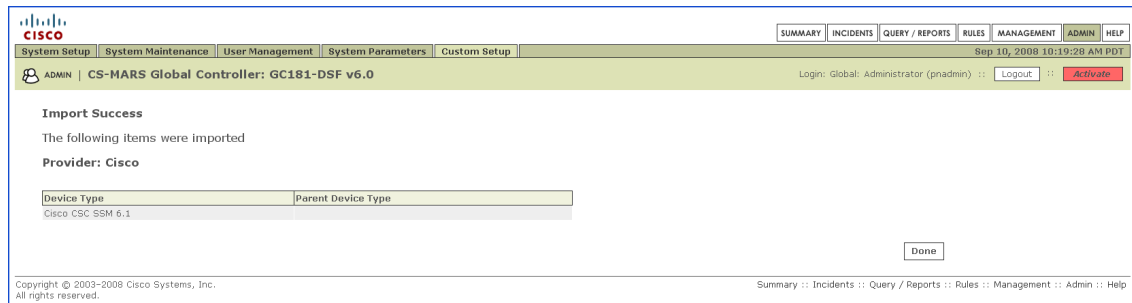
The device support package is imported. You can review the imported packaged by clicking ADMIN > Custom Setup > Device Support Packages.

- Step 6** If the SHA-1 checksum of the package to be imported does not match the checksum contained within the data xml file, a warning appears:

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved.

Click **Yes** to continue.

The Import Success page appears.



Note

The illustrations shown here are typical and are not indicative of a single particular import sequence.

Export a Device Support Package

To export a device support package, you must select the device type or types to export, identify what you want to include in the export, describe the package, and then download the files to an external server. Once you have exported a package, you can import it into a standalone Local Controller or Global Controller.

Before You Begin

Before you can export a device support package, you must have defined the following:

- A custom device type
- One or more custom event types
- One or more user inspection rules
- One or more user reports
- Associations between custom event types and existing system event type group.
- A policy for sharing—or protecting—the device support package.

To export a device support package, follow these steps:

Step 1 Click **ADMIN > Custom Setup > Device Support Packages**.

The Device Support Packages page appears.

☐	Name	Version	Provider	File Name	Summary	Description	Time	Type	Protected
☐	test et group in rule filter	1.0	marsGC181-local	test-etgroup-in-rule-filter.zip	test et group in rule filter (View)	user/system et group in filter	Aug 6, 2008 3:34:05 PM PDT	Exported	No
☐	test et group in rule filter	1.0	mars181	test-etgroup-in-rule-filter.zip	test et group in rule filter (View)	user/system et group in filter	Aug 12, 2008 10:30:55 AM PDT	Imported	No
☐	liz pkg cd4 for filter in report	1.0	mars96-edit	liz-pkg-CD4-for-filter-in-report.zip	liz pkg cd4 for filter in report (View)	1 report	Aug 12, 2008 10:33:49 AM PDT	Imported	No
☐	liz pkg CD4 SNMP test devices	5.0	Local	liz-pkg-CD4-SNMP-test-devices.zip	liz pkg CD4 SNMP test devices (View)	3 device types	Aug 19, 2008 4:10:46 PM PDT	Imported	No
☐	device-type-only-for-Agata-pkgname	10.0	dsf<i>team</i>local	device-type-only-Test1.zip	device-type-only-for-Agata-pkgname (View)	This package contains device types only: 1 local	Sep 10, 2008 9:19:12 AM PDT	Imported	No

Step 2 Click to select the package file to export.
The Choose items to export page appears.

Choose items to export

☐ Device Type
☐ Report
☐ Rules

Step 3 Select the items to export and click **Next**.



Note In this procedure example we'll select device type. Similar steps occur regardless of the items exported.

The Choose Device Types To Export page appears

Choose Device Types To Export

Vendor / Model / Version:

Select Provider:

☐	Vendor	Model	Version	Provider	Last Updated By	Last Updated Time	Update Revision	Derived From Parent / Ancestor
☐	Cisco	PIX	6.2.1	Local	Local		0	Cisco PIX 6.2 / Cisco PIX 6.2
☐	Cisco	PIX	6.2.2	Local	Local		1	Cisco PIX 6.2.1 / Cisco PIX 6.2
☐	Symantec	Manhunt	5.0	Local			0	
☒	Vendor1	Model1	1.2	Local			0	

1 to 4 of 4 25 per page

Step 4 Select the device types to export and click **Next**.



Tip You can filter the device types listed by using the Search field or the Select Provider list.

The Export Summary page appears.

Export Summary

Total Number Of Providers : 1
 Total Number Of Device Types : 1
 Total Number Of Device Event Types : 0
 Total Number Of Event Types : 0
 Total Number Of Event Type Groups : 0

Summary For Provider: Local

Device Type	Parent Device Type
Vendor1 Model1 1.2	
Number Of Device Event Types: 0	
Number Of Event Type Groups: 0	
Number Of Event Types: 0	

Step 5 Verify the summary information and click **Next** to proceed, or click **Back** to return to the Device Support Packages page.

- **Total Number of Providers**—Identifies the number of providers included in this group. This number should be 1 unless you have modified a Cisco-provided device type or have imported device types (and have chosen to export one of those devices) from another Local Controller or provider, such as the MARS forum on NetPro website.
- **Total Number of Devices**—Identifies the number of custom devices that you have chosen to export in this package.
- **Total Number of Device Event Types**—Identifies the total number of custom device event types that have been selected. This number is taken from each device selected, where the events are those associated with each device.
- **Total Number of Event Types**—Identifies the number of system event types that were mapped to the devices that are being exported.

- **Total Number of Event Type Groups**—Identifies the number of event type groups that include one or more of these custom device event types.

The Package Details page appears.

Package Details

251116

Step 6 Enter values for the following fields:

- **Package File Name**—Identifies the name of the file to be created. An example filename is *test.zip*.
- **Package Name**—Identifies the name of the package, which will appear in the list of installed packaged on a MARS Appliance that has imported this package.
- **Version**—Identifies the version number of the custom package. You must revise each exported version.
- **Package Description**—Summarizes the contents of the package, such as the device types that are included in the package. This field appears in the list of installed packages on a MARS Appliance that has imported this package.

Step 7 To protect the package from unauthorized use, perform the following steps

- a. Select **Protect Package**.



Tip

You can choose to protect the package from being imported, from its parser patterns being decrypted, or both.

- b. To protect the package from being imported enter a password and then confirm the password entry.
- c. To protect the parser patterns from being decrypted, enter a password and then confirm the password entry.

Step 8 Click **Export**

The Export Success page appears.

Figure 15-10 Export Success Page: Package File Name of Test**Export Success**

Click on the filename to download the package file

test.zip (Checksum : 26F283F286986FF2847631513FC697CE)

Click on the filename to download the package header file

test-Header.xml

Done

251105

- Step 9** To download the package to a local computer or to a central server/repository, click on the filename to download the package. If you want to publish this package on MARS forum on NetPro, download the package header file.

**Note**

The header file is only needed if you want to upload this package on MARS forum on NetPro, which requires separate DSF pkg and header files. For more information, see [MARS Forum on NetPro: An Overview, page 15-31](#).

- Step 10** Once you have downloaded the needed files, click **Done** to close the Export page.

Remove an Installed Device Support Package

You can remove a custom device support package that is installed on a MARS Appliance. When removing a package, all imported information remains, only the package itself is removed. Therefore, the ability of the MARS Appliance to parse any events received from a reporting device of that type remains.

To access this page, select **ADMIN > Custom Setup > Device Support Packages**.

To remove an installed device support package, follow these steps:

- Step 1** Select the check box next to the package that you want to remove.
- Step 2** Click **Delete**.
- The Confirm Delete page appears.
- Step 3** To confirm the deletion, click **Yes**.

Events and Reports About Device Support Package Activities

The following events appear in the Info/Misc/CS-MARS-DSF-Activity event group and are summarized in the report titled *Activity: CS-MARS importing/exporting DSF packages*:

Normalized Event type: 1000083,

Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100071
Name: CS-MARS-DSF successfully imported a package from a provider

Normalized Event Type: 1000084
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100072
Name: CS-MARS-DSF failed to import a package from a provider

Normalized Event Type: 1000085
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100073
Name: CS-MARS-DSF successfully exported a package

Normalized Event Type: 1000086
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100074
Name: CS-MARS-DSF failed to export a package

Normalized Event Type: 1000087
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100075
Name: CS-MARS-DSF started importing a package from a provider

Normalized Event Type: 1000088
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100076
Name: CS-MARS-DSF started exporting a package

Normalized Event Type: 1000089
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100077
Name: CS-MARS-DSF inserted provider information in provider table

Normalized Event Type: 1000090
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100078
Name: CS-MARS-DSF updated provider information in provider table

Normalized Event Type: 1000091
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100079
Name: CS-MARS-DSF inserted device type information in device type table

Normalized Event Type: 1000092
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100080
Name: CS-MARS-DSF updated device type information in device type table

Normalized Event Type: 1000093
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100081
Name: CS-MARS-DSF inserted event type information in event type table

Normalized Event Type: 1000094
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100082
Name: CS-MARS-DSF updated event type information in event type table

Normalized Event Type: 1000095
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100083
Name: CS-MARS-DSF inserted device event type information in device event type table

Normalized Event Type: 1000096
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100084
Name: CS-MARS-DSF updated device event type information in device event type table

Normalized Event Type: 1000097
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100085
Name: CS-MARS-DSF inserted pattern type information in pattern type table

Normalized Event Type: 1000098
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100086
Name: CS-MARS-DSF updated pattern type information in pattern type table

Normalized Event Type: 1000099
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100087
Name: CS-MARS-DSF inserted event type group information in event type group table

Normalized Event Type: 1000100
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100088
Name: CS-MARS-DSF updated event type group information in event type group table

Normalized Event Type: 1000101
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100089
Name: CS-MARS-DSF inserted inspection rule information in inspection rule table

Normalized Event Type: 1000102
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100090
Name: CS-MARS-DSF updated inspection rule information in inspection rule table

Normalized Event Type: 1000103
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100091
Name: CS-MARS-DSF inserted report information in report table

Normalized Event Type: 1000104
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100092
Name: CS-MARS-DSF updated report information in report table

Normalized Event Type: 1000105
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100093
Name: CS-MARS-DSF inserted inspection rule group information in inspection rule group table

Normalized Event Type: 1000106
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100094
Name: CS-MARS-DSF updated inspection rule group information in inspection rule group table

Normalized Event Type: 1000107
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100095
Name: CS-MARS-DSF inserted report group information in report group table

Normalized Event Type: 1000108
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100096
Name: CS-MARS-DSF updated report group information in report group table

Normalized Event Type: 1000109
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100097
Name: CS-MARS-DSF inserted relationship between event type group to event type

Normalized Event Type: 1000112
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100100
Name: CS-MARS-DSF inserted relationship between inspection rule group to inspection rule

Normalized Event Type: 1000115
Device Event Type: Protego Networks, MARS, 1.0: MARS-3-100103
Name: CS-MARS-DSF inserted relationship between report group to report

MARS Forum on NetPro: An Overview

Device support packages are posted to and downloaded from the Package Sharing page of the MARS forum at the Networking Professionals Connection (NetPro) forum on Cisco.com. The packages uploaded to the Package Sharing page can be

**Tip**

The MARS Forum on NetPro also offers discussion threads, news, and support from Cisco experts in various specialties.

This section contains the following topics:

- [Uploading a Device Support Package to the MARS Forum, page 15-31](#)
- [Download a Device Support Package from the MARS Forum on NetPro, page 15-32](#)
- [Subscribe to Package Sharing Page of the MARS Forum, page 15-33](#)

Uploading a Device Support Package to the MARS Forum

Uploading a device support package file to the NetPro MARS Forum consists of two basic steps:

- Accepting the license agreement
- Selecting and uploading the device support package file

To upload a device support package, follow these steps:

Step 1 Prepare a device support package file for uploading.

Step 2 Log on to Cisco.com.

**Tip**

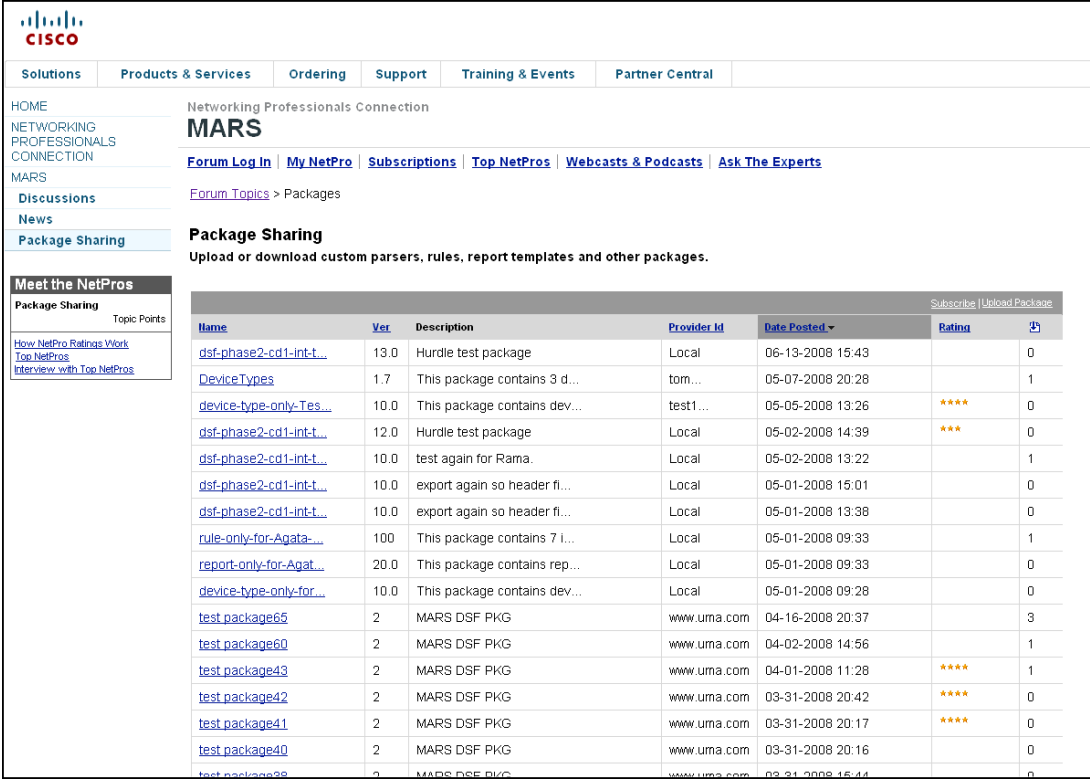
If you have not registered at this site, you'll have to do that.

Step 3 Navigate to the Networking Professionals Connection (NetPro).

Step 4 Select **MARS** from the menu on the left.

The MARS forum options display.

Step 5 Select **Package Sharing**



The screenshot shows the Cisco MARS Forum on NetPro interface. The top navigation bar includes links for Solutions, Products & Services, Ordering, Support, Training & Events, and Partner Central. The left sidebar contains links for HOME, NETWORKING PROFESSIONALS CONNECTION, MARS, Discussions, News, and Package Sharing. The main content area is titled "MARS" and includes links for Forum Log In, My NetPro, Subscriptions, Top NetPros, Webcasts & Podcasts, and Ask The Experts. Below this, there's a "Package Sharing" section with a description: "Upload or download custom parsers, rules, report templates and other packages." A table of available packages is displayed, with columns for Name, Ver, Description, Provider Id, Date Posted, Rating, and a download icon. The table lists various test packages and device-specific packages.

Name	Ver	Description	Provider Id	Date Posted	Rating	Download
dsf-phase2-cd1-int-t...	13.0	Hurdle test package	Local	06-13-2008 15:43		0
DeviceTypes	1.7	This package contains 3 d...	tom...	05-07-2008 20:28		1
device-type-only-Tes...	10.0	This package contains dev...	test1...	05-05-2008 13:26	★★★★	0
dsf-phase2-cd1-int-t...	12.0	Hurdle test package	Local	05-02-2008 14:39	★★★	0
dsf-phase2-cd1-int-t...	10.0	test again for Rama.	Local	05-02-2008 13:22		1
dsf-phase2-cd1-int-t...	10.0	export again so header fi...	Local	05-01-2008 15:01		0
dsf-phase2-cd1-int-t...	10.0	export again so header fi...	Local	05-01-2008 13:38		0
rule-only-for-Agata...	100	This package contains 7 i...	Local	05-01-2008 09:33		1
report-only-for-Agat...	20.0	This package contains rep...	Local	05-01-2008 09:33		0
device-type-only-for...	10.0	This package contains dev...	Local	05-01-2008 09:28		0
test_package65	2	MARS DSF PKG	www.uma.com	04-16-2008 20:37		3
test_package60	2	MARS DSF PKG	www.uma.com	04-02-2008 14:56		1
test_package43	2	MARS DSF PKG	www.uma.com	04-01-2008 11:28	★★★★	1
test_package42	2	MARS DSF PKG	www.uma.com	03-31-2008 20:42	★★★★	0
test_package41	2	MARS DSF PKG	www.uma.com	03-31-2008 20:17	★★★★	0
test_package40	2	MARS DSF PKG	www.uma.com	03-31-2008 20:16		0
test_package39	2	MARS DSF PKG	www.uma.com	03-31-2008 15:44		0

The Package Sharing page displays.

Step 6 Click **Upload Package** (located on the right of the bar above the table headings).

The Step 1 of 2 of Upload Package: Approve License page appears.

Step 7 Enter the Copyright Owner Name/Company and the Copyright year in the fields provided.

Step 8 Read the License Agreement text. Select **Agree**. Then click **Next**.

The Step 2 of 2 of Upload Package: Select File to Upload page appears.

Step 9 Click **Browse** to select the file, and then click **Upload**.

Download a Device Support Package from the MARS Forum on NetPro

To download a device support package, follow these steps:

Step 1 Log on to Cisco.com.



Tip If you have not registered at this site, you'll have to do that.

Step 2 Navigate to the Networking Professionals Connection (NetPro).

Step 3 Select **MARS** from the menu on the left.

The MARS forum options display.

Step 4 Select **Package Sharing**

The Package Sharing page displays.

Step 5 Select and click on a package to download.

To more easily view the packages available, you can sort the listing of packages by clicking on most of the table headings, which include for each package:

- **Name**—the name of the package
- **Ver**—the version number of the package
- **Description**—the package description (not a sort field)
- **Provider ID**—the ID of the package provider
- **Date posted**—the date the package was posted
- **Rating**—The rating given to the package by NetPro Forum users
- **[downloads]**—the number of times the package has been downloaded

The package page appears, showing the posted by and date headings as well as the contents of the package's parameters.

Step 6 After examining the package's parameters to determine its suitability, click the download symbol at the bottom of the package display page.

Step 7 After downloading and unzipping the device support package, you can import it into Mars. For more details see [Import a Device Support Package, page 15-20](#)

Subscribe to Package Sharing Page of the MARS Forum

You can subscribe to the Package Sharing Page of the MARS Forum to receive notice when new device support packages are posted.

To subscribe to the Package Sharing Page of the MARS Forum, follow these steps:

Step 1 Log on to Cisco.com.



Tip

If you have not registered at this site, you'll have to do that.

Step 2 Navigate to the Networking Professionals Connection (NetPro).

Step 3 Select **MARS** from the menu on the left.

The MARS forum options display.

Step 4 Select **Package Sharing**

The Package Sharing page displays.

Step 5 Click **Subscribe** (located on the right of the bar above the table headings).

Example Custom Device Type: Custom Software Application

You can define a custom software application and add it to the MARS environment.

To define a new custom software application, follow these steps:

Step 1 Click **MANAGEMENT > Device Type Management**.

The Device Type Management list appears.

Step 2 Click **Add**.

Figure 15-11 Example: New software based Apache Webserver application.

Device/Application Type Definition

The screenshot shows a form titled "Device/Application Type Definition". It has four fields:

- *Type: Radio buttons for "Appliance" and "Software". "Software" is selected.
- *Vendor: Text input field containing "Apache".
- *Model: Text input field containing "Webserver".
- *Version: Text input field containing "1.1".

 At the bottom right, there are two buttons: "Back" and "Submit".

143237

Figure 15-12 Example: Definition for Apache Webserver1.1

Log Template for : Apache Webserver 1.1

The screenshot shows a form titled "Log Template for : Apache Webserver 1.1". It has two tabs: "Definition" (selected) and "Patterns".

Under the "Definition" tab, there are two fields:

- *Log ID: Text input field containing "HTTP Status OK".
- Description: Text input field containing "HTTP Status 200 (OK) log".

 Below these is a section titled "Map to Event Type". It contains:

- A dropdown menu for "System" set to "System".
- A dropdown menu for "All Severity" set to "All Severity".
- A "Get" button.
- A text input field containing "HTTP Status".
- A "Search" button.
- *Event Type: A list box containing "HTTP Status - OK".
- A list of HTTP status codes with radio buttons:
 - HTTP Status - Accepted
 - HTTP Status - Bad Gateway
 - HTTP Status - Bad Request
 - HTTP Status - Conflict
 - HTTP Status - Continue
 - HTTP Status - Created
 - HTTP Status - Expectation Failed
 - HTTP Status - Forbidden
 - HTTP Status - Found
 - HTTP Status - Gateway Timeout
 - HTTP Status - OK (selected)
- At the bottom, there are three buttons: "Add", "Edit", and "Delete".

143238

- Step 3** Define the log template for a HTTP Status OK log message. And associate a system defined event type. In order to find the event type, specify the search string 'HTTP Status' and find it defined as above.
- Step 4** The parsing patterns for 'HTTP Status OK' are specified to match the following example raw message reported in an event.

```
155.98.65.40 - - [21/Nov/2004:21:08:47 -0800] "GET /~shash/ HTTP/1.0" 200 1633 "-"
"Lynx/2.8.2rel.1 libwww-FM/2.14"
```

Figure 15-13 Example: Key Pattern for HTTP Status OK

Pattern definition for Log ID : HTTP Status OK

→ Position: 1

→ Key Pattern:

→ Parsed Field: Source Address

→ Value Type: IPv4 (Dotted Quad)

→ Pattern Name: IPv4_DOTQUAD

Or enter new:

→ Description: IPv4 Address, Dotted Quad

→ Value Pattern: (((01)?\d\d?|2[0-4]\d|25[0-5])\.){3}([01]?

Cancel Submit

- Step 5** The key pattern is empty above since the log message starts with a value pattern.

Figure 15-14 Example: Position 2 Key Pattern for HTTP Status OK

Pattern definition for Log ID : HTTP Status OK

→ Position: 2

→ Key Pattern: \Q- - [\E

→ Parsed Field: Received Time

→ Value Type: Time

→ Pattern Name: DD/MON/YYYY:HH:MM:SS TZ

Or enter new:

→ Description: Time, Format example:
05/Oct/2004:13:08:47 -0700

→ Value Format: %d/%b/%Y:%H:%M:%S%z

→ Value Pattern: \d{1,2}\w+\d{4}:\d{1,2}:\d{1,2}:\d{1,2}

Cancel Submit

- Step 6** The Parsed Field above is a Date/Time field. In addition to Value Pattern, a value format is required since a date/time can be specified in arbitrarily different ways. Details on how to specify the value format are given in Appendix F. Several pattern names with a few of the commonly used date/time formats have been predefined.

Figure 15-15 Example: Position 3 Key Pattern for HTTP Status OK

Pattern definition for Log ID : HTTP Status OK

→ Position:

→ Key Pattern:

→ Parsed Field:

→ Value Type:

→ Pattern Name:

Or enter new:

→ Description:

→ Value Pattern:

143241

Figure 15-16 Example: Pattern log for HTTP Status OK

Patterns for Log Template : HTTP Status OK

Definition Patterns

	Position	Key Pattern	Parsed Field	Value Type	Value Format	Value Pattern
☐	1		Source Address	IPv4 Dotted Quad		(([01]?[d\d]?[2[0-4]\d 25[0-5]]\.){3}([01]?[d\d]?[2[0-4]\d 25[0-5]])
☐	2	\Q- - [\E	Received Time	Time	%d/%b/%Y:%H:%M:%S%z	\d{1,2}/\w+/\d{4}:\d{1,2}:\d{1,2}:\d{1,2} [+ -]\d{4}
☐	3	\\"([^\\"\\\\]*(\\\\)*)*\" 200	Transmitted Bytes	Number		(0x)?[a-fA-F\d]+

1 to 3 of 3

143242

Figure 15-17 Example: User Defined Log Parser for Apache Webserver1.1

User Defined Log Parser Templates

Device/Application Type: Apache Webserver 1.1

Log Templates for : Apache Webserver 1.1

Log ID	Log Description	Mapped to Event Type	Severity
HTTP Status OK	HTTP Status 200 (OK) log	HTTP Status - OK	✓

1 to 1 of 1 25 per page

After the log template is defined and submitted, you must define a reporting device based on the custom device. For more information, see [Add a Reporting Device based on a Custom Appliance Device Type](#), page 15-18.

■ Example Custom Device Type: Custom Software Application



APPENDIX A

Date/Time Format Specification

The date/time field parsing is supported using the Unix **strptime()** standard C library function.

Using **strptime()**

The **strptime()** function is the converse function to **strftime()** and converts the character string pointed to by *s* to values which are stored in the *tm* structure pointed to by *tm*, using the format specified by *format*. Here *format* is a character string that consists of field descriptors and text characters, reminiscent of **scanf(3)**. Each field descriptor consists of a **%** character followed by another character that specifies the replacement for the field descriptor. All other characters in the *format* string must have a matching character in the input string, except for whitespace, which matches zero or more whitespace characters in the input string.

The **strptime()** function processes the input string from left to right. Each of the three possible input elements (whitespace, literal, or format) are handled one after the other. If the input cannot be matched to the format string the function stops. The remainder of the format and input strings are not processed.

The supported input field descriptors are listed below. In case a text string (such as a weekday or month name) is to be matched, the comparison is case insensitive. In case a number is to be matched, leading zeros are permitted but not required.

- **% %**—The **%** character.
- **%a or %A**—The weekday name according to the current locale, in abbreviated form or the full name.
- **%b or %B or %h**—The month name according to the current locale, in abbreviated form or the full name.
- **%c**—The date and time representation for the current locale.
- **%C**—The century number (0-99).
- **%d or %e**—The day of month (1-31).
- **%D**—Equivalent to **%m/%d/%y**. (This is the American style date, very confusing to non-Americans, especially since **%d/%m/%y** is widely used in Europe. The ISO 8601 standard format is **%Y-%m-%d**.)
- **%H**—The hour (0-23).
- **%I**—The hour on a 12-hour clock (1-12).
- **%j**—The day number in the year (1-366).
- **%m**—The month number (1-12).

- **%M**—The minute (0-59).
- **%n or %t**—Arbitrary whitespace.
- **%p**—The locale's equivalent of AM or PM. (Note: there may be none.)
- **%r**—The 12-hour clock time (using the locale's AM or PM). In the POSIX locale equivalent to **%I:%M:%S %p**. If `t_fmt_ampm` is empty in the `LC_TIME` part of the current locale then the behaviour is undefined.
- **%R**—Equivalent to **%H:%M**.
- **%S**—The second (0-60; 60 may occur for leap seconds; earlier also 61 was allowed).
- **%T**—Equivalent to **%H:%M:%S**.
- **%U**—The week number with Sunday the first day of the week (0-53). The first Sunday of January is the first day of week 1.
- **%w**—The weekday number (0-6) with Sunday = 0.
- **%W**—The week number with Monday the first day of the week (0-53). The first Monday of January is the first day of week 1.
- **%x**—The date, using the locale's date format.
- **%X**—The time, using the locale's time format.
- **%y**—The year within century (0-99). When a century is not otherwise specified, values in the range 69-99 refer to years in the twentieth century (1969-1999); values in the range 00-68 refer to years in the twenty-first century (2000-2068).
- **%Y**—The year, including century (for example, 1991).

Some field descriptors can be modified by the E or O modifier characters to indicate that an alternative format or specification should be used. If the alternative format or specification does not exist in the current locale, the unmodified field descriptor is used.

The E modifier specifies that the input string may contain alternative locale-dependent versions of the date and time representation:

- **%Ec**—The locale's alternative date and time representation.
- **%EC**—The name of the base year (period) in the locale's alternative representation.
- **%Ex**—The locale's alternative date representation.
- **%EX**—The locale's alternative time representation.
- **%Ey**—The offset from **%EC** (year only) in the locale's alternative representation.
- **%EY**—The full alternative year representation.

The O modifier specifies that the numerical input may be in an alternative locale-dependent format:

- **%Od or %Oe**—The day of the month using the locale's alternative numeric symbols; leading zeros are permitted but not required.
- **%OH**—The hour (24-hour clock) using the locale's alternative numeric symbols.
- **%OI**—The hour (12-hour clock) using the locale's alternative numeric symbols.
- **%Om**—The month using the locale's alternative numeric symbols.
- **%OM**—The minutes using the locale's alternative numeric symbols.
- **%OS**—The seconds using the locale's alternative numeric symbols.
- **%OU**—The week number of the year (Sunday as the first day of the week) using the locale's alternative numeric symbols.

- **%Ow**—The number of the weekday (Sunday=0) using the locale's alternative numeric symbols.
- **%OW**—The week number of the year (Monday as the first day of the week) using the locale's alternative numeric symbols.
- **%Oy**—The year (offset from **%C**) using the locale's alternative numeric symbols.
- **%F**—Equivalent to **%Y-%m-%d**, the ISO 8601 date format.
- **%g**—The year corresponding to the ISO week number, but without the century (0-99).
- **%G**—The year corresponding to the ISO week number. (For example, 1991.)
- **%u**—The day of the week as a decimal number (1-7, where Monday = 1).
- **%V**—The ISO 8601:1988 week number as a decimal number (1-53). If the week (starting on Monday) containing 1 January has four or more days in the new year, then it is considered week 1. Otherwise, it is the last week of the previous year, and the next week is week 1.
- **%z**—An RFC-822/ISO 8601 standard time zone specification.
- **%Z**—The timezone name.

Similarly, because of GNU extensions to `strptime`, **%k** is accepted as a synonym for **%H**, and **%l** should be accepted as a synonym for **%I**, and **%P** is accepted as a synonym for **%p**.

- **%s**—The number of seconds since the epoch, that is, since 1970-01-01 00:00:00 UTC. Leap seconds are not counted unless leap second support is available.



APPENDIX **B**

Regular Expression Reference

The following topics detail the regular expression syntax used by the custom parser feature in MARS.

This chapter contains the following topics:

- [PCRE Regular Expression Details, page B-2](#)
- [Backslash, page B-3](#)
- [Circumflex and Dollar, page B-7](#)
- [Full Stop \(Period, Dot\), page B-8](#)
- [Matching a Single Byte, page B-8](#)
- [Square Brackets and Character Classes, page B-8](#)
- [Posix Character Classes, page B-9](#)
- [Vertical Bar, page B-10](#)
- [Internal Option Setting, page B-10](#)
- [Subpatterns, page B-11](#)
- [Named Subpatterns, page B-12](#)
- [Repetition, page B-12](#)
- [Atomic Grouping and Possessive Quantifiers, page B-14](#)
- [Back References, page B-15](#)
- [Assertions, page B-16](#)
- [Conditional Subpatterns, page B-18](#)
- [Comments, page B-19](#)
- [Recursive Patterns, page B-19](#)
- [Subpatterns as Subroutines, page B-21](#)
- [Callouts, page B-21](#)

PCRE Regular Expression Details

The syntax and semantics of the regular expressions supported by PCRE are described below. Regular expressions are also described in the Perl documentation and in several books, some of which have copious examples. Jeffrey Friedl's *Mastering Regular Expressions*, published by O'Reilly, covers regular expressions in great detail. This description of PCRE's regular expressions is intended as reference material.

The original operation of PCRE was on strings of one-byte characters. However, there is now also support for UTF-8 character strings. To use this, you must build PCRE to include UTF-8 support, and then call `pcre_compile()` with the `PCRE_UTF8` option. How this affects pattern matching is mentioned in several places below. There is also a summary of UTF-8 features in the section on UTF-8 support in the main PCRE page.

A regular expression is a pattern that is matched against a subject string from left to right. Most characters stand for themselves in a pattern, and match the corresponding characters in the subject. As a simple example, the pattern

```
The quick brown fox
```

matches a portion of a subject string that is identical to itself. The power of regular expressions comes from the ability to include alternatives and repetitions in the pattern. These are encoded in the pattern by the use of metacharacters, which do not stand for themselves but instead are interpreted in some special way.

There are two different sets of *metacharacters*: those that are recognized anywhere in the pattern except within square brackets, and those that are recognized in square brackets. Outside square brackets, the metacharacters are as follows:

```
\      general escape character with several uses
^      assert start of string (or line, in multiline mode)
$      assert end of string (or line, in multiline mode)
.      match any character except newline (by default)
[      start character class definition
|      start of alternative branch
(      start subpattern
)      end subpattern
?      extends the meaning of (
      also 0 or 1 quantifier
      also quantifier minimizer
*      0 or more quantifier
+      1 or more quantifier
      also "possessive quantifier"
{      start min/max quantifier
```

Part of a pattern that is in square brackets is called a "character class." In a character class the only metacharacters are:

```
\      general escape character
^      negate the class, but only if the first character
-      indicates character range
[      POSIX character class (only if followed by POSIX syntax)
]      terminates the character class
```

The following sections describe the use of each metacharacter.

Backslash

The backslash character has several uses. First, if it is followed by a non-alphanumeric character, it takes away any special meaning that character may have. This use of backslash as an escape character applies both inside and outside character classes.

For example, if you want to match a `*` character, you write `\*` in the pattern. This escaping action applies whether or not the following character would otherwise be interpreted as a metacharacter, so it is always safe to precede a non-alphanumeric with backslash to specify that it stands for itself. In particular, if you want to match a backslash, you write `\\`.

If a pattern is compiled with the `PCRE_EXTENDED` option, whitespace in the pattern (other than in a character class) and characters between a `#` outside a character class and the next newline character are ignored. An escaping backslash can be used to include a whitespace or `#` character as part of the pattern.

If you want to remove the special meaning from a sequence of characters, you can do so by putting them between `\Q` and `\E`. This is different from Perl in that `$` and `@` are handled as literals in `\Q...\E` sequences in PCRE, whereas in Perl, `$` and `@` cause variable interpolation. Note the following examples:

Pattern	PCRE matches	Perl matches
<code>\Qabc\$xyz\E</code>	<code>abc\$xyz</code>	<code>abc</code> followed by the contents of <code>\$xyz</code>
<code>\Qabc\ \$xyz\E</code>	<code>abc\ \$xyz</code>	<code>abc\ \$xyz</code>
<code>\Qabc\E\ \$Qxyz\E</code>	<code>abc\$xyz</code>	<code>abc\$xyz</code>

The `\Q...\E` sequence is recognized both inside and outside character classes.

Non-printing Characters

A second use of backslash provides a way of encoding non-printing characters in patterns in a visible manner. There is no restriction on the appearance of non-printing characters, apart from the binary zero that terminates a pattern, but when a pattern is being prepared by text editing, it is usually easier to use one of the following escape sequences than the binary character it represents:

<code>\a</code>	alarm, that is, the BEL character (hex 07)
<code>\cx</code>	"control-x", where x is any character
<code>\e</code>	escape (hex 1B)
<code>\f</code>	formfeed (hex 0C)
<code>\n</code>	newline (hex 0A)
<code>\r</code>	carriage return (hex 0D)
<code>\t</code>	tab (hex 09)
<code>\ddd</code>	character with octal code ddd, or backreference
<code>\xhh</code>	character with hex code hh
<code>\x{hhh..}</code>	character with hex code hhh... (UTF-8 mode only)

The precise effect of `\cx` is as follows: if x is a lowercase letter, it is converted to uppercase. Then bit 6 of the character (hex 40) is inverted. Thus `\cz` becomes hex 1A, but `\c{` becomes hex 3B, while `\c;` becomes hex 7B.

After `\x`, from zero to two hexadecimal digits are read (letters can be in upper or lower case). In UTF-8 mode, any number of hexadecimal digits may appear between `\x{` and `}`, but the value of the character code must be less than 2^{31} (that is, the maximum hexadecimal value is 7FFFFFFF). If characters other than hexadecimal digits appear between `\x{` and `}`, or if there is no terminating `}`, this form of escape is not recognized. Instead, the initial `\x` will be interpreted as a basic hexadecimal escape, with no following digits, giving a character whose value is zero.

Characters whose value is less than 256 can be defined by either of the two syntaxes for `\x` when PCRE is in UTF-8 mode. There is no difference in the way they are handled. For example, `\xdc` is exactly the same as `\x{dc}`.

After `\0`, up to two further octal digits are read. In both cases, if there are fewer than two digits, just those that are present are used. Thus the sequence `\0\x07` specifies two binary zeros followed by a BEL character (code value 7). Make sure you supply two digits after the initial zero if the pattern character that follows is itself an octal digit.

The handling of a backslash followed by a digit other than 0 is complicated. Outside a character class, PCRE reads it and any following digits as a decimal number. If the number is less than 10, or if there have been at least that many previous capturing left parentheses in the expression, the entire sequence is taken as a back reference. A description of how this works is given later, following the discussion of parenthesized subpatterns.

Inside a character class, or if the decimal number is greater than 9 and there have not been that many capturing subpatterns, PCRE re-reads up to three octal digits following the backslash, and generates a single byte from the least significant 8 bits of the value. Any subsequent digits stand for themselves. For example:

```
\040  is another way of writing a space
\40   is the same, provided there are fewer than 40 previous capturing subpatterns
\7    is always a back reference
\11   might be a back reference, or another way of writing a tab
\011  is always a tab
\0113 is a tab followed by the character "3"
\113  might be a back reference, otherwise the character with octal code 113
\377  might be a back reference, otherwise the byte consisting entirely of 1 bits
\81   is either a back reference, or a binary zero followed by the two characters "8" and "1"
```

Octal values of 100 or greater must not be introduced by a leading zero, because no more than three octal digits are ever read.

All the sequences that define a single byte value or a single UTF-8 character (in UTF-8 mode) can be used both inside and outside character classes. In addition, inside a character class, the sequence `\b` is interpreted as the backspace character (hex 08), and the sequence `\X` is interpreted as the character "X". Outside a character class, these sequences have different meanings (see [Unicode Character Properties](#), page B-5).

Generic Character Types

The third use of backslash is for specifying generic character types. The following are always recognized:

```
\d    any decimal digit
\D    any character that is not a decimal digit
\s    any whitespace character
\S    any character that is not a whitespace character
\w    any "word" character
\W    any "non-word" character
```

Each pair of escape sequences partitions the complete set of characters into two disjoint sets. Any given character matches one, and only one, of each pair.

These character type sequences can appear both inside and outside character classes. They each match one character of the appropriate type. If the current matching point is at the end of the subject string, all of them fail, since there is no character to match.

For compatibility with Perl, `\s` does not match the VT character (code 11). This makes it different from the POSIX "space" class. The `\s` characters are HT (9), LF (10), FF (12), CR (13), and space (32).

A "word" character is an underscore or any character less than 256 that is a letter or digit. The definition of letters and digits is controlled by PCRE's low-valued character tables, and may vary if locale-specific matching is taking place (see "Locale support" in the [pcreapi](#) page). For example, in the "fr_FR" (French) locale, some character codes greater than 128 are used for accented letters, and these are matched by `\w`.

In UTF-8 mode, characters with values greater than 128 never match `\d`, `\s`, or `\w`, and always match `\D`, `\S`, and `\W`. This is true even when Unicode character property support is available.

Unicode Character Properties

When PCRE is built with Unicode character property support, three additional escape sequences to match generic character types are available when UTF-8 mode is selected. They are:

```
\p{xx}  a character with the xx property
\P{xx}  a character without the xx property
\X      an extended Unicode sequence
```

The property names represented by `xx` above are limited to the Unicode general category properties. Each character has exactly one such property, specified by a two-letter abbreviation. For compatibility with Perl, negation can be specified by including a circumflex between the opening brace and the property name. For example, `\p{^Lu}` is the same as `\P{Lu}`.

If only one letter is specified with `\p` or `\P`, it includes all the properties that start with that letter. In this case, in the absence of negation, the curly brackets in the escape sequence are optional; these two examples have the same effect:

```
\p{L}
\pL
```

The following property codes are supported:

C	Other
Cc	Control
Cf	Format
Cn	Unassigned
Co	Private use
Cs	Surrogate
L	Letter
Ll	Lower case letter
Lm	Modifier letter
Lo	Other letter
Lt	Title case letter
Lu	Upper case letter
M	Mark
Mc	Spacing mark
Me	Enclosing mark
Mn	Non-spacing mark
N	Number
Nd	Decimal number
Nl	Letter number
No	Other number
P	Punctuation
Pc	Connector punctuation

Pd	Dash punctuation
Pe	Close punctuation
Pf	Final punctuation
Pi	Initial punctuation
Po	Other punctuation
Ps	Open punctuation
S	Symbol
Sc	Currency symbol
Sk	Modifier symbol
Sm	Mathematical symbol
So	Other symbol
Z	Separator
Zl	Line separator
Zp	Paragraph separator
Zs	Space separator

Extended properties such as "Greek" or "InMusicalSymbols" are not supported by PCRE.

Specifying caseless matching does not affect these escape sequences. For example, `\p{Lu}` always matches only uppercase letters.

The `\X` escape matches any number of Unicode characters that form an extended Unicode sequence. `\X` is equivalent to

```
(?>\PM\pM*)
```

That is, it matches a character without the "mark" property, followed by zero or more characters with the "mark" property, and treats the sequence as an atomic group (see below). Characters with the "mark" property are typically accents that affect the preceding character.

Matching characters by Unicode property is not fast, because PCRE has to search a structure that contains data for over fifteen thousand characters. That is why the traditional escape sequences such as `\d` and `\w` do not use Unicode properties in PCRE.

Simple Assertions

The fourth use of backslash is for certain simple assertions. An assertion specifies a condition that has to be met at a particular point in a match, without consuming any characters from the subject string. The use of subpatterns for more complicated assertions is described below. The backslashed assertions are:

<code>\b</code>	matches at a word boundary
<code>\B</code>	matches when not at a word boundary
<code>\A</code>	matches at start of subject
<code>\Z</code>	matches at end of subject or before newline at end
<code>\z</code>	matches at end of subject
<code>\G</code>	matches at first matching position in subject

These assertions may not appear in character classes (but note that `\b` has a different meaning, namely the backspace character, inside a character class).

A word boundary is a position in the subject string where the current character and the previous character do not both match `\w` or `\W` (that is, one matches `\w` and the other matches `\W`), or the start or end of the string if the first or last character matches `\w`, respectively.

The `\A`, `\Z`, and `\z` assertions differ from the traditional circumflex and dollar (described in the next section) in that they only ever match at the very start and end of the subject string, whatever options are set. Thus, they are independent of multiline mode. These three assertions are not affected by the `PCRE_NOTBOL` or `PCRE_NOTEOL` options, which affect only the behavior of the circumflex and

dollar metacharacters. However, if the `startoffset` argument of `pcre_exec()` is non-zero, indicating that matching is to start at a point other than the beginning of the subject, `\A` can never match. The difference between `\Z` and `\z` is that `\Z` matches before a newline that is the last character of the string as well as at the end of the string, whereas `\z` matches only at the end.

The `\G` assertion is true only when the current matching position is at the start point of the match, as specified by the `startoffset` argument of `pcre_exec()`. It differs from `\A` when the value of `startoffset` is non-zero. By calling `pcre_exec()` multiple times with appropriate arguments, you can mimic Perl's `/g` option, and it is in this kind of implementation where `\G` can be useful.

Note, however, that PCRE's interpretation of `\G`, as the start of the current match, is subtly different from Perl's, which defines it as the end of the previous match. In Perl, these can be different when the previously matched string was empty. Because PCRE does just one match at a time, it cannot reproduce this behavior.

If all the alternatives of a pattern begin with `\G`, the expression is anchored to the starting match position, and the "anchored" flag is set in the compiled regular expression.

Circumflex and Dollar

Outside a character class, in the default matching mode, the circumflex character is an assertion that is true only if the current matching point is at the start of the subject string. If the `startoffset` argument of `pcre_exec()` is non-zero, circumflex can never match if the `PCRE_MULTILINE` option is unset. Inside a character class, circumflex has an entirely different meaning (see [Square Brackets and Character Classes](#), page B-8 and [Posix Character Classes](#), page B-9).

Circumflex need not be the first character of the pattern if a number of alternatives are involved, but it should be the first thing in each alternative in which it appears if the pattern is ever to match that branch. If all possible alternatives start with a circumflex, that is, if the pattern is constrained to match only at the start of the subject, it is said to be an "anchored" pattern. (There are also other constructs that can cause a pattern to be anchored.)

A dollar character is an assertion that is true only if the current matching point is at the end of the subject string, or immediately before a newline character that is the last character in the string (by default). Dollar need not be the last character of the pattern if a number of alternatives are involved, but it should be the last item in any branch in which it appears. Dollar has no special meaning in a character class.

The meaning of dollar can be changed so that it matches only at the very end of the string, by setting the `PCRE_DOLLAR_ENDONLY` option at compile time. This does not affect the `\Z` assertion.

The meanings of the circumflex and dollar characters are changed if the `PCRE_MULTILINE` option is set. When this is the case, they match immediately after and immediately before an internal newline character, respectively, in addition to matching at the start and end of the subject string. For example, the pattern `/^abc$/` matches the subject string "def\nabc" (where `\n` represents a newline character) in multiline mode, but not otherwise. Consequently, patterns that are anchored in single line mode because all branches start with `^` are not anchored in multiline mode, and a match for circumflex is possible when the `startoffset` argument of `pcre_exec()` is non-zero. The `PCRE_DOLLAR_ENDONLY` option is ignored if `PCRE_MULTILINE` is set.

The sequences `\A`, `\Z`, and `\z` can be used to match the start and end of the subject in both modes, and if all branches of a pattern start with `\A` it is always anchored, whether `PCRE_MULTILINE` is set or not.

Full Stop (Period, Dot)

Outside a character class, a dot in the pattern matches any one character in the subject, including a non-printing character, but not (by default) newline. In UTF-8 mode, a dot matches any UTF-8 character, which might be more than one byte long, except (by default) newline. If the `PCRE_DOTALL` option is set, dots match newlines as well. The handling of dot is entirely independent of the handling of circumflex and dollar, the only relationship being that they both involve newline characters. Dot has no special meaning in a character class.

Matching a Single Byte

Outside a character class, the escape sequence `\C` matches any one byte, both in and out of UTF-8 mode. Unlike a dot, it can match a newline. The feature is provided in Perl in order to match individual bytes in UTF-8 mode. Because it breaks up UTF-8 characters into individual bytes, what remains in the string may be a malformed UTF-8 string. For this reason, the `\C` escape sequence is best avoided.

PCRE does not allow `\C` to appear in lookbehind assertions (described below), because in UTF-8 mode this would make it impossible to calculate the length of the lookbehind.

Square Brackets and Character Classes

An opening square bracket introduces a character class, terminated by a closing square bracket. A closing square bracket on its own is not special. If a closing square bracket is required as a member of the class, it should be the first data character in the class (after an initial circumflex, if present) or escaped with a backslash.

A character class matches a single character in the subject. In UTF-8 mode, the character may occupy more than one byte. A matched character must be in the set of characters defined by the class, unless the first character in the class definition is a circumflex, in which case the subject character must not be in the set defined by the class. If a circumflex is actually required as a member of the class, ensure it is not the first character, or escape it with a backslash.

For example, the character class `[aeiou]` matches any lower case vowel, while `^[aeiou]` matches any character that is not a lower case vowel. A circumflex is just a convenient notation for specifying the characters that are in the class by enumerating those that are not. A class that starts with a circumflex is not an assertion: it still consumes a character from the subject string, and therefore it fails if the current pointer is at the end of the string.

In UTF-8 mode, characters with values greater than 255 can be included in a class as a literal string of bytes, or by using the `\x{ }` escaping mechanism.

When caseless matching is set, any letters in a class represent both their upper case and lower case versions, so for example, a caseless `[aeiou]` matches "A" as well as "a", and a caseless `^[aeiou]` does not match "A", whereas a careful version would. When running in UTF-8 mode, PCRE supports the concept of case for characters with values greater than 128 only when it is compiled with Unicode property support.

The newline character is never treated in any special way in character classes, whatever the setting of the `PCRE_DOTALL` or `PCRE_MULTILINE` options is. A class such as `^[a]` will always match a newline.

The minus (hyphen) character can be used to specify a range of characters in a character class. For example, `[d-m]` matches any letter between d and m, inclusive. If a minus character is required in a class, it must be escaped with a backslash or appear in a position where it cannot be interpreted as indicating a range, typically as the first or last character in the class.

It is not possible to have the literal character "]" as the end character of a range. A pattern such as `[W-]46]` is interpreted as a class of two characters ("W" and "-") followed by a literal string "46]", so it would match "W46]" or "-46]". However, if the "]" is escaped with a backslash it is interpreted as the end of range, so `[W-\\]46]` is interpreted as a class containing a range followed by two other characters. The octal or hexadecimal representation of "]" can also be used to end a range.

Ranges operate in the collating sequence of character values. They can also be used for characters specified numerically, for example `[\000-\037]`. In UTF-8 mode, ranges can include characters whose values are greater than 255, for example `[\x{100}-\x{2ff}]`.

If a range that includes letters is used when caseless matching is set, it matches the letters in either case. For example, `[W-c]` is equivalent to `[][\^\_`wxyzabc]`, matched caselessly, and in non-UTF-8 mode, if character tables for the "fr\_FR" locale are in use, `[\xc8-\xcb]` matches accented E characters in both cases. In UTF-8 mode, PCRE supports the concept of case for characters with values greater than 128 only when it is compiled with Unicode property support.

The character types `\d`, `\D`, `\p`, `\P`, `\s`, `\S`, `\w`, and `\W` may also appear in a character class, and add the characters that they match to the class. For example, `[\dABCDEF]` matches any hexadecimal digit. A circumflex can conveniently be used with the uppercase character types to specify a more restricted set of characters than the matching lower case type. For example, the class `^[^W_]` matches any letter or digit, but not underscore.

The only metacharacters that are recognized in character classes are backslash, hyphen (only where it can be interpreted as specifying a range), circumflex (only at the start), opening square bracket (only when it can be interpreted as introducing a POSIX class name - see the next section), and the terminating closing square bracket. However, escaping other non-alphanumeric characters does no harm.

Posix Character Classes

Perl supports the POSIX notation for character classes. This uses names enclosed by `[:` and `:]` within the enclosing square brackets. PCRE also supports this notation. For example,

```
[01[:alpha:]]%
```

matches "0", "1", any alphabetic character, or "%". The supported class names are

<code>alnum</code>	letters and digits
<code>alpha</code>	letters
<code>ascii</code>	character codes 0 - 127
<code>blank</code>	space or tab only
<code>cntrl</code>	control characters
<code>digit</code>	decimal digits (same as <code>\d</code>)
<code>graph</code>	printing characters, excluding space
<code>lower</code>	lower case letters
<code>print</code>	printing characters, including space
<code>punct</code>	printing characters, excluding letters and digits
<code>space</code>	white space (not quite the same as <code>\s</code>)
<code>upper</code>	upper case letters
<code>word</code>	"word" characters (same as <code>\w</code>)
<code>xdigit</code>	hexadecimal digits

The "space" characters are HT (9), LF (10), VT (11), FF (12), CR (13), and space (32). Notice that this list includes the VT character (code 11). This makes "space" different to `\s`, which does not include VT (for Perl compatibility).

The name "word" is a Perl extension, and "blank" is a GNU extension from Perl 5.8. Another Perl extension is negation, which is indicated by a `^` character after the colon. For example,

```
[12[:^digit:]]
```

matches "1", "2", or any non-digit. PCRE (and Perl) also recognize the POSIX syntax `[.ch.]` and `[=ch=]` where "ch" is a "collating element", but these are not supported, and an error is given if they are encountered.

In UTF-8 mode, characters with values greater than 128 do not match any of the POSIX character classes.

Vertical Bar

Vertical bar characters are used to separate alternative patterns. For example, the pattern

```
gilbert|sullivan
```

matches either "gilbert" or "sullivan". Any number of alternatives may appear, and an empty alternative is permitted (matching the empty string). The matching process tries each alternative in turn, from left to right, and the first one that succeeds is used. If the alternatives are within a subpattern (defined below), "succeeds" means matching the rest of the main pattern as well as the alternative in the subpattern.

Internal Option Setting

The settings of the `PCRE_CASELESS`, `PCRE_MULTILINE`, `PCRE_DOTALL`, and `PCRE_EXTENDED` options can be changed from within the pattern by a sequence of Perl option letters enclosed between `"(?"` and `)"`. The option letters are

```
i for PCRE_CASELESS
m for PCRE_MULTILINE
s for PCRE_DOTALL
x for PCRE_EXTENDED
```

For example, `(?im)` sets caseless, multiline matching. It is also possible to unset these options by preceding the letter with a hyphen, and a combined setting and unsetting such as `(?im-sx)`, which sets `PCRE_CASELESS` and `PCRE_MULTILINE` while unsetting `PCRE_DOTALL` and `PCRE_EXTENDED`, is also permitted. If a letter appears both before and after the hyphen, the option is unset.

When an option change occurs at top level (that is, not inside subpattern parentheses), the change applies to the remainder of the pattern that follows. If the change is placed right at the start of a pattern, PCRE extracts it into the global options (and it will therefore show up in data extracted by the `pcre_fullinfo()` function).

An option change within a subpattern affects only that part of the current pattern that follows it, so

```
(a(?i)b)c
```

matches `abc` and `aBc` and no other strings (assuming `PCRE_CASELESS` is not used). By this means, options can be made to have different settings in different parts of the pattern. Any changes made in one alternative do carry on into subsequent branches within the same subpattern. For example,


```
(a(?i)b|c)
```

matches "ab", "aB", "c", and "C", even though when matching "C" the first branch is abandoned before the option setting. This is because the effects of option settings happen at compile time. There would be some very weird behavior otherwise.

The PCRE-specific options PCRE_UNGREEDY and PCRE_EXTRA can be changed in the same way as the Perl-compatible options by using the characters U and X respectively. The (?X) flag setting is special in that it must always occur earlier in the pattern than any of the additional features it turns on, even when it is at top level. It is best to put it at the start.

Subpatterns

Subpatterns are delimited by parentheses (round brackets), which can be nested. Turning part of a pattern into a subpattern does two things:

Step 1 It localizes a set of alternatives. For example, the pattern :

```
cat(aract|erpillar|)
```

matches one of the words "cat", "cataract", or "caterpillar". Without the parentheses, it would match "cataract", "erpillar" or the empty string.

Step 2 It sets up the subpattern as a capturing subpattern. This means that, when the whole pattern matches, the portion of the subject string that matched the subpattern is passed back to the caller via the ovector argument of **pcre_exec()**. Opening parentheses are counted from left to right (starting from 1) to obtain numbers for the capturing subpatterns.

For example, if the string "the red king" is matched against the pattern

```
the ((red|white) (king|queen))
```

the captured substrings are "red king", "red", and "king", and are numbered 1, 2, and 3, respectively.

The fact that plain parentheses fulfill two functions is not always helpful. There are often times when a grouping subpattern is required without a capturing requirement. If an opening parenthesis is followed by a question mark and a colon, the subpattern does not do any capturing, and is not counted when computing the number of any subsequent capturing subpatterns. For example, if the string "the white queen" is matched against the pattern

```
the (?:red|white) (king|queen)
```

the captured substrings are "white queen" and "queen", and are numbered 1 and 2. The maximum number of capturing subpatterns is 65535, and the maximum depth of nesting of all subpatterns, both capturing and non-capturing, is 200.

As a convenient shorthand, if any option settings are required at the start of a non-capturing subpattern, the option letters may appear between the "?" and the ":". Thus the two patterns

```
(?i:saturday|sunday)
```

```
(?:(?i)saturday|sunday)
```

match exactly the same set of strings. Because alternative branches are tried from left to right, and options are not reset until the end of the subpattern is reached, an option setting in one branch does affect subsequent branches, so the above patterns match "SUNDAY" as well as "Saturday".

Named Subpatterns

Identifying capturing parentheses by number is simple, but it can be very hard to keep track of the numbers in complicated regular expressions. Furthermore, if an expression is modified, the numbers may change. To help with this difficulty, PCRE supports the naming of subpatterns, something that Perl does not provide. The Python syntax (*?P<name>...*) is used. Names consist of alphanumeric characters and underscores, and must be unique within a pattern.

Named capturing parentheses are still allocated numbers as well as names. The PCRE API provides function calls for extracting the name-to-number translation table from a compiled pattern. There is also a convenience function for extracting a captured substring by name. For further details see the *pcreapi* documentation.

Repetition

Repetition is specified by quantifiers, which can follow any of the following items:

- a literal data character
- the `.` metacharacter
- the `\C` escape sequence
- the `\X` escape sequence (in UTF-8 mode with Unicode properties)
- an escape such as `\d` that matches a single character
- a character class
- a back reference (see next section)
- a parenthesized subpattern (unless it is an assertion)

The general repetition quantifier specifies a minimum and maximum number of permitted matches, by giving the two numbers in curly brackets (braces), separated by a comma. The numbers must be less than 65536, and the first must be less than or equal to the second. For example:

```
z{2,4}
```

matches "zz", "zzz", or "zzzz". A closing brace on its own is not a special character. If the second number is omitted, but the comma is present, there is no upper limit; if the second number and the comma are both omitted, the quantifier specifies an exact number of required matches. Thus

```
[aeiou]{3,}
```

matches at least 3 successive vowels, but may match many more, while

```
\d{8}
```

matches exactly 8 digits. An opening curly bracket that appears in a position where a quantifier is not allowed, or one that does not match the syntax of a quantifier, is taken as a literal character. For example, `{,6}` is not a quantifier, but a literal string of four characters.

In UTF-8 mode, quantifiers apply to UTF-8 characters rather than to individual bytes. Thus, for example, `\x{100}{2}` matches two UTF-8 characters, each of which is represented by a two-byte sequence. Similarly, when Unicode property support is available, `\X{3}` matches three Unicode extended sequences, each of which may be several bytes long (and they may be of different lengths).

The quantifier `{0}` is permitted, causing the expression to behave as if the previous item and the quantifier were not present.

For convenience (and historical compatibility) the three most common quantifiers have single-character abbreviations:

- `*` is equivalent to `{0,}`
- `+` is equivalent to `{1,}`

`?` is equivalent to `{0,1}`

It is possible to construct infinite loops by following a subpattern that can match no characters with a quantifier that has no upper limit, for example:

```
(a?)*
```

Earlier versions of Perl and PCRE used to give an error at compile time for such patterns. However, because there are cases where this can be useful, such patterns are now accepted, but if any repetition of the subpattern does in fact match no characters, the loop is forcibly broken.

By default, the quantifiers are "greedy", that is, they match as much as possible (up to the maximum number of permitted times), without causing the rest of the pattern to fail. The classic example of where this gives problems is in trying to match comments in C programs. These appear between `/*` and `*/` and within the comment, individual `*` and `/` characters may appear. An attempt to match C comments by applying the pattern

```
/\*. *\*/
```

to the string

```
/* first comment */ not comment /* second comment */
```

fails, because it matches the entire string owing to the greediness of the `.*` item.

However, if a quantifier is followed by a question mark, it ceases to be greedy, and instead matches the minimum number of times possible, so the pattern

```
/\*. *?\*/
```

does the right thing with the C comments. The meaning of the various quantifiers is not otherwise changed, just the preferred number of matches. Do not confuse this use of question mark with its use as a quantifier in its own right. Because it has two uses, it can sometimes appear doubled, as in

```
\d??\d
```

which matches one digit by preference, but can match two if that is the only way the rest of the pattern matches.

If the `PCRE_UNGREEDY` option is set (an option which is not available in Perl), the quantifiers are not greedy by default, but individual ones can be made greedy by following them with a question mark. In other words, it inverts the default behavior.

When a parenthesized subpattern is quantified with a minimum repeat count that is greater than 1 or with a limited maximum, more memory is required for the compiled pattern, in proportion to the size of the minimum or maximum.

If a pattern starts with `.*` or `{0,}` and the `PCRE_DOTALL` option (equivalent to Perl's `/s`) is set, thus allowing the `.` to match newlines, the pattern is implicitly anchored, because whatever follows will be tried against every character position in the subject string, so there is no point in retrying the overall match at any position after the first. PCRE normally treats such a pattern as though it were preceded by `\A`.

In cases where it is known that the subject string contains no newlines, it is worth setting `PCRE_DOTALL` in order to obtain this optimization, or alternatively using `^` to indicate anchoring explicitly.

However, there is one situation where the optimization cannot be used. When `.*` is inside capturing parentheses that are the subject of a backreference elsewhere in the pattern, a match at the start may fail, and a later one succeed. Consider, for example:

```
(.*)abc\1
```

If the subject is "xyz123abc123" the match point is the fourth character. For this reason, such a pattern is not implicitly anchored.

When a capturing subpattern is repeated, the value captured is the substring that matched the final iteration. For example, after

```
(tweedle[dume]{3}\s*)+
```

has matched "tweedledum tweedledee" the value of the captured substring is "tweedledee". However, if there are nested capturing subpatterns, the corresponding captured values may have been set in previous iterations. For example, after

```
/(a|(b))+/
```

matches "aba" the value of the second captured substring is "b".

Atomic Grouping and Possessive Quantifiers

With both maximizing and minimizing repetition, failure of what follows normally causes the repeated item to be re-evaluated to see if a different number of repeats allows the rest of the pattern to match. Sometimes it is useful to prevent this, either to change the nature of the match, or to cause it fail earlier than it otherwise might, when the author of the pattern knows there is no point in carrying on.

Consider, for example, the pattern `\d+foo` when applied to the subject line

```
123456bar
```

After matching all 6 digits and then failing to match "foo", the normal action of the matcher is to try again with only 5 digits matching the `\d+` item, and then with 4, and so on, before ultimately failing. "Atomic grouping" (a term taken from Jeffrey Friedl's book) provides the means for specifying that once a subpattern has matched, it is not to be re-evaluated in this way.

If we use atomic grouping for the previous example, the matcher would give up immediately on failing to match "foo" the first time. The notation is a kind of special parenthesis, starting with `(?>` as in this example:

```
(?>\d+)foo
```

This kind of parenthesis "locks up" the part of the pattern it contains once it has matched, and a failure further into the pattern is prevented from backtracking into it. Backtracking past it to previous items, however, works as normal.

An alternative description is that a subpattern of this type matches the string of characters that an identical standalone pattern would match, if anchored at the current point in the subject string.

Atomic grouping subpatterns are not capturing subpatterns. Simple cases such as the above example can be thought of as a maximizing repeat that must swallow everything it can. So, while both `\d+` and `\d+?` are prepared to adjust the number of digits they match in order to make the rest of the pattern match, `(?>\d+)` can only match an entire sequence of digits.

Atomic groups in general can of course contain arbitrarily complicated subpatterns, and can be nested. However, when the subpattern for an atomic group is just a single repeated item, as in the example above, a simpler notation, called a "possessive quantifier" can be used. This consists of an additional `+` character following a quantifier. Using this notation, the previous example can be rewritten as

```
\d++foo
```

Possessive quantifiers are always greedy; the setting of the PCRE_UNGREEDY option is ignored. They are a convenient notation for the simpler forms of atomic group. However, there is no difference in the meaning or processing of a possessive quantifier and the equivalent atomic group.

The possessive quantifier syntax is an extension to the Perl syntax. It originates in Sun's Java package.

When a pattern contains an unlimited repeat inside a subpattern that can itself be repeated an unlimited number of times, the use of an atomic group is the only way to avoid some failing matches taking a very long time indeed. The pattern

```
(\D+|<\d+>)*[!?]
```

matches an unlimited number of substrings that either consist of non-digits, or digits enclosed in <>, followed by either ! or ?. When it matches, it runs quickly. However, if it is applied to

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

it takes a long time before reporting failure. This is because the string can be divided between the internal \D+ repeat and the external * repeat in a large number of ways, and all have to be tried. (The example uses [!?] rather than a single character at the end, because both PCRE and Perl have an optimization that allows for fast failure when a single character is used. They remember the last single character that is required for a match, and fail early if it is not present in the string.) If the pattern is changed so that it uses an atomic group, like this:

```
((?>\D+)|<\d+>)*[!?]
```

sequences of non-digits cannot be broken, and failure happens quickly.

Back References



Note

Cisco Security MARS does not support numbered back references.

Outside a character class, a backslash followed by a digit greater than 0 (and possibly further digits) is a back reference to a capturing subpattern earlier (that is, to its left) in the pattern, provided there have been that many previous capturing left parentheses.

However, if the decimal number following the backslash is less than 10, it is always taken as a back reference, and causes an error only if there are not that many capturing left parentheses in the entire pattern. In other words, the parentheses that are referenced need not be to the left of the reference for numbers less than 10. See [Non-printing Characters, page B-3](#) for further details of the handling of digits following a backslash.

A back reference matches whatever actually matched the capturing subpattern in the current subject string, rather than anything matching the subpattern itself (see [Subpatterns as Subroutines, page B-21](#) for a way of doing that). So the pattern

```
(sens|respons)e and \1bility
```

matches "sense and sensibility" and "response and responsibility", but not "sense and responsibility". If careful matching is in force at the time of the back reference, the case of letters is relevant. For example,

```
((?i)rah)\s+1
```

matches "rah rah" and "RAH RAH", but not "RAH rah", even though the original capturing subpattern is matched caselessly.

Back references to named subpatterns use the Python syntax (`?P=name`). We could rewrite the above example as follows:

```
(?<p1>( ?i) rah) \s+ (?P=p1)
```

There may be more than one back reference to the same subpattern. If a subpattern has not actually been used in a particular match, any back references to it always fail. For example, the pattern

```
(a| (bc)) \2
```

always fails if it starts to match "a" rather than "bc". Because there may be many capturing parentheses in a pattern, all digits following the backslash are taken as part of a potential back reference number. If the pattern continues with a digit character, some delimiter must be used to terminate the back reference. If the `PCRE_EXTENDED` option is set, this can be whitespace. Otherwise an empty comment (see [Comments, page B-19](#)) can be used.

A back reference that occurs inside the parentheses to which it refers fails when the subpattern is first used, so, for example, `(a\1)` never matches. However, such references can be useful inside repeated subpatterns. For example, the pattern

```
(a|b\1)+
```

matches any number of "a"s and also "aba", "ababbaa" etc. At each iteration of the subpattern, the back reference matches the character string corresponding to the previous iteration. In order for this to work, the pattern must be such that the first iteration does not need to match the back reference. This can be done using alternation, as in the example above, or by a quantifier with a minimum of zero.

Assertions

An assertion is a test on the characters following or preceding the current matching point that does not actually consume any characters. The simple assertions coded as `\b`, `\B`, `\A`, `\G`, `\Z`, `\z`, `^` and `$` are described in [Simple Assertions, page B-6](#).

More complicated assertions are coded as subpatterns. There are two kinds: those that look ahead of the current position in the subject string, and those that look behind it. An assertion subpattern is matched in the normal way, except that it does not cause the current matching position to be changed.

Assertion subpatterns are not capturing subpatterns, and may not be repeated, because it makes no sense to assert the same thing several times. If any kind of assertion contains capturing subpatterns within it, these are counted for the purposes of numbering the capturing subpatterns in the whole pattern. However, substring capturing is carried out only for positive assertions, because it does not make sense for negative assertions.

Lookahead Assertions

Lookahead assertions start with `(?=` for positive assertions and `(?!` for negative assertions. For example,

```
\w+ ( ?= ; )
```

matches a word followed by a semicolon, but does not include the semicolon in the match, and

```
foo (?!bar)
```

matches any occurrence of "foo" that is not followed by "bar". Note that the apparently similar pattern

```
(?!foo)bar
```

does not find an occurrence of "bar" that is preceded by something other than "foo"; it finds any occurrence of "bar" whatsoever, because the assertion (?!foo) is always true when the next three characters are "bar". A lookbehind assertion is needed to achieve the other effect.

If you want to force a matching failure at some point in a pattern, the most convenient way to do it is with (?! because an empty string always matches, so an assertion that requires there not to be an empty string must always fail.

Lookbehind Assertions

Lookbehind assertions start with (?<= for positive assertions and (?<!= for negative assertions. For example,

```
(?<!=foo)bar
```

does find an occurrence of "bar" that is not preceded by "foo". The contents of a lookbehind assertion are restricted such that all the strings it matches must have a fixed length. However, if there are several alternatives, they do not all have to have the same fixed length. Thus

```
(?<=bullock|donkey)
```

is permitted, but

```
(?<!=dogs?|cats?)
```

causes an error at compile time. Branches that match different length strings are permitted only at the top level of a lookbehind assertion. This is an extension compared with Perl (at least for 5.8), which requires all branches to match the same length of string. An assertion such as

```
(?<=ab(c|de))
```

is not permitted, because its single top-level branch can match two different lengths, but it is acceptable if rewritten to use two top-level branches:

```
(?<=abc|abde)
```

The implementation of lookbehind assertions is, for each alternative, to temporarily move the current position back by the fixed width and then try to match. If there are insufficient characters before the current position, the match is deemed to fail.

PCRE does not allow the \C escape (which matches a single byte in UTF-8 mode) to appear in lookbehind assertions, because it makes it impossible to calculate the length of the lookbehind. The \X escape, which can match different numbers of bytes, is also not permitted.

Atomic groups can be used in conjunction with lookbehind assertions to specify efficient matching at the end of the subject string. Consider a simple pattern such as

```
abcd$
```

when applied to a long string that does not match. Because matching proceeds from left to right, PCRE will look for each "a" in the subject and then see if what follows matches the rest of the pattern. If the pattern is specified as

```
^.*abcd$
```

the initial .* matches the entire string at first, but when this fails (because there is no following "a"), it backtracks to match all but the last character, then all but the last two characters, and so on. Once again the search for "a" covers the entire string, from right to left, so we are no better off. However, if the pattern is written as

```
^(?>.*)(?<=abcd)
```

or, equivalently, using the possessive quantifier syntax,

```
^.*+(?<=abcd)
```

there can be no backtracking for the `.*` item; it can match only the entire string. The subsequent lookbehind assertion does a single test on the last four characters. If it fails, the match fails immediately. For long strings, this approach makes a significant difference to the processing time.

Using Multiple Assertions

Several assertions (of any sort) may occur in succession. For example,

```
(?<=\d{3})(?!999)foo
```

matches "foo" preceded by three digits that are not "999". Notice that each of the assertions is applied independently at the same point in the subject string. First there is a check that the previous three characters are all digits, and then there is a check that the same three characters are not "999". This pattern does not match "foo" preceded by six characters, the first of which are digits and the last three of which are not "999". For example, it doesn't match "123abcfoo". A pattern to do that is

```
(?<=\d{3}...)(?!999)foo
```

This time the first assertion looks at the preceding six characters, checking that the first three are digits, and then the second assertion checks that the preceding three characters are not "999".

Assertions can be nested in any combination. For example,

```
(?<=(?!foo)bar)baz
```

matches an occurrence of "baz" that is preceded by "bar" which in turn is not preceded by "foo", while

```
(?<=\d{3})(?!999)...foo
```

is another pattern that matches "foo" preceded by three digits and any three characters that are not "999".

Conditional Subpatterns

It is possible to cause the matching process to obey a subpattern conditionally or to choose between two alternative subpatterns, depending on the result of an assertion, or whether a previous capturing subpattern matched or not. The two possible forms of conditional subpattern are

```
(?(condition)yes-pattern)
(?(condition)yes-pattern|no-pattern)
```

If the condition is satisfied, the yes-pattern is used; otherwise the no-pattern (if present) is used. If there are more than two alternatives in the subpattern, a compile-time error occurs.

There are three kinds of condition. If the text between the parentheses consists of a sequence of digits, the condition is satisfied if the capturing subpattern of that number has previously matched. The number must be greater than zero. Consider the following pattern, which contains non-significant white space to make it more readable (assume the PCRE_EXTENDED option) and to divide it into three parts for ease of discussion:

```
( \ ( ) ?      [ ^ ( ) ] +      ( ? ( 1 ) \ ) )
```


The first part matches an optional opening parenthesis, and if that character is present, sets it as the first captured substring. The second part matches one or more characters that are not parentheses. The third part is a conditional subpattern that tests whether the first set of parentheses matched or not. If they did, that is, if subject started with an opening parenthesis, the condition is true, and so the yes-pattern is executed and a closing parenthesis is required. Otherwise, since no-pattern is not present, the subpattern matches nothing. In other words, this pattern matches a sequence of non-parentheses, optionally enclosed in parentheses.

If the condition is the string (R), it is satisfied if a recursive call to the pattern or subpattern has been made. At "top level", the condition is false. This is a PCRE extension. Recursive patterns are described in the next section.

If the condition is not a sequence of digits or (R), it must be an assertion. This may be a positive or negative lookahead or lookbehind assertion. Consider this pattern, again containing non-significant white space, and with the two alternatives on the second line:

```
(? (?!=[^a-z]*[a-z])
  \d{2}-[a-z]{3}-\d{2} | \d{2}-\d{2}-\d{2} )
```

The condition is a positive lookahead assertion that matches an optional sequence of non-letters followed by a letter. In other words, it tests for the presence of at least one letter in the subject. If a letter is found, the subject is matched against the first alternative; otherwise it is matched against the second. This pattern matches strings in one of the two forms dd-aaa-dd or dd-dd-dd, where aaa are letters and dd are digits.

Comments

The sequence `(?#` marks the start of a comment that continues up to the next closing parenthesis. Nested parentheses are not permitted. The characters that make up a comment play no part in the pattern matching at all.

If the `PCRE_EXTENDED` option is set, an unescaped `#` character outside a character class introduces a comment that continues up to the next newline character in the pattern.

Recursive Patterns

Consider the problem of matching a string in parentheses, allowing for unlimited nested parentheses. Without the use of recursion, the best that can be done is to use a pattern that matches up to some fixed depth of nesting. It is not possible to handle an arbitrary nesting depth. Perl provides a facility that allows regular expressions to recurse (amongst other things). It does this by interpolating Perl code in the expression at run time, and the code can refer to the expression itself. A Perl pattern to solve the parentheses problem can be created like this:

```
$re = qr{\( (? : (?>[^()]+) | (?p{$re}) )* \)}x;
```

The `(?p{...})` item interpolates Perl code at run time, and in this case refers recursively to the pattern in which it appears. Obviously, PCRE cannot support the interpolation of Perl code. Instead, it supports some special syntax for recursion of the entire pattern, and also for individual subpattern recursion.

The special item that consists of `(?` followed by a number greater than zero and a closing parenthesis is a recursive call of the subpattern of the given number, provided that it occurs inside that subpattern. (If not, it is a "subroutine" call, which is described in the next section.) The special item `(?R)` is a recursive call of the entire regular expression.

For example, this PCRE pattern solves the nested parentheses problem (assume the PCRE_EXTENDED option is set so that white space is ignored):

```
\( ( (?>[^\()]+) | (?R) )* \)
```

First it matches an opening parenthesis. Then it matches any number of substrings which can either be a sequence of non-parentheses, or a recursive match of the pattern itself (that is a correctly parenthesized substring). Finally there is a closing parenthesis.

If this were part of a larger pattern, you would not want to recurse the entire pattern, so instead you could use this:

```
( \ ( ( (?>[^\()]+) | (?1) )* \ ) )
```

We have put the pattern into parentheses, and caused the recursion to refer to them instead of the whole pattern. In a larger pattern, keeping track of parenthesis numbers can be tricky. It may be more convenient to use named parentheses instead. For this, PCRE uses (?P>name), which is an extension to the Python syntax that PCRE uses for named parentheses (Perl does not provide named parentheses). We could rewrite the above example as follows:

```
(?P<pn> \ ( ( (?>[^\()]+) | (?P>pn) )* \ ) )
```

This particular example pattern contains nested unlimited repeats, and so the use of atomic grouping for matching strings of non-parentheses is important when applying the pattern to strings that do not match. For example, when this pattern is applied to

```
(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa())
```

it yields "no match" quickly. However, if atomic grouping is not used, the match runs for a very long time indeed because there are so many different ways the + and * repeats can carve up the subject, and all have to be tested before failure can be reported.

At the end of a match, the values set for any capturing subpatterns are those from the outermost level of the recursion at which the subpattern value is set. If you want to obtain intermediate values, a callout function can be used (see [Subpatterns as Subroutines](#), page B-21 and the **pcrcallout** documentation). If the pattern above is matched against

```
(ab(cd)ef)
```

the value for the capturing parentheses is "ef", which is the last value taken on at the top level. If additional parentheses are added, giving

```
\( ( ( (?>[^\()]+) | (?R) )* ) ^
    ^
    ^
```

the string they capture is "ab(cd)ef", the contents of the top level parentheses. If there are more than 15 capturing parentheses in a pattern, PCRE has to obtain extra memory to store data during a recursion, which it does by using **pcrc_malloc**, freeing it via **pcrc_free** afterwards. If no memory can be obtained, the match fails with the PCRE_ERROR_NOMEMORY error.

Do not confuse the (?R) item with the condition (R), which tests for recursion. Consider this pattern, which matches text in angle brackets, allowing for arbitrary nesting. Only digits are allowed in nested brackets (that is, when recursing), whereas any characters are permitted at the outer level.

```
< (? : (? (R) \d++ | [^<>]*+) | (?R) ) * >
```

In this pattern, (?R) is the start of a conditional subpattern, with two different alternatives for the recursive and non-recursive cases. The (?R) item is the actual recursive call.

Subpatterns as Subroutines

If the syntax for a recursive subpattern reference (either by number or by name) is used outside the parentheses to which it refers, it operates like a subroutine in a programming language. An earlier example pointed out that the pattern

```
(sens|respons)e and \libility
```

matches "sense and sensibility" and "response and responsibility", but not "sense and responsibility". If instead the pattern

```
(sens|respons)e and (?1)ibility
```

is used, it does match "sense and responsibility" as well as the other two strings. Such references must, however, follow the subpattern to which they refer.

Callouts

Perl has a feature whereby using the sequence `(?{...})` causes arbitrary Perl code to be obeyed in the middle of matching a regular expression. This makes it possible, amongst other things, to extract different substrings that match the same pair of parentheses when there is a repetition.

PCRE provides a similar feature, but of course it cannot obey arbitrary Perl code. The feature is called "callout". The caller of PCRE provides an external function by putting its entry point in the global variable *pcre_callout*. By default, this variable contains NULL, which disables all calling out.

Within a regular expression, `(?C)` indicates the points at which the external function is to be called. If you want to identify different callout points, you can put a number less than 256 after the letter C. The default value is zero. For example, this pattern has two callout points:

```
(?C1)\dabc(?C2)def
```

If the `PCRE_AUTO_CALLOUT` flag is passed to **pcre_compile()**, callouts are automatically installed before each item in the pattern. They are all numbered 255.

During matching, when PCRE reaches a callout point (and *pcre_callout* is set), the external function is called. It is provided with the number of the callout, the position in the pattern, and, optionally, one item of data originally supplied by the caller of **pcre_exec()**. The callout function may cause matching to proceed, to backtrack, or to fail altogether. A complete description of the interface to the callout function is given in the *precallout* documentation.

Last updated: 09 September 2004 Copyright © 1997-2004 University of Cambridge.



APPENDIX C

DSF Event Type Group Reference

This chapter contains the following topics:

- [DSF Event Type Group Descriptions, page C-1](#)

DSF Event Type Group Descriptions

[Table C-1 on page C-1](#) lists the event type groups that can be used when defining an event type in a device support framework package.

Table C-1 **Event Type Group Description**

AppPolicyViolation/Misc	This group includes events triggered when miscellaneous applications drop a packet because of the application level policy violations.
AppPolicyViolation/Web	This group includes events triggered when a web server denies a packet because of web server policy violations.
AttacksProtected	This group includes events triggered when a intrusion protection device is statically configured to drop an attack.
AttacksProtected/Worm	This group includes events triggered when a worm attack was prevented.
ConfigError/CiscoCatOS	This group includes events that indicate a configuration error on a Cisco catalyst switch running Catalyst operating system. Configuration errors cause improper operation of the switch.
ConfigError/CiscoIOS	This group includes events that indicate a configuration error on a Cisco switch/router running IOS. Configuration errors cause improper operation of the switch.
ConfigError/CiscoPix	This group includes events that indicate a configuration error on a Cisco PIX firewall. Configuration errors cause improper operation of the firewall.
ConfigError/CiscoVPNConc	This group includes events that indicate a configuration error on a Cisco VPN Concentrator. Configuration errors cause improper operation of the switch.
ConfigError/CS-MARS	This group includes events that indicate a configuration error on CS-MARS preventing it from connecting to monitored devices. This can cause disruption in log collection from the device.
ConfigError/Host	This group includes events that indicate an configuration error on a host application.
ConfigError/NetScreenFirewall	This group includes events that indicate a configuration error on a Netscreen firewall running ScreenOS operating system. Configuration errors cause improper operation of the firewall.

Table C-1 Event Type Group Description (Continued)

ConfigError/Network	This group includes events that indicate a network configuration error preventing packets to reach the destination. This includes ICMP unreachable, ICMP time exceeded, duplicate addresses etc.
ContentPolicyViolation/All	This group includes all events related to violation of content policies.
ContentPolicyViolation/Email	This group includes events related to content policies violation in email.
ContentPolicyViolation/Web	This group includes events related to web content policy violation.
DoS/All	This group includes all events that indicate denial of service, including DoS to network, to network devices, to certain hosts, to various servers like mail servers and web servers, or distributed DoS activity.
DoS/DBServer	This group includes events that indicate attempts to crash or cause a denial of service on a database server.
DoS/Distributed	This group includes events that indicate distributed denial of service attacks e.g. from tools such as TFN, Trinoo, Mstream etc.
DoS/DNS	This group includes events that indicate attempts to crash or cause a denial of service on a DNS server.
DoS/FTPServer	This group includes events that indicate attempts to crash or cause a denial of service on an FTP server.
DoS/Host	This group includes events that indicate attempts to crash or cause a denial of service on a host.
DoS/MailServer	This group includes events that indicate attempts to crash or cause a denial of service on a mail server running SMTP, IMAP or POP.
DoS/MiscServer	This group includes events that indicate attempts to crash or cause a denial of service on a generic server.
DoS/ModbusServer	This group includes events that indicate attempts to crash or cause a denial of service on a MODBUS server. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
DoS/Network/ICMP	This group includes events that indicate a network level denial of service using the ICMP protocol.
DoS/Network/Misc	This group includes miscellaneous events that indicate a high network usage.
DoS/Network/TCP	This group includes events that indicate a network level denial of service using the TCP protocol.
DoS/Network/UDP	This group includes events that indicate a network level denial of service using the UDP protocol.
DoS/Network/WLAN	This group includes events that indicate wireless DoS attacks
DoS/NetworkDevice	This group includes events that indicate attempts to crash or cause a denial of service on network infrastructure devices such as routers, switches, AAA servers etc.
DoS/RPCService	This group includes events that indicate attempts to crash or cause a denial of service on a RPC service on a host.
DoS/SMBService	This group includes events that indicate attempts to crash or cause a denial of service on the SMB service on a host.
DoS/Sniffer	This group includes events that indicate attempts to crash or cause a denial of service on a network sniffer such as a network IDS.

Table C-1 *Event Type Group Description (Continued)*

DoS/TelnetServer	This group includes events that indicate attempts to crash or cause a denial of service on a Telnet server.
DoS/WebServer	This group includes events that indicate attempts to crash or cause a denial of service on a web server.
FirewallPolicyViolation/AAA	This group includes events triggered when a firewall denies a packet because of AAA policy violations and AAA access control list checks.
FirewallPolicyViolation/ACL	This group includes events triggered when a firewall denies a packet because of access control list checks.
FirewallPolicyViolation/All	This group includes all events triggered when a firewall denies a packet because of missing or incorrect NAT translations, various policy violations and access control list checks related to AAA, IPSec, SSL VPN, PPP and other protocol violations.
FirewallPolicyViolation/IPSec	This group includes events triggered when a firewall denies a packet because of IPSec policy violations and/or IPSec access control list checks.
FirewallPolicyViolation/Misc	This group includes events triggered when a firewall denies a packet because of various protocol policy violations.
FirewallPolicyViolation/NAT	This group includes events triggered when a firewall denies a packet because of missing or incorrect NAT translations.
FirewallPolicyViolation/PPP	This group includes events triggered when a firewall denies a packet because of PPP policy violations.
FirewallPolicyViolation/SSLVPN	This group includes events triggered when a firewall denies a packet because of SSL VPN policy violations and/or SSL VPN access control list checks.
Info/AllSession	This group includes events which indicate a IP session was established between two end points.
Info/CS-MARS-Upgrade-Available	This group includes all events related to MARS upgrade package or new image or new patch availability.
Info/DetailedTracking/Host	This group includes events that tracks operations in detail on a host.
Info/DTM	This group includes informational events from Cisco IOS Distributed Threat Mitigation.
Info/FailedAuth/AAA	This group includes all events that indicate failed authentication at the AAA servers. The events can include user credential errors or attacks, configuration, network and operational errors.
Info/HighUsage/CS-MARS	This group includes events that indicate high resource usage conditions (e.g. events or netflows dropped) on the CS-MARS device.
Info/HighUsage/Host	This group includes events that indicate high resource usage conditions (e.g. CPU, memory etc.) on a host.
Info/HighUsage/NetworkDevice	This group includes events that indicate high resource usage conditions (e.g. CPU, memory etc.) on a network device.
Info/LicenseNotification	This group includes license related notifications.
Info/Misc	This group includes generic informational events.
Info/Misc/AAA	This group includes generic informational events from AAA servers.
Info/Misc/AntiVirus	This group includes generic informational events on Anti-virus agent activity on desktops.
Info/Misc/AuthProxy	This group includes generic informational events on Authentication Proxy protocol on Cisco devices.

Table C-1 Event Type Group Description (Continued)

Info/Misc/CICS	This group includes generic informational events from Cisco Incident Control Servers.
Info/Misc/CiscoVPNConc	This group includes generic informational events from Cisco VPN Concentrators.
Info/Misc/ContentManagement	This group includes informational events related to content management devices.
Info/Misc/CS-MARS	This group includes informational events pertaining to the CS-MARS device, e.g. new SSL certificates or SSH fingerprints accepted etc.
Info/Misc/CS-MARS-DSF-Activity	This group includes events related to MARS Device Support Framework activity, such as export/import success/failure, and details of export/import activity.
Info/Misc/DB	This group includes generic informational events on database servers.
Info/Misc/DHCP	This group includes generic informational events from DHCP protocol.
Info/Misc/DMVPN	This group includes generic informational events regarding DMVPN.
Info/Misc/DNS	This group includes generic informational events on DNS servers.
Info/Misc/EAPoUDP	This group includes generic informational events on the EAPoUDP protocol which is used by Network Admission Control capable Cisco Network Access Devices to communicate with AAA servers.
Info/Misc/FDM	This group includes generic informational events regarding FWSM Device Manager.
Info/Misc/FTP	This group includes generic informational events on FTP protocol
Info/Misc/FW	This group includes generic informational events from firewalls.
Info/Misc/GTP	This group includes generic informational events from GTP protocol.
Info/Misc/H323	This group includes generic informational events from H323 protocol.
Info/Misc/Host	This group includes generic informational events on hosts.
Info/Misc/IDS	This group includes generic informational events from Network or Host IDS devices.
Info/Misc/IPS	This group includes generic informational events from IPS.
Info/Misc/IPSec	This group includes generic informational events from IPSec protocol.
Info/Misc/L2TP	This group includes generic informational events from L2TP protocol.
Info/Misc/LDAP	This group includes generic informational events from LDAP protocol.
Info/Misc/Login	This group includes generic informational events on services that provide login e.g. telnet, ssh, r-protocols.
Info/Misc/Mail	This group includes generic informational events on mail protocols SMTP, IMAP, POP.
Info/Misc/Modbus	This group includes generic informational events regarding Modbus, Scada, and DNP.
Info/Misc/NAC	This group includes generic informational events regarding Network Admission Control system.
Info/Misc/NetBios	This group includes generic informational events from NetBios protocol.
Info/Misc/NFS	This group includes generic informational events from NFS protocol.
Info/Misc/NNTP	This group includes generic informational events from NNTP protocol.
Info/Misc/PPP	This group includes generic informational events from PPP protocol.
Info/Misc/PPTP	This group includes generic informational events from PPTP protocol.
Info/Misc/Printer	This group includes generic informational events on lpr protocol.
Info/Misc/RDP	This group includes generic informational events from RDP protocol.
Info/Misc/Router	This group includes generic informational events from routers.

Table C-1 *Event Type Group Description (Continued)*

Info/Misc/Routing	This group includes generic informational events from routing protocols: OSPF, BGP, RIP, HSRP etc.
Info/Misc/RPC	This group includes generic informational events on RPC services.
Info/Misc/Scanner	This group includes generic informational events on Vulnerability scanners.
Info/Misc/SNMP	This group includes generic informational events on SNMP protocol.
Info/Misc/SOCKS	This group includes generic informational events from SOCKS proxy protocol.
Info/Misc/SSL	This group includes generic informational events from SSL protocol.
Info/Misc/SSLVPN	This group includes generic informational events from SSL VPN servers.
Info/Misc/Switch	This group includes generic informational events from switches.
Info/Misc/TFTP	This group includes generic informational events on TFTP protocol
Info/Misc/VoIP	This group includes generic informational events regarding Voice over IP.
Info/Misc/Web	This group includes generic informational events on HTTP protocol.
Info/Misc/WLAN	This group includes informational events pertaining to the WLAN
Info/Mitigation/CS-MARS	This group includes events indicating CS-MARS host mitigation successes and failures.
Info/Mitigation/WLAN	This group includes events indicating WLAN host and AP mitigation successes and failures.
Info/NewOutbreak/Download	This group includes informational events from Cisco Incident Control Servers indicating successful download of OPACL, OPSig, Damage Clean Engine, Damage Clean Template, or Spyware pattern from Active Update server. These are for prevention of newly occurred virus or worm outbreak.
Info/NewOutbreak/PreventionDeploy/Attempt	This group includes informational events from Cisco Incident Control Servers indicating starting of outbreak management task and preparation to deploy OPACL. These are for prevention of newly occurred virus or worm outbreak.
Info/NewOutbreak/PreventionDeploy/Match	This group includes events from Cisco Incident Control Server, Cisco IOS and IPS devices that indicate matches to dynamically deployed ACL and signatures for prevention of newly discovered virus or worm outbreaks.
Info/NewOutbreak/PreventionDeploy/Success	This group includes informational events from Cisco Incident Control Servers indicating successful deployments for prevention of newly occurred virus or worm outbreak.
Info/ObjectAccess/Host	This group includes events that indicate object (e.g. a file) access and operations on a host.
Info/PrivilegedUse/Host	This group includes privileged operations on a host.
Info/ResourceUtilization/CS-MARS	This group includes informational events pertaining to the CS-MARS device utilization, e.g. Database partition filling up, etc.
Info/ResourceUtilization/NAC	This group includes informational events pertaining to the NAC Appliance server resource utilization, e.g. CPU load on the Appliance, Memory used etc.
Info/SecPostureStatus/Healthy	This group includes events that indicate that the Security Posture status of a host, as reported by the Cisco Network Admission Control system, is healthy. These hosts are security policy compliant and hence the software on these hosts does not need to be upgraded.
Info/SecPostureStatus/Healthy/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicate that the Security Posture status of a host is healthy. These hosts are security policy compliant and hence the software on these hosts does not need to be upgraded.

Table C-1 Event Type Group Description (Continued)

Info/SecPostureStatus/NotHealthy	This group includes events that indicate that the Security Posture status of a host, as reported by the Cisco Network Admission Control system, is not healthy. These hosts are in either a CHECKUP, QUARANTINE, INFECTED or UNKNOWN state and the software on these hosts may need to be upgraded.
Info/SecPostureStatus/NotHealthy/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicate that the Security Posture status of a host is not healthy. These hosts are in either a CHECKUP, QUARANTINE, INFECTED or UNKNOWN state.
Info/SecPostureStatus/Transition	This group includes events that indicate an end host in a TRANSITION security posture state. This state implies that the host is not running a Cisco Trust Agent (CTA) software and consequently, needs to be audited and assigned a proper security posture token by the Audit Server.
Info/SecPostureStatus/Transition/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicates the Security Posture status of a host is in a TRANSITION state. This state implies that the host is not running a Cisco Trust Agent (CTA) software.
Info/SecPostureValidation/All	This group includes all the Cisco NAC based Security Posture validation events from network access devices and AAA server.
Info/SecPostureValidation/Failure	This group includes events that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host. Such failures are likely caused by configuration errors in posture validation rule.
Info/SecPostureValidation/Failure/NAD	This group includes events reported by network access devices such as switches, routers etc. that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host. Such failures are likely due to configuration errors in posture validation rule.
Info/SecPostureValidation/NoCredentials	This group includes events that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host since there is no Cisco Trust Agent running on that host.
Info/SecPostureValidation/StaticAuth	This group includes events that indicate that a network access device (NAD) permitted an end host by static configuration - the NAD did not validate the posture by communicating to a AAA server.
Info/SecPostureValidation/StatusQuery/Failed	This group indicates that the security posture status query from a network access device (NAD) to an end host failed. Status queries are done once the host security posture is validated and failed queries may indicate a security posture change in the end host.
Info/SecPostureValidation/Success	This group includes events that indicate that the Cisco Network Admission Control system successfully validated the security posture of a host.
Info/SuccessfulLogin/AAA	This group includes events which indicate that an user has successfully logged on using AAA credentials. The logon could be for either logging into a device or for network access via VPN e.g. IPSec, PPTP, L2TP, SSL VPN etc.
Info/SuccessfulLogin/CS-MARS/Non-root	This group includes events which indicate that an user has successfully logged into a CS-MARS system as a normal user either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/CS-MARS/Root	This group includes events which indicate that an user has successfully logged into a CS-MARS system as an admin user (or system user) either using local console or via protocols such as SSH or HTTPS.

Table C-1 Event Type Group Description (Continued)

Info/SuccessfulLogin/DB	This group includes events which indicate that an user has successfully logged into an database server.
Info/SuccessfulLogin/FTP	This group includes events which indicate that an user has successfully logged into an FTP server.
Info/SuccessfulLogin/IPSec	This group includes events which indicate that an user has successfully logged on via IPSec VPN.
Info/SuccessfulLogin/Mail	This group includes events which indicate that an user has successfully logged into a mail server.
Info/SuccessfulLogin/Misc	This group includes events which indicate that an user has successfully logged on to miscellaneous applications (other than SSH, Telnet, POP, IMAP, SMTP, FTP, database servers) using application specific credentials.
Info/SuccessfulLogin/NetBios	This group includes events which indicate that an user has successfully accessed a network share.
Info/SuccessfulLogin/PPP	This group includes events which indicate that an user has successfully logged onto the network for remote access via PPP based protocols such as L2TP, PPTP etc.
Info/SuccessfulLogin/SSLVPN	This group includes events which indicate that an user has successfully logged onto the network for remote access via SSL VPN.
Info/SuccessfulLogin/System/Non-root	This group includes events which indicate that an user has successfully logged into a system as a normal user either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/System/Root	This group includes events which indicate that an user has successfully logged into a system as root (or system user) either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/WindowsDomain	This group includes events which indicate that an user has successfully logged into an Windows domain.
Info/SuspiciousFileFound/Cleaned	This group includes events that indicate that an Anti-virus software running on a host has found a Suspicious file and then cleaned (i.e. deleted, repaired or quarantined) the file.
Info/SuspiciousFileFound/NotCleaned	This group includes events that indicate that an Anti-virus software running on a host has found a Suspicious file but could not clean (i.e. deleted, repaired or quarantined) the file.
Info/SystemEvent/Host	This group includes miscellaneous system events on a host.
Info/UncommonTraffic/Adult	This group includes events which indicate that an user is surfing adult pornographic sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Chat	This group includes events which indicate that an user is invoking chat protocols such AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC, Hotline etc. These events are typically reported by Network IDS.
Info/UncommonTraffic/Chat/FileTransfer	This group includes events which indicate that files are being transferred over chat protocols such as AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC. Such files often carry worms and viruses and may be inappropriate in corporate environments.
Info/UncommonTraffic/Chat/Proxy	This group includes events which indicate that chat protocols such AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC, Hotline etc. are being initiated via HTTP proxy methods. These events are typically reported by Network IDS.
Info/UncommonTraffic/Gambling	This group includes events which indicate that an user is gambling sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Games	This group includes events which indicate that an user is surfing gaming sites. These events are typically reported by Network IDS.

Table C-1 *Event Type Group Description (Continued)*

Info/UncommonTraffic/ICMP	This group includes events which indicate that uncommon ICMP traffic such as Source Quench, Timestamp request/response, Information Request/Response, Address mask Request/response etc.
Info/UncommonTraffic/JobSearch	This group includes events which indicate that an user is surfing job search sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Multimedia	This group includes events which indicate that an user is invoking media players to connect to media sites on the Internet. These events are typically reported by Network IDS.
Info/UncommonTraffic/Non-standardPort	This group includes events which indicate that standard protocols such as SSH, IRC, SMTP are being run on non-standard ports that do not comply with IETF RFC specifications.
Info/UncommonTraffic/P2PFileShare	This group includes events which indicate the use of person-to-person (P2P) file sharing protocols and applications such as KaZaa, Bearshare, Mutella, Limewire, Napster. Often inappropriate content are shared over these protocols and the files often carry worms and viruses.
Info/UncommonTraffic/P2PFileShare/FileTransfer	This group includes events which indicate the actual transfer of files via person-to-person (P2P) file sharing protocols and applications such as KaZaa, Bearshare, Mutella, Limewire, Napster. Often inappropriate content or files containing worms/viruses are shared over these protocols.
Info/UncommonTraffic/SocialNetworks	This group includes events which indicate that an user is surfing social network like http://myspace.com . These events are typically reported by Network IDS
Info/UncommonTraffic/StockTrading	This group includes events which indicate that an user is surfing stock trading sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Suspicious	This group includes events which indicate that legitimate but highly uncommon traffic, typically associated with experimental protocols.
Info/UncommonTraffic/TCPIPOptions	This group includes events which indicate the use of rarely used TCP/IP header option fields such as Record Route, Timestamp etc. These events are typically reported by Network IDS.
Info/VirusFound/Cleaned	This group includes events that indicate that an Anti-virus software running on a host has found a virus infected file and then cleaned (i.e. deleted, repaired or quarantined) the file.
Info/VirusFound/NotCleaned	This group includes events that indicate that an Anti-virus software running on a host has found a virus infected file but could not clean (i.e. deleted, repair or quarantine) the file. Such viruses must be immediately quarantined.
Info/VulnerableHostFound	This group includes events which indicate that a vulnerable host is found. The host could be running old and vulnerable protocols such as SSHv1 or could have some other vulnerabilities as detected by Network IDS or vulnerability scanners.
Info/WLAN/RogueFound	This group includes events which indicate that a Rogue AP or Adhoc has been detected.
OperationalError/AAAServer	This group includes events that indicate an operational error on an Access Control Server. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CICS	This group includes events that indicate an operational error on a Cisco ICS server. Operational error includes internal software errors such as change account/device and generating reports, errors in verifying device connection status, errors in downloading updates etc.

Table C-1 **Event Type Group Description (Continued)**

OperationalError/CICS/Deploy	This group includes events that indicate an operational error on a Cisco ICS server in deploying OPS components: OPACL, OPSig, DCE, DCT and Spyware pattern to devices such as routers, switches and IPS devices.
OperationalError/CiscoCatOS	This group includes events that indicate an operational error on a Cisco catalyst switch running Catalyst operating system. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoIOS	This group includes events that indicate an operational error on a Cisco router or switch running Cisco IOS. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoNIDS	This group includes events that indicate an operational error on a appliance or switch/router module runing Cisco Network IDS module. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoPix	This group includes events that indicate an operational error on a Cisco PIX firewall. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoVPNConc	This group includes events that indicate an operational error on a Cisco VPN Concentrator appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/ContentManagement	This group includes events that indicate erroneous situation in content management device(s).
OperationalError/CS-MARS	This group includes events that indicate an operational error on CS-MARS . Operational error includes internal software errors such as failure to accept SSH/SSL key/certificate, errors in verifying device connectivity or errors in discovering the device.
OperationalError/ExtremeSwitch	This group includes events that indicate an operational error on a switch running Extreme Extremeware Operating system. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/Host	This group includes events that indicate an operational error on host applications. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/ISSSensor	This group includes events that indicate an operational error on a host or appliance running ISS real Secure Network/Host Sensor software. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NAC	This group includes events that indicate an operational error on a NAC System. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc. NAC System includes NAC Appliance and NAC Framework components.
OperationalError/NetScreenFirewall	This group includes events that indicate an operational error on a Netscreen firewall appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NetScreenIDP	This group includes events that indicate an operational error on a Netscreen IDP appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NetworkDevice/Misc	This group includes events that indicate an interface on a network device such as a firewall, router switch etc reporting excessive packets transmission and reception errors.

Table C-1 Event Type Group Description (Continued)

OperationalError/SymantecManHuntNIDS	This group includes events that indicate an operational error on a Symantec Manhunt Network IDS host. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/WLAN	This group includes events that indicate an operational error on WLAN such as a WEP decrypt error and others.
OperationalStatusChange/AAA Server	This group includes events that indicate a significant change in the operational status of an Access Control Server - examples are RADIUS or TACACS+ services started or stopped
OperationalStatusChange/Appl	This group includes events that indicate a significant change in the operational status of an application - examples are application shutting down.
OperationalStatusChange/CICS	This group includes events that indicate a significant change in the operational status of a Cisco ICS server - examples are ICS service stopped.
OperationalStatusChange/Cisco IOS	This group includes events that indicate a significant change in the operational status of a switch or router running Cisco IOS - examples are interface down
OperationalStatusChange/Cisco Pix	This group includes events that indicate a significant change in the operational status of a Cisco PIX firewall - examples are failover not working, interface down, appliance reloading etc.
OperationalStatusChange/Cisco VPNConc	This group includes events that indicate a significant change in the operational status of a Cisco VPN concentrator - examples are interface down
OperationalStatusChange/ContentManagement	This group includes events which depicts change in operational status on content management device(s).
OperationalStatusChange/CS-MARS	This group includes events that indicate a significant change in the operational status of a Cisco CS-MARS - examples are LC-GC connectivity issues, etc.
OperationalStatusChange/Host	This group includes events that indicate a significant change in the operational status of a host - examples are host shutting down.
OperationalStatusChange/IDS	This group includes events that indicate a significant change in the operational status of an IDS sensor - examples are stopped receiving traffic etc.
OperationalStatusChange/Modbus	This group includes events that indicate a significant change in the operational status of a MODBUS server. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
OperationalStatusChange/NAC	This group includes events that indicate a significant change in the operational status of a NAC system - NAC System includes NAC appliance and NAC Framework components.
OperationalStatusChange/NetscreenFirewall	This group includes events that indicate a significant change in the operational status of a Netscreen firewall - examples are failover not working, interface down, appliance reloading etc.
OperationalStatusChange/WLAN	This group includes events that indicate a significant change in the operational status of a WLAN - examples are a particular radio network enabled or disabled
Penetrate/All	This group includes all events which indicate remote attempts to gain access to host or unauthorized information, or to attack a host, including buffer overflow, remote code execution, escalate to an unauthorized privilege, connect to backdoor, etc.
Penetrate/ArpPoisoning	This group includes events that indicate attempts to poison the ARP cache and divert traffic.
Penetrate/Backdoor/CommandShell	This group includes events that indicate an attempt to logon or remotely execute various commands to a command shell in the clear - this indicates that a backdoor may be running on the destination.

Table C-1 *Event Type Group Description (Continued)*

Penetrate/Backdoor/CovertChannel	This group includes events that indicate a covert channel; e.g. an HTTP tunnel to communicate non-HTTP protocols, an ICMP tunnel to communicate non ICMP protocols.
Penetrate/Backdoor/MiscApp	This group includes events that indicate backdoors found in various applications. Such backdoors enable unauthorized accesses to the creators of the applications.
Penetrate/Backdoor/RemoteControlApp/Connect	This group includes events that indicate a connection to a legitimate remote control program (e.g. VNC, pcAnywhere etc.) running on a host.
Penetrate/Backdoor/RemoteControlApp/Response	This group includes events that indicate a response from a legitimate remote control program (e.g. VNC, pcAnywhere etc.) running on a host.
Penetrate/Backdoor/Rootkit/Connect	This group includes events that indicate attempts to connect to a rootkit application on a host. A rootkit is a collection of trojaned OS utilities that can be left by an attacker on a successfully compromised host for future remote access.
Penetrate/Backdoor/Spyware/Request	This group includes events that indicate an adware/spyware application on a host connecting back to pre-specified servers. These applications track a user's personal information and web surfing habits and send them back to third parties, without the user's authorization.
Penetrate/Backdoor/Spyware/Response	This group includes events that indicate an response to a adware/spyware application on a host from pre-specified servers. These applications track a user's personal information and web surfing habits and send them back to third parties, without the user's authorization.
Penetrate/Backdoor/Trojan/Connect	This group includes events that indicate an established connection to a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/Response	This group includes events that indicate a connection response from a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/SYN	This group includes events that indicate TCP SYN connect attempts to a backdoor program on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/SYN-ACK	This group includes events that indicate TCP SYN-ACK response from a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/BufferOverflow/DB	This group includes events that indicate buffer overflow attempts on a database server.
Penetrate/BufferOverflow/DB/MSSQL	This group includes events that indicate buffer overflow attempts on the MS SQL database server.
Penetrate/BufferOverflow/DB/Oracle	This group includes events that indicate buffer overflow attempts on Oracle database server.
Penetrate/BufferOverflow/DNS	This group includes events that indicate buffer overflow attempts on a DNS server.
Penetrate/BufferOverflow/FTP	This group includes events that indicate buffer overflow attempts on an FTP server.
Penetrate/BufferOverflow/Login	This group includes events that indicate buffer overflow attempts on login service such as Telnet, SSH, r-protocols.

Table C-1 Event Type Group Description (Continued)

Penetrate/BufferOverflow/Mail	This group includes events that indicate buffer overflow attempts on a mail server running SMTP, POP, IMAP.
Penetrate/BufferOverflow/Misc	This group includes events that indicate buffer overflow attempts on miscellaneous protocols.
Penetrate/BufferOverflow/RPC	This group includes events that indicate buffer overflow attempts on an RPC service such as statd, cmsd, nfs, mountd, automountd, yppaswdd, rwalld etc.
Penetrate/BufferOverflow/SNMP	This group includes events that indicate buffer overflow attempts on SNMP service.
Penetrate/BufferOverflow/Web	This group includes events that indicate buffer overflow attempts on a web server.
Penetrate/BufferOverflow/Web/Apache	This group includes events that indicate buffer overflow attempts on an Apache web server.
Penetrate/BufferOverflow/Web/IIS	This group includes events that indicate buffer overflow attempts on a Microsoft IIS Web server.
Penetrate/BufferOverflow/Web/iPlanet	This group includes events that indicate buffer overflow attempts on an SunOne iPlanet web server.
Penetrate/ClientExploit/Mail	This group includes events that indicate attempts by an attacker masquerading as a mail server, to exploit various vulnerabilities of a mail client on a client workstation.
Penetrate/ClientExploit/Misc	This group includes events that indicate attempts by an attacker to exploit various vulnerabilities on a client workstation. The vulnerable protocols can be client versions of DHCP, various Instant Messengers, DNS, FTP, P2P protocols and Windows OS.
Penetrate/ClientExploit/Web	This group includes events that indicate attempts by an attacker masquerading as a web server, to exploit various vulnerabilities of a web browser on a client workstation.
Penetrate/Evasion/FTP	This group includes events that indicate maliciously constructed packets within an FTP session - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Generic	This group includes events that indicate maliciously constructed packets within a session for miscellaneous protocols such as SMB, SNMP, IDENT - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Login	This group includes events that indicate maliciously constructed packets within a login session involving telnet/ssh protocol - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Mail	This group includes events that indicate maliciously constructed SMTP packets - this might indicate attempts to bypass mail filtering software.
Penetrate/Evasion/RPC	This group includes events that indicate maliciously constructed packets within an RPC session - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/TCP/IP	This group includes events that indicate excessive or malicious packet fragmentation - this might indicate attempts to bypass IDS devices.
Penetrate/Evasion/Web	This group includes events that indicate maliciously encoded HTTP payloads - this might indicate attempts to bypass IDS devices.
Penetrate/GuessPassword/AAA	This group includes events that indicate AAA server authentication and authorization failures. AAA servers are often used to offload Authentication and Authorization functionalities from network devices.

Table C-1 **Event Type Group Description (Continued)**

Penetrate/GuessPassword/All	This group includes all authentication failure events which indicate unusual attempts to guess passwords of OS accounts, for accessing various services such as mail/FTP/database/web/VNC/CVS/windows domain/network share, for remote access such as PPP/P2TP/L2TP/IPSec/SSLVPN, etc.
Penetrate/GuessPassword/CS-MARS/Non-root	This group includes authentication failure events which indicate unusual attempts to guess user passwords on a CS-MARS device either using local console or via protocols such as SSH or HTTPS.
Penetrate/GuessPassword/CS-MARS/Root	This group includes authentication failure events which indicate unusual attempts to guess admin user or system passwords on a CS-MARS device either using local console or via protocols such as SSH or HTTPS.
Penetrate/GuessPassword/DB	This group includes authentication failure events which indicate unusual attempts to guess database server passwords.
Penetrate/GuessPassword/DB/System	This group includes authentication failure events for privileged users such as sa, dvo and Administrator, which indicate unusual attempts to guess database server passwords.
Penetrate/GuessPassword/FTP	This group includes authentication failure events which indicate unusual attempts to guess FTP server passwords.
Penetrate/GuessPassword/IPSec	This group includes authentication failure events which indicate unusual attempts to guess IPSec passwords. IPSec is a protocol for secure site-to-site or remote access.
Penetrate/GuessPassword/Mail	This group includes authentication failure events which indicate unusual attempts to guess mail server passwords.
Penetrate/GuessPassword/Misc	This group includes miscellaneous authentication failure events which indicate unusual attempts to access various services such as SOCKS, VNC, NNTP, pcAnywhere, CVS etc.
Penetrate/GuessPassword/NetworkShares	This group includes authentication failure events which indicate unusual attempts to guess passwords for accessing network shares. Worms propagate by copying malicious executables into network shares.
Penetrate/GuessPassword/RemoteAccess	This group includes authentication failure events which indicate unusual attempts to guess passwords for generic remote access protocols such as PPP, P2TP, L2TP etc.
Penetrate/GuessPassword/SNMP	This group includes authentication failure events which indicate unusual attempts to guess SNMP community strings.
Penetrate/GuessPassword/SSLVPN	This group includes authentication failure events which indicate unusual attempts to guess SSLVPN passwords. SSLVPN is a protocol for secure remote access.
Penetrate/GuessPassword/System/DisabledAcct	This group includes events that indicate failed logins to disabled, expired or locked accounts.
Penetrate/GuessPassword/System/Non-root	This group includes authentication failure events which indicate unusual attempts to guess user passwords (e.g. Telnet, SSH, R-protocol passwords) on a host.
Penetrate/GuessPassword/System/RestrictedTime	This group includes events that indicate failed logins during restricted times.
Penetrate/GuessPassword/System/Root	This group includes authentication failure events which indicate unusual attempts to guess root or system passwords (e.g. Telnet, SSH, R-protocol passwords) on a host.
Penetrate/GuessPassword/WebServer	This group includes authentication failure events which indicate unusual attempts to guess web server account passwords.
Penetrate/GuessPassword/WindowsDomain	This group includes authentication failure events which indicate unusual attempts to break into Windows Domain accounts.
Penetrate/HijackSession	This group includes events that indicate attempts to hijack a TCP session.

Table C-1 Event Type Group Description (Continued)

Penetrate/Nimdaworm	This group includes events that indicate a Nimda worm.
Penetrate/PrivilegeEscalation/ApplAdmin	This group includes events that indicate an attempt for a regular user to become a web application admin in a suspicious manner.
Penetrate/PrivilegeEscalation/Login	This group includes events that indicate an attempt for a regular user to gain system user (or root user) privileges via login protocols (e.g. SSH, telnet etc.)
Penetrate/PrivilegeEscalation/Mail	This group includes events that indicate an attempt for a regular user to gain elevated privileges offered by Mail services: SMTP, POP, IMAP.
Penetrate/PrivilegeEscalation/Misc	This group includes events that indicate an attempt for a regular user to gain elevated privileges by exploiting miscellaneous protocols.
Penetrate/PrivilegeEscalation/RPC	This group includes events that indicate an attempt for a regular user to gain elevated privileges offered by RPC services.
Penetrate/ProtocolAnomaly/DNS	This group includes events that indicate DNS IETF RFC specification violations.
Penetrate/ProtocolAnomaly/FTP	This group includes events that indicate FTP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Login	This group includes events that indicate telnet/SSH/r-protocol IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Mail	This group includes events that indicate SMTP/POP/IMAP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Misc	This group includes events that indicate violations of miscellaneous protocols such as IRC, SOCKS, LDAP etc.
Penetrate/ProtocolAnomaly/Modbus	This group includes events that indicate Modbus specification violations. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Penetrate/ProtocolAnomaly/Routing	This group includes events that indicate IETF RFC specification violations of routing protocols such as BGP, OSPF, RIP.
Penetrate/ProtocolAnomaly/RPC	This group includes events that indicate IETF RFC specification violations of RPC services such as rstatd, mound, nfs, rwalld, rusers etc.
Penetrate/ProtocolAnomaly/SNMP	This group includes events that indicate SNMP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/TCP/IP	This group includes events that indicate TCP, UDP, IP headers that do not conform to IETF RFC specifications.
Penetrate/ProtocolAnomaly/Web	This group includes events that indicate HTTP IETF RFC specification violations.
Penetrate/RemoteCmdExec/DB	This group includes events that indicate attempts to execute unauthorized commands on a database server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/FTP	This group includes events that indicate attempts to execute unauthorized commands within an FTP session by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Mail	This group includes events that indicate attempts to execute unauthorized commands within an SMTP/POP/IMAP session to a mail server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Misc	This group includes events that indicate attempts to execute unauthorized commands on a host running miscellaneous services by executing exploits other than buffer overflows.

Table C-1 *Event Type Group Description (Continued)*

Penetrate/RemoteCmdExec/RPC	This group includes events that indicate attempts to execute unauthorized commands on a host running RPC services by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/SNMP	This group includes events that indicate attempts to execute unauthorized commands on a host running SNMP server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web/ Apache	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session to a Apache Web server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web/ IIS	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session to a Microsoft IIS Web server by executing exploits other than buffer overflows.
Penetrate/ReplayAttack	This group includes events that indicate replay attacks.
Penetrate/RetrievePassword/All	This group includes events which indicate unusual attempts to remotely retrieve system password files, SNMP community strings, FTP passwords, or miscellaneous application (mostly administrative) passwords.
Penetrate/RetrievePassword/Apple	This group includes events which indicate unusual attempts to remotely retrieve miscellaneous application (mostly administrative) passwords.
Penetrate/RetrievePassword/FTP	This group includes events which indicate unusual attempts to remotely retrieve FTP passwords.
Penetrate/RetrievePassword/SNMP	This group includes events which indicate unusual attempts to remotely retrieve SNMP community strings.
Penetrate/RetrievePassword/System	This group includes events which indicate unusual attempts to remotely retrieve system password files or sensitive system files containing passwords.
Penetrate/Spam	This group includes events that indicate e-mail spoofing techniques to hide e-mail sender identity - this may indicate SPAM attempts.
Penetrate/SpoofIdentity/DNS	This group includes events that indicate spoofed DNS responses - this may cause traffic to be redirected to another address.
Penetrate/SpoofIdentity/DNS/Success	This group includes events that indicate successful spoofed DNS responses - this may cause traffic to be redirected to another address.
Penetrate/SpoofIdentity/FTP	This group includes events that indicate spoofed FTP commands in order to bypass stateful firewall restrictions.
Penetrate/SpoofIdentity/FTP/Success	This group includes events that indicate successful spoofed FTP commands in order to bypass stateful firewall restrictions.
Penetrate/SpoofIdentity/Mail	This group includes events that indicate e-mail spoofing techniques to hide e-mail sender identity - third party relaying, use of SMTP TURN command etc.
Penetrate/SpoofIdentity/Misc	This group includes events that indicate spoofing behavior in miscellaneous protocols such as Kerberos, SOCKS etc.
Penetrate/SpoofIdentity/RPC	This group includes events that indicate proxied (spoofed) RPC requests in order to bypass authentication.
Penetrate/SpoofIdentity/SNMP	This group includes events that indicate attempts to hide the identity of SNMP sender to bypass authentication.
Penetrate/SpoofIdentity/TCPIP	This group includes events that indicate spoofed network addresses.

Table C-1 Event Type Group Description (Continued)

Penetrate/SpoofIdentity/Web	This group includes events that indicate attempts to hide the identity of web pages - including cache poisoning, IDN URL spoofing, etc.
Penetrate/SQLInjection	This group includes events that indicate SQL Injection attempts on database servers. Inadequate processing of URL requests may allow users to execute unauthorized SQL commands by embedding them inside URLs. This can lead to modification of database tables.
Penetrate/ViewFiles/DB	This group includes events which indicate unusual attempts to view or determine the existence of files visible to a database service (such as MS SQL, Oracle, Sybase etc.) but not accessible to the typical user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/FTP	This group includes events which indicate FTP based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the FTP process but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/Misc	This group includes events which indicate miscellaneous protocol based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to those service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/NetBios	This group includes events which indicate NetBios based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files in a directory not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/NetMeeting	This group includes events which indicate Netmeeting based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the NetMeeting service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/RPC	This group includes events which indicate RPC based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the RPC service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversal/Web	This group includes events which indicate HTTP based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the web server but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/HTTPSource	This group includes events which indicate attempts to view the source code of scripts in web servers. Source code contain sensitive information such as passwords. This can lead to targetted attacks on the scripts or password based attacks.
Penetrate/ViewFiles/Sensitive	This group includes events which indicate unusual attempts to view sensitive system files on a web server via HTTP. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/WebOrderInfo	This group includes events which indicate unusual attempts to view customer sensitive files containing orders, credit card numbers in web servers. This can cause this sensitive information to be stolen and misused.
Persist/All	This group includes all events that indicate activity on a host with authenticated access.
Persist/CaptureSensitiveInfo	This group includes events that indicate an attempt to capture sensitive information from a host by installing special applications - examples are PWDUMP tool installation/activation, packet capturing tool activation etc. These typically require root access.
Persist/ExecCommand/DB/Privileged/Failure	This group includes events that indicate failed privileged or system level database command execution (e.g. audit, grant, revoke etc.). These are reported by the database server audit logs.

Table C-1 **Event Type Group Description (Continued)**

Persist/ExecCommand/DB/Privileged/Success	This group includes events that indicate successful privileged or system level database command execution (e.g. audit, grant, revoke etc.). These are reported by the database server audit logs.
Persist/ExecCommand/DB/Regular/Failure	This group includes events that indicate failed regular database command execution (e.g. select, insert, update, delete, PL/SQL execute, Associate statistics views etc.). These are reported by the database server audit logs.
Persist/ExecCommand/DB/Regular/Success	This group includes events that indicate successful regular database command execution (e.g. select, insert, update, delete, PL/SQL execute, Associate statistics views etc.). These are reported by the database server audit logs.
Persist/ExecuteFile	This group includes events that indicate attempts to execute a file on a host.
Persist/HostCompromised/DB	This group includes events that indicate a compromised database server.
Persist/HostCompromised/DNS	This group includes events that indicate a compromised DNS server.
Persist/HostCompromised/FTP	This group includes events that indicate a compromised FTP server.
Persist/HostCompromised/Mail	This group includes events that indicate a compromised Mail server.
Persist/HostCompromised/Misc	This group includes events that indicate a compromised server.
Persist/HostCompromised/RPC	This group includes events that indicate a compromised RPC service.
Persist/HostCompromised/Web	This group includes events that indicate a compromised web server.
Persist/HostCompromised/Web/Failed	This group includes events that indicate a compromised web server and failure.
Persist/InstallServices/All	This group includes events that indicate an attempt to install various kinds of services on a host, including malicious, remote access, suspicious, auto run service, etc. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/Autorun	This group includes events that indicate an attempt to install auto run services on a host. These services would be run automatically after next reboot. Worms typically install malicious auto run services on a compromised host.
Persist/InstallServices/Malicious	This group includes events that indicate an attempt to install malicious trojans (e.g. Asylum, NetBus etc.) on a host. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/RemoteAccess	This group includes events that indicate an attempt to install remote control applications on a host. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/Suspicious	This group includes events that indicate an attempt to install services on a host. These are generally suspicious and are reported by Host IDS. Worms typically install malicious services on a compromised host.
Persist/ModifyHost/All	This group includes all events that indicate attempts to modify configuration/files on a host, including using SNMP, modifying files, registry, user accounts, group accounts, security policy, service settings, logs, etc.
Persist/ModifyHost/CICS	This group includes events that indicate attempts to change configuration on Cisco ICS servers, such as addition/change/removal of accounts and devices.
Persist/ModifyHost/DB/DBObject/Failure	This group includes events that indicate failed database object (e.g. tables, views, indexes, clusters etc.) modification. These are reported by the database server audit logs.
Persist/ModifyHost/DB/DBObject/Success	This group includes events that indicate successful database object (tables, views, indexes, clusters etc.). These are reported by the database server audit logs.

Table C-1 Event Type Group Description (Continued)

Persist/ModifyHost/DB/UserGroup/Failure	This group includes events that indicate failed database server user group modification attempts. These are reported by the database server audit logs.
Persist/ModifyHost/DB/UserGroup/Success	This group includes events that indicate successful database server user group modification. These are reported by the database server audit logs.
Persist/ModifyHost/Files	This group includes events that indicate attempts to modify files on a host.
Persist/ModifyHost/Log	This group includes events that indicate attempts to modify logs on hosts. Attackers may attempt to destroy or modify logs in order to hide activity.
Persist/ModifyHost/Misc	This group includes events that indicate miscellaneous aspects of host modification.
Persist/ModifyHost/Modbus	This group includes events that indicate attempts to modify Modbus control servers. Modbus protocol has become a defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Persist/ModifyHost/Registry	This group includes events that indicate attempts to modify registry entries on a windows host.
Persist/ModifyHost/SecurityPolicy	This group includes events that indicate attempts to modify security policies (e.g. user rights, audit policies etc.) on workstations and servers.
Persist/ModifyHost/SecurityPolicy/Weaken	This group includes events that indicate attempts to weaken security policies on workstations and servers. Such examples include disabling strong password enforcement, enabling IE ActiveX scripting etc.
Persist/ModifyHost/ServiceSettings	This group includes events that indicate attempts to modify the service settings on workstations and servers.
Persist/ModifyHost/SNMP	This group includes events that indicate attempts to modify configuration via SNMP SET commands.
Persist/ModifyHost/UserGroup	This group includes events that indicate attempts to modify user group settings on workstations and servers.
Persist/ModifyNetworkConfig	This group includes events that indicate attempts to modify configuration of network devices such as firewalls, routers, switches etc.
Persist/PrivilegeEscalation/LocalBufferOverflow	This group includes events that indicate an attempt to cause a local buffer overflow on a host - this events require access to the host and can provide root access.
Persist/PrivilegeEscalation/Misc	This group includes events that indicate an attempt to escalate privileges after having regular access. The mechanisms would include exploiting vulnerabilities of known applications that run with system privileges.
Persist/PrivilegeEscalation/SymbolicLink	This group includes events that indicate an attempt to gain system privileges by symbolically linking to special files - this events require access to the host.
Persist/SuspiciousActivity	This group includes events that indicate suspicious activity on a host.
Probe/ClientInfo/Login	This group includes events which indicate attempts to gather information (e.g. version, setup etc.) about clients to the login services (e.g. Telnet, SSH etc.) on a host. This can lead to targetted attacks on those protocols or password guessing attacks.
Probe/Firewall	This group includes events which indicate an attempt to discover firewall rules. The knowledge of firewall rules may enable an attacker to discover exposed servers and services and launch targeted attacks.
Probe/FromScanner	This group includes events which detect that a scanner application (e.g. Nessus, E-eye Retina, ISS Scanner etc.) is being used to map hosts in a network and discover vulnerabilities.

Table C-1 Event Type Group Description (Continued)

Probe/Host/Config	This group includes events which indicate attempts to gather information about the generic configuration of a host: its operating system, environment variables, hardware set up etc. This could lead to targetted attacks.
Probe/Host/NetworkShare	This group includes events which indicate attempts to gather information about remotely accessible shares. Worms propagate by first connecting to and then dumping malicious files on remotely accesible shares.
Probe/Host/Stealth	This group includes events which indicate stealthy attempts to determine the presence of a host. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/Host/UserName	This group includes events which indicate attempts to gather information about user accounts on a host. This can lead to password guessing attacks on that host.
Probe/Host/WinRegistry	This group includes events which indicate attempts to gather information about the host and various applications running on a windows host by reading the windows registry on the host. This could lead to targetted attacks.
Probe/HostInfo/All	This group includes all events which detect that an attacker is probing information regarding hosts, including using sweep to find live hosts, scanning specifie ports, scanning hosts in promiscuous state, probing firewall rules to find exposed hosts, etc.
Probe/HostSweep/Non-stealth	This group includes events which detect that an attacker is scanning the hosts in a network in a non-stealth mode looking for live hosts. Non-Stealth operation includes simple ICMP based ping packets.
Probe/HostSweep/Stealth	This group includes events which detect that an attacker is scanning the hosts in a network in a stealth mode looking for live hosts. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/NetworkInfo	This group includes events which indicate an attempt to discover network devices, network device configurations, DNS zone transfers etc.
Probe/PortSweep/Non-stealth	This group includes events which detect that an attacker is scanning the ports of a particular host in a non-stealth mode looking for open services. Non-Stealth operation includes simple ICMP based ping packets.
Probe/PortSweep/Stealth	This group includes events which detect that an attacker is scanning the ports of a particular host in a stealth mode looking for open services. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/PromiscuousHost	This group includes events which indicate an attempt to locate hosts running in promiscuous mode. Hosts running in promiscuous mode are either IDS systems or have access to privilege information and hence are prime targets for attackers.
Probe/ServerInfo/DB	This group includes events which indicate attempts to gather information (e.g. version, setup, users) about the database services e.g. MS SQL, Otacle, Sybase, MySQL running on a host. This can lead to targetted database specific attacks or password attacks for database access.
Probe/ServerInfo/DB/Response	This group includes events which indicate responses to attempts to gather information (e.g. version, setup, users) about the database services e.g. MS SQL, Otacle, Sybase, MySQL running on a host. This can lead to targetted database specific attacks or password attacks for database access.

Table C-1 Event Type Group Description (Continued)

Probe/ServerInfo/DNS	This group includes events which indicate attempts to gather information (e.g. the version, author, setup etc.) about the DNS service on a host. This can lead to targetted DNS based attacks on that host.
Probe/ServerInfo/FTP	This group includes events which indicate attempts to gather information (e.g. version, setup, commands exposed) about the FTP service running on a host. This can lead to targetted attacks on the FTP protocol or password attacks for FTP access.
Probe/ServerInfo/Login	This group includes events which indicate attempts to gather information (e.g. version, setup etc.) about the login services (e.g. Telnet, SSH etc.) on a host. This can lead to targetted attacks on those protocols or password guessing attacks.
Probe/ServerInfo/Mail	This group includes events which indicate attempts to gather information (e.g. version, setup, commands supported etc.) about the mail services: SMTP, POP, IMAP. This can lead to targetted attacks on those protocols.
Probe/ServerInfo/Misc	This group includes events which indicate attempts to gather information about miscellaneous services (e.g. finger, Bugzilla, XDMCP etc.) on a host.
Probe/ServerInfo/Modbus	This group includes events which indicate attempts to gather information about ModBus service on a host. This can lead to targetted Modbus specific attacks. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Probe/ServerInfo/RPC	This group includes events which indicate attempts to gather information (e.g. version, setup, dynamic ports for specific services) about the RPC service running on a host. This can lead to targetted attacks on RPC based services such as RSTATD, MOUNTD etc.
Probe/ServerInfo/Web	This group includes events which indicate attempts to gather information (e.g. version, setup, users, existence of specific scripts) about the web server running on a host. This can lead to targetted web server specific attacks.
Probe/SpecificPorts	This group includes events which detect that an attacker is looking for all hosts that are running a particular service, e.g. TCP port 445. This may be a precursor to exploiting a very specific vulnerability.
Probe/WLAN	This group includes events which indicate attempts to gather information about WLAN. Examples are various wireless scanners such as NetStumbler 3.2.0
Propagate/CopyFiles	This group includes events that indicate an attempt to copy files over the network. While this is a typical property of worms, the files as captured by these events are not necessarily malicious.
Propagate/Worm	This group includes events that indicate a worm propagation via various protocols such as e-mail, NetBios shares, P2P, FTP, TFTP. The source in these events is likely infected.
SANSTop20	This group includes the Top 20 Internet Security vulnerabilities as of version 5.0 October 2004 compiled by the SANS Institute. These can be found in http://www.sans.org/top20/
SwitchPolicyViolation/PortSecurity	This group includes events that indicate switch port policy violations on a network switch. Switch port policies include acceptable per port MAC, IP etc.
SystemCompliance	This group includes events which indicate that the system is not up-to-date with desired security patches.



APPENDIX **D**

Cisco Security MARS XML API Reference

This appendix provides resources for creating XML applications that integrate Cisco Security MARS XML data into third-party applications.

XML Schema Overview

The XML schema are written in conformance with the standard World Wide Web Consortium (W3C) XML schema language. A schema by definition, describes all data and data structures required to create your application. Many XML development environments provide enough capability to view the schema in a way that you can identify all components, their relationships, constraints, attributes, annotations, and usage guidelines at a glance. Some applications generate hyperlinked reference documentation. By providing sufficient documentation and annotation tags within the schemas, Cisco supports such documentation generating applications.

Table D-1 lists resources for XML development.

Table D-1 XML Resources

Resource Description	URL
W3C XML Schema standards forum with resource links	http://www.w3.org/XML/Schema
General XML description with resource links	http://en.wikipedia.org/wiki/Xml
Online XML Tutorials	http://www.w3schools.com/xml/default.asp

XML Incident Notification Data File and Schema

XML incident notification sends an email notification of an incident with an attached XML data file. The XML data file contains all incident details that can be viewed on the GUI except for Path/Mitigation data. The XML data file can be sent as a plain-text file or as a compressed gzip file. The filename is constructed with the incident ID number, for example CS-MARS-Incident-13725095.xml. The compressed version of the same data file would be CS-MARS-Incident-13725095.xml.gz.

An XML application can be written to parse and extract data from the XML incident notification data file for integration into third-party software, such as a trouble ticketing system, or helpdesk software.

Table D-2 lists the documentation for the Cisco Security MARS XML incident notification feature.

Table D-2 Related XML Incident Notification Documents

Resource Description	Resource Location
Configuring XML incident notification on MARS	Chapter 5, “Alerts and Incident Notifications”
A ZIP file containing the XML incident notification schema	http://www.cisco.com/en/US/products/ps6241/prod_technical_reference_list.html
A hyperlinked component reference, generated from the XML incident notification schema	http://www.cisco.com/en/US/products/ps6241/prod_technical_reference_list.html
Sample XML incident notification data generated by MARS	Example D-1

XML Incident Notification Data File Sample Output

[Example D-1](#) is XML incident notification data generated by the events that trigger the rule “CS-MARS Database Partition Usage.”

Example D-1 XML Incident Notification Data File Contents

```
<?xml version="1.0" encoding="UTF-8"?>
<CSMARS-NOTIFICATION>
  <Header>
    <Version>1.0</Version>
    <GenTimeStamp>May 23, 2007 8:13:19 AM PDT</GenTimeStamp>
    <CSMARSHostIpAddr_eth0>10.2.3.48</CSMARSHostIpAddr_eth0>
    <CSMARSHostIpAddr_eth1>192.168.1.110</CSMARSHostIpAddr_eth1>
    <CSMARSHostName>pnmars</CSMARSHostName>
    <CSMARSZoneName />
    <CSMARSVersion>4.2.2</CSMARSVersion>
  </Header>
  <Data>
    <Incident id="287001899">
      <StartTime>May 23, 2007 8:13:09 AM PDT</StartTime>
      <EndTime>May 23, 2007 8:13:10 AM PDT</EndTime>
      <Severity>HIGH</Severity>
      <Session id="286913412">
        <Instance>0</Instance>
        <SessionEndPoints>
          <Source ipaddress="10.3.50.200" />
          <Destination ipaddress="248.64.35.88" />
          <SourcePort>15330</SourcePort>
          <DestinationPort>3890</DestinationPort>
          <Protocol>6</Protocol>
        </SessionEndPoints>
      <Event id="286914062">
        <EventType id="1135" />
        <TimeStamp>May 23, 2007 8:13:09 AM PDT</TimeStamp>
        <ReportingDevice id="128783" />
        <RawMessage>Wed May 23 08:13:09 2007 &lt;134&gt;%PIX-2-106001: Inbound TCP
connection denied from 10.3.50.200/15330 to 248.64.35.88/3890 flags FIN on interface
inside</RawMessage>
        <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
        <EventEndPoints>
          <Source ipaddress="10.3.50.200" />
          <Destination ipaddress="248.64.35.88" />
          <SourcePort>15330</SourcePort>
          <DestinationPort>3890</DestinationPort>
        </EventEndPoints>
      </Event>
    </Incident>
  </Data>
</CSMARS-NOTIFICATION>
```

```

        <Protocol>6</Protocol>
    </EventEndPoints>
    <NATtedEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>true</FiringEventFlag>
    <RuleMatchOffset>1</RuleMatchOffset>
</Event>
<Event id="286913412">
    <EventType id="1135" />
    <TimeStamp>May 23, 2007 8:11:53 AM PDT</TimeStamp>
    <ReportingDevice id="128783" />
    <RawMessage>Wed May 23 08:11:53 2007 &lt;134&gt;%PIX-2-106001: Inbound TCP
connection denied from 10.3.50.200/15330 to 248.64.35.88/3890 flags FIN on interface
inside</RawMessage>
    <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
    <EventEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </EventEndPoints>
    <NATtedEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>false</FiringEventFlag>
</Event>
</Session>
<Session id="286914063">
    <Instance>0</Instance>
    <SessionEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="105.74.127.53" />
        <SourcePort>0</SourcePort>
        <DestinationPort>0</DestinationPort>
        <Protocol>0</Protocol>
    </SessionEndPoints>
    <Event id="286914063">
        <EventType id="1137" />
        <TimeStamp>May 23, 2007 8:13:10 AM PDT</TimeStamp>
        <ReportingDevice id="128783" />
        <RawMessage>Wed May 23 08:13:10 2007 &lt;134&gt;%PIX-2-106016: Deny IP spoof
from (10.3.50.200) to 105.74.127.53 on interface inside</RawMessage>
        <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
        <EventEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="105.74.127.53" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>0</Protocol>
        </EventEndPoints>
        <NATtedEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="105.74.127.53" />
            <SourcePort>0</SourcePort>

```

```

        <DestinationPort>0</DestinationPort>
        <Protocol>0</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>true</FiringEventFlag>
    <RuleMatchOffset>1</RuleMatchOffset>
</Event>
</Session>
<Session id="286914072">
    <Instance>0</Instance>
    <SessionEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="133.67.205.96" />
        <SourcePort>0</SourcePort>
        <DestinationPort>0</DestinationPort>
        <Protocol>6</Protocol>
    </SessionEndPoints>
    <Event id="286914072">
        <EventType id="1139" />
        <TimeStamp>May 23, 2007 8:13:10 AM PDT</TimeStamp>
        <ReportingDevice id="128783" />
        <RawMessage>Wed May 23 08:13:10 2007 &lt;134&gt;%PIX-1-106022: Deny tcp
connection spoof from 10.3.50.200 to 133.67.205.96 on interface inside</RawMessage>
        <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
        <EventEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="133.67.205.96" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>6</Protocol>
        </EventEndPoints>
        <NATtedEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="133.67.205.96" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>6</Protocol>
        </NATtedEndPoints>
        <FiringEventFlag>true</FiringEventFlag>
        <RuleMatchOffset>1</RuleMatchOffset>
    </Event>
</Session>
<Rule id="128791">
    <Name>bd</Name>
    <Description>stack and decker</Description>
</Rule>
<NetworkAddressObj id="4164952920">
    <IPAddress>248.64.35.88</IPAddress>
    <MAC />
    <DNSName />
    <DynamicInfo>
        <HostName />
        <MACAddress />
        <AAAUser />
        <EnforcementDeviceAndPort />
        <ReportingDevice />
        <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
        <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
        <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
    </DynamicInfo>
</NetworkAddressObj>
<NetworkAddressObj id="2235813216">
    <IPAddress>133.67.205.96</IPAddress>
    <MAC />
    <DNSName />

```

```

    <DynamicInfo>
      <HostName />
      <MACAddress />
      <AAAUser />
      <EnforcementDeviceAndPort />
      <ReportingDevice />
      <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
      <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
      <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
    </DynamicInfo>
  </NetworkAddressObj>
  <NetworkAddressObj id="167981768">
    <IPAddress>10.3.50.200</IPAddress>
    <MAC />
    <DNSName />
    <DynamicInfo>
      <HostName />
      <MACAddress />
      <AAAUser />
      <EnforcementDeviceAndPort />
      <ReportingDevice />
      <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
      <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
      <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
    </DynamicInfo>
  </NetworkAddressObj>
  <NetworkAddressObj id="1766489909">
    <IPAddress>105.74.127.53</IPAddress>
    <MAC />
    <DNSName />
    <DynamicInfo>
      <HostName />
      <MACAddress />
      <AAAUser />
      <EnforcementDeviceAndPort />
      <ReportingDevice />
      <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
      <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
      <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
    </DynamicInfo>
  </NetworkAddressObj>
  <EventTypeObj id="1139">
    <Name>1106022</Name>
    <Description>Denied spoofed packet - different ingress interface</Description>
    <Severity>HIGH</Severity>
    <CVE />
  </EventTypeObj>
  <EventTypeObj id="1135">
    <Name>1106001</Name>
    <Description>Deny packet due to security policy</Description>
    <Severity>LOW</Severity>
    <CVE />
  </EventTypeObj>
  <EventTypeObj id="1137">
    <Name>1106016</Name>
    <Description>Denied IP spoof</Description>
    <Severity>MEDIUM</Severity>
    <CVE />
  </EventTypeObj>
  <DeviceObj id="128783">
    <Name>pixie</Name>
    <NetBiosName />
    <DefaultGateway>0.0.0.0</DefaultGateway>
    <OperatingSystem id="0" />

```

```

    </DeviceObj>
  </Incident>
</Data>
</CSMARS-NOTIFICATION>

```

XML Incident Notification Schema

The XML incident notification schema document (csmars-incident-notification-v1_0.xsd) can be downloaded from the following URL:

http://www.cisco.com/en/US/products/ps6241/prod_technical_reference_list.html

Usage Guidelines and Conventions for XML Incident Notification

All XML incident notification elements are defined in the XML incident notification schema. A WinZip archive containing a component reference document generated from the schema is available for your convenience at the following URL:

http://www.cisco.com/en/US/products/ps6241/prod_technical_reference_list.html

You can generate a similar document with the application of your choice, or view components, their relationships, constraints, attributes, annotations, and usage guidelines within your XML development environment.

MARS uses a best effort approach to create XML incident notification data. If an error occurs during data compilation, MARS does not stop the process, but sends the data, even if it is partial. Validating the data file against the schema would result in errors for these cases.

The following conventions are observed for XML incident notification data:

- Character encoding is Unicode Transformation Format 8 (UTF-8).
- The reported time zone would be the time zone of the local controller reporting the incident.
- Raw messages from reporting devices are XML-escaped in the data file. Your XML parser should be able to unescape XML data.
- If there is no value for an element available from MARS, the element is included in the data file as an empty node. For instance, a DNS name may not be available for a device.
- All date formats are **Mmm dd, yyyy hh:mm:ss AM TZD**.
 - **Mmm** is the month (Jan, Feb, Mar. . . Dec)
 - **dd** is the day (1-9, 10-31)
 - **yyyy** is the year (0000-9999)
 - **hh :mm :ss** is hours, minutes, seconds
 - hh** are 1-9, 10-12
 - mm** are 00-60
 - ss** are 00-60
 - **AM** or **PM**
 - **TZD** is time zone designator (PDT, PST, MDT, MST, etc.)



APPENDIX **E**

System Rules and Reports

This appendix presents the list of system rules and reports and provides a brief description of their intended use.

This chapter contains the following topics:

- [System Rules by Category, page E-1](#)
- [System Reports by Category, page E-28](#)

System Rules by Category

This topic identifies the categories in which the system rules issued with this release are organized.

This section contains the following topics:

- [System: ASA Botnet Traffic Filter, page E-2](#)
- [System: Access, page E-2](#)
- [System: CS-MARS Distributed Threat Mitigation \(Cisco DTM\), page E-5](#)
- [System: CS-MARS Incident Response, page E-6](#)
- [System: CS-MARS Issue, page E-6](#)
- [System: Client Exploits, Virus, Worm and Malware, page E-8](#)
- [System: Configuration Issue, page E-12](#)
- [System: Database Server Activity, page E-12](#)
- [System: Host Activity, page E-13](#)
- [System: Network Attacks and DoS, page E-14](#)
- [System: New Malware Outbreak \(Cisco ICS\), page E-15](#)
- [System: Operational Issue, page E-16](#)
- [System: Reconnaissance, page E-19](#)
- [System: Resource Issue, page E-19](#)
- [System: Restricted Network Traffic, page E-20](#)
- [System: Security Posture Compliance \(Cisco NAC\), page E-21](#)
- [System: Server Exploits, page E-23](#)

System: ASA Botnet Traffic Filter

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter, page E-11](#)
- [System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter, page E-19](#)

System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter

This rule detects phone home activity to black/grey listed sites/IPs, as reported by ASA Botnet Traffic Filter.

System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter

This rule detects traffic activity originating from black/grey listed sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Access

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Password Attack: Remote VPN Access - Success Likely, page E-3](#)
- [System Rule: Password Attack: System - Success Likely, page E-3](#)
- [System Rule: Password Attack: Database - Attempt, page E-3](#)
- [System Rule: Password Attack: Database - Success Likely, page E-3](#)
- [System Rule: Password Attack: FTP Server - Attempt, page E-3](#)
- [System Rule: Password Attack: Mail Server - Attempt, page E-3](#)
- [System Rule: Password Attack: Remote VPN Access - Attempt, page E-3](#)
- [System Rule: Password Attack: Network Share - Attempt, page E-4](#)
- [System Rule: Password Attack: SNMP - Attempt, page E-4](#)
- [System Rule: Password Attack: System - Attempt, page E-4](#)
- [System Rule: Password Attack: Misc. Application - Attempt, page E-4](#)
- [System Rule: Password Attack: Web Server - Attempt, page E-4](#)
- [System Rule: Password Attack: FTP Server - Success Likely, page E-4](#)
- [System Rule: Password Attack: Mail Server - Success Likely, page E-4](#)
- [System Rule: Password Attack: Network Share - Success Likely, page E-5](#)
- [System Rule: Password Attack: SNMP - Success Likely, page E-5](#)
- [System Rule: Password Attack: Disabled Accounts, page E-5](#)
- [System Rule: Password Scan: Disabled Accounts: Distinct Hosts, page E-5](#)
- [System Rule: Password Scan: Disabled Accounts: Same Host, page E-5](#)

- [System Rule: Password Scan: Distinct Hosts, page E-5](#)
- [System Rule: Password Scan: Same Host, page E-5](#)

System Rule: Password Attack: Remote VPN Access - Success Likely

This correlation rule detects a password guessing attack while authenticating to a remote access service (e.g. Windows L2TP, PPTP based RAS, IPSec etc.), followed by a successful logon. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: System - Success Likely

This correlation rule detects a successful password attack to gain system level access to a host or to a windows domain- such an attack consists of a successful login occurring after attempts to retrieve passwords or guess passwords while authenticating to that host. The password attack may be preceded by reconnaissance attacks to the host. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Database - Attempt

This correlation rule detects a password guessing attack to a database server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Database - Success Likely

This correlation rule detects a password guessing attack on a database server followed by a successful logon. The attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: FTP Server - Attempt

This correlation rule detects a password guessing attack to an FTP server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Mail Server - Attempt

This correlation rule detects a password guessing attack on a mail server (SMTP, POP, IMAP), preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Remote VPN Access - Attempt

This correlation rule detects a password guessing attack while authenticating to a remote access service (e.g. Windows L2TP, PPTP based RAS, IPSec etc.), preceded by reconnaissance attacks, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Network Share - Attempt

This correlation rule detects a password guessing attack on a network share, preceded by reconnaissance attacks, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: SNMP - Attempt

This correlation rule detects attempts to retrieve SNMP community strings or access SNMP information by guessing SNMP community strings. Many SNMP installations have easily guessable passwords by default. The password attack may be preceded by reconnaissance attacks to the host.

System Rule: Password Attack: System - Attempt

This correlation rule detects attempts to retrieve system passwords or multiple login failures while authenticating to a particular system/domain via telnet, SSH or local console/terminal logon. These attempts can be optionally preceded by reconnaissance attempts. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Misc. Application - Attempt

This correlation rule detects attempts to retrieve application passwords or multiple login failures while authenticating to a particular application. These attempts can be optionally preceded by reconnaissance attempts. Authentication failures may sometimes be caused by a user forgetting the password. The applications covered by this rule exclude common ones such as Mail, FTP, SSH, Telnet, SNMP, Network/File/Print share, for which there are special rules.

System Rule: Password Attack: Web Server - Attempt

This correlation rule detects a password guessing attack to a Web server, preceded by reconnaissance attacks to the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: FTP Server - Success Likely

This correlation rule detects a password guessing attack on a FTP server followed by a successful logon. The attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Mail Server - Success Likely

This correlation rule detects a password guessing attack on a mail server (SMTP, POP, IMAP) followed by a successful logon. The password attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: Network Share - Success Likely

This correlation rule detects a password guessing attack on a network share, followed by a successful logon. The password attack may be preceded by reconnaissance attacks to the host. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgetting the password.

System Rule: Password Attack: SNMP - Success Likely

This correlation rule detects a likely successful SNMP community string guessing attack - such an attack consists of a community string guessing attempt followed by a SNMP modification at the target host. The attack may be preceded by reconnaissance attacks to the host.

System Rule: Password Attack: Disabled Accounts

This rule detects repeated failed password attempts on locked, expired or disabled accounts on a host

System Rule: Password Scan: Disabled Accounts: Distinct Hosts

This rule detects repeated failed password attempts on locked, expired or disabled accounts on distinct hosts.

System Rule: Password Scan: Disabled Accounts: Same Host

This rule detects repeated failed password attempts on distinct locked, expired or disabled accounts on a host.

System Rule: Password Scan: Distinct Hosts

This rule detects repeated failed password attempts on distinct hosts.

System Rule: Password Scan: Same Host

This rule detects repeated failed password attempts on multiple distinct accounts on the same host.

System: CS-MARS Distributed Threat Mitigation (Cisco DTM)

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Connectivity Issue: IOS IPS DTM, page E-17](#)
- [System Rule: Resource Issue: IOS IPS DTM, page E-20](#)

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System: CS-MARS Incident Response

This category contains the following system rules:

This section contains the following topics:

- [System Rule: CS-MARS Host Mitigation - Failure, page E-6](#)
- [System Rule: CS-MARS Host Mitigation - Success, page E-6](#)
- [System Rule: Connectivity Issue: IOS IPS DTM, page E-17](#)
- [System Rule: Resource Issue: IOS IPS DTM, page E-20](#)

System Rule: CS-MARS Host Mitigation - Failure

This rule triggers when CS-MARS is unable to successfully mitigate a host after having tried a few times.

System Rule: CS-MARS Host Mitigation - Success

This rule triggers when CS-MARS is able to successfully mitigate a host.

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System: CS-MARS Issue

This category contains the following system rules:

This section contains the following topics:

- [System Rule: CS-MARS Database Partition Usage, page E-18](#)
- [System Rule: Resource Issue: CS-MARS, page E-20](#)
- [System Rule: CS-MARS Failure Saving Certificates/Fingerprints, page E-18](#)
- [System Rule: CS-MARS Authentication Method Modified - AAA to Local, page E-7](#)
- [System Rule: CS-MARS IPS Signature Update Failure, page E-18](#)
- [System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch, page E-18](#)

- [System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue, page E-18](#)
- [System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions, page E-18](#)
- [System Rule: CS-MARS Login Failures - Admin User, page E-8](#)
- [System Rule: CS-MARS Login Failures - Non-Admin User, page E-8](#)
- [System Rule: CS-MARS SMTP Server Communication Failure, page E-8](#)

System Rule: CS-MARS Database Partition Usage

This rule indicates that the current CS-MARS database partition filled up to 75% of its capacity and the next database partition will be purged soon to create space for new events. The estimated purge times are in the event message. This is normal CS-MARS activity and will result in old events and incidents to be purged from CS-MARS database. Users are urged to archive CS-MARS data to prevent permanent data loss.

System Rule: Resource Issue: CS-MARS

This rule detects resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System Rule: CS-MARS Failure Saving Certificates/Fingerprints

This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.

System Rule: CS-MARS Authentication Method Modified - AAA to Local

This rule indicates that CS-MARS authentication method was changed from AAA based authentication to Local authentication. Note that a prior change from Local to AAA would have invalidated the passwords in the local CS-MARS database for all but user: pnadmin. Therefore, administrative action is needed on an incident for this rule to re-enable local users if it is intended for them to access CS-MARS.

System Rule: CS-MARS IPS Signature Update Failure

This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.

System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a connectivity issue after 6 retries over the past 12 minutes. Prior to the past 12 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to incompatible software or data versions after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS Login Failures - Admin User

This correlation rule detects a CS-MARS admin user being locked out after several failed login attempts via the GUI. In addition to this, the rule detects 3 login failures via the CLI (count of 2 is used due to idiosyncrasies of CS-MARS/Linux login failure syslogs) as well as failed attempts to switch to expert mode. Note that the pnadmin user is never locked out from the CLI. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: CS-MARS Login Failures - Non-Admin User

This correlation rule detects a CS-MARS admin user being locked out after several failed login attempts. Authentication failures may sometimes be caused by a user forgetting the password.

System Rule: CS-MARS SMTP Server Communication Failure

This rule indicates that the CS-MARS failed to communicate with the SMTP server after 1 try over the past 3 minutes. Prior to past 3 minutes, communication was either healthy or the status was not known

System: Client Exploits, Virus, Worm and Malware

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Backdoor: Connect, page E-9](#)
- [System Rule: Client Exploit - Attempt, page E-9](#)
- [System Rule: Backdoor: Covert Channel, page E-9](#)
- [System Rule: Worm Propagation - Success Likely, page E-9](#)
- [System Rule: Client Exploit - Sysbug Trojan, page E-9](#)
- [System Rule: Backdoor: Spyware, page E-10](#)
- [System Rule: Network Activity: Windows Popup Spam, page E-10](#)
- [System Rule: Worm Propagation - Attempt, page E-10](#)
- [System Rule: Backdoor: Active, page E-10](#)
- [System Rule: Client Exploit - Success Likely, page E-10](#)

- [System Rule: Network Activity: Excessive Denies - Host Compromise Likely, page E-10](#)
- [System Rule: Client Exploit - Mass Mailing Worm, page E-10](#)
- [System Rule: Client Exploit - Sasser Worm, page E-11](#)
- [System Rule: Virus Found - Cleaned, page E-11](#)
- [System Rule: Virus Found - Not Cleaned, page E-11](#)
- [System Rule: New Malware Discovered, page E-15](#)
- [System Rule: New Malware Prevention Deployed, page E-15](#)
- [System Rule: New Malware Prevention Deployment Failed, page E-16](#)
- [System Rule: New Malware Traffic Match, page E-16](#)
- [System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter, page E-11](#)
- [System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter, page E-19](#)

System Rule: Backdoor: Connect

This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network - there may or may not be any follow-up activity on the destination host. Backdoors (e.g. Rootkits, Trojan Horse programs) and command shells provide extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

System Rule: Client Exploit - Attempt

This rule detects a client workstation exploit - this means a workstation is either downloading executable content via Web or email or sending web requests that contain scripts or is the target of an (client side) exploit via protocols such as IRC, DHCP, DNS, P2P Worms.

System Rule: Backdoor: Covert Channel

This correlation rule detects communication over covert channels - this means DMZ services such as HTTP, DNS, ICMP, FTP, SMTP etc. are being misused to tunnel inappropriate traffic via those ports. DMZ services are chosen since firewalls permit them but may not perform deep protocol inspection. Either the source or the destination in this event may be compromised.

System Rule: Worm Propagation - Success Likely

This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares accompanied by suspicious follow-up activity at the target destination host. Suspicious follow-up activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc.

System Rule: Client Exploit - Sysbug Trojan

This correlation rule detects a Sysbug Trojan exploit on a client workstation - the workstation downloaded executable content via email and the code executed and likely opened up Sysbug Trojan service on port 5555 to which other machines attempted to connect. Here, the source represents the client workstation and the destination represents the systems to which a connection is made after the trojan is installed.

System Rule: Backdoor: Spyware

This rule detects spyware e.g. Gator, Bonzi etc. installed on hosts or requests to hosts with spyware installed. Spyware are malicious applications that can be installed on a computer without the knowledge of the user, e.g. when one visits a web site or clicks on an advertising link or installs file sharing freeware such as KaZaA, iMesh, and AudioGalaxy. Once installed, the spyware automatically runs each time the host PC is started and records URLs visited, the username, password, and credit card information used, and then sends this information to the spyware writers.

System Rule: Network Activity: Windows Popup Spam

This correlation detects excessive traffic (likely pop up spam) from the same source to the Windows Messenger service.

System Rule: Worm Propagation - Attempt

This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.

System Rule: Backdoor: Active

This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network accompanied by malicious follow-up activity on the server hosting the backdoor - this may indicate that a malicious backdoor service is likely running in your network. Malicious follow-up activity includes excessive scans, denied packets, installation of malicious services, local buffer overflow attacks etc. Backdoors such as Unix rootkits or Trojan horses are malicious programs that offer extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

System Rule: Client Exploit - Success Likely

This correlation rule detects a client workstation exploit followed by the client performing anomalous activities. Client exploits include download of dynamically executable content via Web or email, web requests containing scripts, client side exploits via protocols such as IRC, DHCP, DNS, P2P Worms. Client anomalous activities include the client originating excessive denies and scans, attempting to connect to backdoors, propagating worms over the network. The presence of such activities may indicate that the client exploit is successful.

System Rule: Network Activity: Excessive Denies - Host Compromise Likely

This correlation rule detects a large frequency (excess of 10/sec) of denies from a particular host to a particular destination port. This is a typical behavior of a compromised host looking to exploit hosts with a specific vulnerability.

System Rule: Client Exploit - Mass Mailing Worm

This signature detects excessive amount of e-mail (at least 20/min) from a single host. To sharpen this rule for non-mail server hosts, create a group of mail server hosts and then create an exception by excluding these hosts in the source of this rule.

System Rule: Client Exploit - Sasser Worm

This correlation rule detects a successful infection spread of the Sasser worm - an attack on port 445 followed by the any of the following (a) command shell connection to the victim on port 9996, (b) an FTP connection back to the victim on port 5554, (c) excessive scans on port 445 from the victim. This indicates that both the source and the destinations are likely infected with the Sasser worm. This worm exploits the Microsoft Windows vulnerability as described in Microsoft Security Bulletin MS04-011

System Rule: Virus Found - Cleaned

This rule indicates that virus scanning software detected a virus and was able to clean it.

System Rule: Virus Found - Not Cleaned

This rule indicates that virus scanning software detected a virus and was unable to clean it.

System Rule: New Malware Discovered

This rule detects that Cisco Incident Control Server (ICS) has received information about a new virus/worm/malware outbreak. ICS is going to deploy ACLs or signatures to routers and IPS devices

System Rule: New Malware Prevention Deployed

This rule detects that Cisco Incident Control Server (ICS) has successfully deployed ACLs or signatures to routers and IPS devices in an attempt to prevent a newly discovered virus/worm/malware outbreak.

System Rule: New Malware Prevention Deployment Failed

This rule detects that Cisco Incident Control Server (ICS) has failed to deploy ACLs or signatures to routers and IPS devices for preventing a new virus/worm/malware outbreak.

System Rule: New Malware Traffic Match

This correlated rule detects a traffic pattern that (a) matches a worm pattern: same source to many distinct destinations and (b) matches the ACLs and signatures deployed by Cisco Incident Control Server (ICS) in response to a newly discovered virus/worm/malware outbreak.

System Rule: Suspicious Phone Home Activity: ASA Botnet Traffic Filter

This rule detects phone home activity to black/grey listed sites/IPs, as reported by ASA Botnet Traffic Filter.

System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter

This rule detects traffic activity originating from black/grey listed sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Configuration Issue

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Configuration Issue: Firewall, page E-12](#)
- [System Rule: Configuration Issue: Server, page E-12](#)
- [System Rule: Modify Network Config, page E-12](#)
- [System Rule: Modify Server: SCADA Modbus, page E-12](#)

System Rule: Configuration Issue: Firewall

This rule detects configuration errors reported by a firewall - this may cause certain traffic to be dropped by the firewall.

System Rule: Configuration Issue: Server

This rule detects configuration errors reported by a server - this may cause certain services to be not available at the server.

System Rule: Modify Network Config

This rule detects attempts to modify the configurations on a network device such as routers, switches, firewalls etc.

System Rule: Modify Server: SCADA Modbus

This rule detects attempts to modify the counters and diagnostics on a Modbus Servers. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System: Database Server Activity

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Database Privileged Command - Failures, page E-12](#)

System Rule: Database Privileged Command - Failures

This correlation rule detects multiple failed attempts from the same database user to execute privileged database commands.

System: Host Activity

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Modify Host: Files, page E-13](#)
- [System Rule: Modify Host: Service, page E-13](#)
- [System Rule: Modify Host: Logs, page E-13](#)
- [System Rule: Modify Host: Registry, page E-13](#)
- [System Rule: Modify Host: Security, page E-13](#)
- [System Rule: Modify Host: User Group, page E-13](#)
- [System Rule: Modify Host: Database Object - Failures, page E-13](#)
- [System Rule: Modify Host: Database User/Group - Failures, page E-14](#)

System Rule: Modify Host: Files

This rule detects attempts to modify files on a host.

System Rule: Modify Host: Service

This rule detects attempts to modify the settings of services on a host.

System Rule: Modify Host: Logs

This rule detects attempts to modify log files on a host.

System Rule: Modify Host: Registry

This rule detects attempts to modify windows registry entries on a host.

System Rule: Modify Host: Security

This rule detects attempts to modify the security settings on a host.

System Rule: Modify Host: User Group

This rule detects attempts to modify the user group definitions on a host.

System Rule: Modify Host: Database Object - Failures

This correlation rule detects multiple failed attempts from the same database user to modify database objects such as tables, indices etc.

System Rule: Modify Host: Database User/Group - Failures

This correlation rule detects multiple failed attempts from the same database user to modify database user groups

System: Network Attacks and DoS

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Sudden Traffic Increase To Port, page E-14](#)
- [System Rule: DoS: Network - Attempt, page E-14](#)
- [System Rule: Misc. Attacks: ARP Poisoning, page E-14](#)
- [System Rule: Misc. Attacks: Session Hijacking, page E-14](#)
- [System Rule: Misc. Attacks: Identity Spoofing, page E-14](#)
- [System Rule: DoS: Network - Success Likely, page E-15](#)
- [System Rule: DoS: Network Device - Attempt, page E-15](#)
- [System Rule: DoS: Network Device - Success Likely, page E-15](#)
- [System Rule: WLAN DoS Attack Detected, page E-15](#)

System Rule: Sudden Traffic Increase To Port

This rule detects scans statistically significant increase in traffic to a particular port.

System Rule: DoS: Network - Attempt

This rule detects network level denial of service (DoS) attacks along with relevant reconnaissance activity that may have preceded the attacks. Such attacks can create a dramatic increase in overall network traffic.

System Rule: Misc. Attacks: ARP Poisoning

This correlation rule detects ARP Poisoning attacks preceded by reconnaissance attempts to that host, if any.

System Rule: Misc. Attacks: Session Hijacking

This correlation rule detects attempts to hijack a TCP connection to that host, preceded by reconnaissance attempts to that host, if any.

System Rule: Misc. Attacks: Identity Spoofing

This correlation rule detects attempts to used spoofed source IP addresses.

System Rule: DoS: Network - Success Likely

This correlation rule detects the simultaneous occurrence of network level denial of service (DoS) attacks along with related events such as traffic anomaly (e.g. ICMP echo request/reply or TCP SYN/FIN anomaly), network devices reporting high utilization, excessive scans or denies in the network etc. This may indicate that the network is under denial of service attack.

System Rule: DoS: Network Device - Attempt

This correlation rule detects attacks on network devices (such as switches, routers, firewalls) along with relevant reconnaissance activity that may have preceded these attacks. Such attacks if successful, can crash the network devices and create a denial of service for the network segment containing these devices.

System Rule: DoS: Network Device - Success Likely

This correlation rule detects attacks on network devices (such as switches, routers, firewalls) along with (a) local high usage conditions reported by the device and (b) relevant reconnaissance activity that may have preceded these attacks.

System Rule: WLAN DoS Attack Detected

This rule detects various Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

System: New Malware Outbreak (Cisco ICS)

This category contains the following system rules:

This section contains the following topics:

- [System Rule: New Malware Discovered, page E-15](#)
- [System Rule: New Malware Prevention Deployed, page E-15](#)
- [System Rule: New Malware Prevention Deployment Failed, page E-16](#)
- [System Rule: New Malware Traffic Match, page E-16](#)

System Rule: New Malware Discovered

This rule detects that Cisco Incident Control Server (ICS) has received information about a new virus/worm/malware outbreak. ICS is going to deploy ACLs or signatures to routers and IPS devices

System Rule: New Malware Prevention Deployed

This rule detects that Cisco Incident Control Server (ICS) has successfully deployed ACLs or signatures to routers and IPS devices in an attempt to prevent a newly discovered virus/worm/malware outbreak.

System Rule: New Malware Prevention Deployment Failed

This rule detects that Cisco Incident Control Server (ICS) has failed to deploy ACLs or signatures to routers and IPS devices for preventing a new virus/worm/malware outbreak.

System Rule: New Malware Traffic Match

This correlated rule detects a traffic pattern that (a) matches a worm pattern: same source to many distinct destinations and (b) matches the ACLs and signatures deployed by Cisco Incident Control Server (ICS) in response to a newly discovered virus/worm/malware outbreak.

System: Operational Issue

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Network Errors - Likely Routing Related, page E-16](#)
- [System Rule: State Change: Host, page E-17](#)
- [System Rule: State Change: SCADA Modbus, page E-17](#)
- [System Rule: Operational Issue: Firewall, page E-17](#)
- [System Rule: Operational Issue: IDS, page E-17](#)
- [System Rule: Operational Issue: Server, page E-17](#)
- [System Rule: Operational Issue: Router / Switch, page E-17](#)
- [System Rule: State Change: Network Device, page E-17](#)
- [System Rule: Inactive CS-MARS Reporting Device, page E-17](#)
- [System Rule: Connectivity Issue: IOS IPS DTM, page E-17](#)
- [System Rule: CS-MARS Database Partition Usage, page E-18](#)
- [System Rule: CS-MARS Failure Saving Certificates/Fingerprints, page E-18](#)
- [System Rule: CS-MARS IPS Signature Update Failure, page E-18](#)
- [System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch, page E-18](#)
- [System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue, page E-18](#)
- [System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions, page E-18](#)
- [System Rule: Operational Issue: WLAN, page E-18](#)
- [System Rule: Rogue WLAN AP Detected, page E-18](#)

System Rule: Network Errors - Likely Routing Related

This rule detects a large frequency of denied packets or ICMP destination unreachable events between the same source, destination pair - this may indicate a network routing error and may be caused by periodic retransmission attempts by TCP or the application itself (e.g. DNS).

System Rule: State Change: Host

This correlation rule detects significant host status change events such as system failing, rebooting, interface cards coming up and down, audit log filling up or getting deleted etc...

System Rule: State Change: SCADA Modbus

This rule detects Modbus servers restarting. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Operational Issue: Firewall

This rule detects operational errors (e.g. bad network connectivity, failover errors, internal software/hardware errors) reported by a firewall - this may indicate that the firewall is not functioning properly.

System Rule: Operational Issue: IDS

This rule detects operational errors reported by a intrusion detection system (IDS) - this may indicate that the device is not functioning properly.

System Rule: Operational Issue: Server

This rule detects operational errors reported by a host or by applications on a host - this may indicate that either the host or the specific application on the host is not functioning properly.

System Rule: Operational Issue: Router / Switch

This rule detects operational errors reported by non-security network devices such as routers and switches.

System Rule: State Change: Network Device

This correlation rule detects significant network status state change events such as system failing, failover occurring, interface cards coming up and down etc.

System Rule: Inactive CS-MARS Reporting Device

This rule detects reporting devices that have not reported an event in the last hour. For chatty devices such as firewalls and IDS, this may indicate connectivity issues or an issue with the device themselves. This rule should be scoped down to only include chatty network infrastructure devices.

System Rule: Connectivity Issue: IOS IPS DTM

This rule detects connectivity issues between CS-MARS and IOS - CS-MARS may not be able to dynamically turn on ACTIVE signatures on IOS.

System Rule: CS-MARS Database Partition Usage

This rule indicates that the current CS-MARS database partition filled up to 75% of its capacity and the next database partition will be purged soon to create space for new events. The estimated purge times are in the event message. This is normal CS-MARS activity and will result in old events and incidents to be purged from CS-MARS database. Users are urged to archive CS-MARS data to prevent permanent data loss.

System Rule: CS-MARS Failure Saving Certificates/Fingerprints

This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.

System Rule: CS-MARS IPS Signature Update Failure

This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.

System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a connectivity issue after 6 retries over the past 12 minutes. Prior to the past 12 minutes, communication was either healthy or the status was not known.

System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions

This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to incompatible software or data versions after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

System Rule: Operational Issue: WLAN

This rule detects operational errors reported by a Cisco WLAN Controller - this may indicate that the device is not functioning properly.

System Rule: Rogue WLAN AP Detected

This rule detects Rogue Access Points as reported by events from a Cisco WLAN Controller.

System: Reconnaissance

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Scans: SCADA Modbus, page E-19](#)
- [System Rule: Scans: Stealth, page E-19](#)
- [System Rule: Scans: Targeted, page E-19](#)
- [System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter, page E-19](#)

System Rule: Scans: SCADA Modbus

This correlation rule detects scans targeted at Modbus servers. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Scans: Stealth

This rule detects highly suspicious scans that are performed by sending malformed TCP/IP packets with an intent to discover host and application characteristics such as OS name, OS version etc. A vulnerability assessment tool such as Nmap can generate such scans. The source of the scans, if from inside the trusted network, must be investigated to see if it is from an authorized source. A MARS appliance may be performing such a test as part of false positive analysis.

System Rule: Scans: Targeted

This rule detects scans that are either (a) targeted at a host to identify its operating environment, such as users on a host, DNS version, RPC services open etc. or (b) targeted at a well-known service to determine the set of host that offer that service.

System Rule: Suspicious Traffic from site: ASA Botnet Traffic Filter

This rule detects traffic activity originating from black/grey listed sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Resource Issue

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Resource Issue: Host, page E-20](#)
- [System Rule: Resource Issue: Network Device, page E-20](#)
- [System Rule: Resource Issue: IOS IPS DTM, page E-20](#)
- [System Rule: Resource Issue: CS-MARS, page E-20](#)

System Rule: Resource Issue: Host

This rule detects resource issues at a host, e.g. event log being full, disk near capacity, too many logged in users etc.

System Rule: Resource Issue: Network Device

This rule detects resource issues at a network device, e.g. router, switch, firewall or IDS. Such issues include high CPU usage, a firewall reaching session limit, insufficient memory etc.

System Rule: Resource Issue: IOS IPS DTM

This rule detects that a Cisco IOS router has too little memory for running the required set of ACTIVE IPS signatures. CS-MARS was not successful in downloading the complete ACTIVE signature set.

System Rule: Resource Issue: CS-MARS

This rule detects resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System: Restricted Network Traffic

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Network Activity: Excessive IRC, page E-20](#)
- [System Rule: Network Activity: Chat/IM - File Transfer, page E-20](#)
- [System Rule: Network Activity: P2P File Sharing - File Transfer, page E-21](#)
- [System Rule: Network Activity: Chat/IM - Active, page E-21](#)
- [System Rule: Network Activity: P2P File Sharing - Active, page E-21](#)
- [System Rule: Network Activity: Recreational, page E-21](#)
- [System Rule: Network Activity: Uncommon Traffic, page E-21](#)

System Rule: Network Activity: Excessive IRC

This correlation rule detects excessive Internet relay Chat (IRC) connections from the same source - this indicates that a Remote Admin Trojan (RAT) is likely running on the source and is likely compromised.

System Rule: Network Activity: Chat/IM - File Transfer

This rule detects file transfers via person-to-person Chat or Instant Messengers along with increase in network traffic if any. File transfer is not a normal use of Chat/IM and is suspicious. In addition, files shared with other IM users could contain viruses or other backdoor programs.

System Rule: Network Activity: P2P File Sharing - File Transfer

This rule detects a file transfer via a person-to-person file sharing application such as KaZaa, Napster, EDonkey, Gnutella, Bearshare etc. along with increase in network traffic if any. The programs may consume significant amount of network bandwidth and furthermore, inappropriate materials possibly containing viruses and backdoors may be distributed.

System Rule: Network Activity: Chat/IM - Active

This rule detects person-to-person Chat or Instant Messenger protocol activity.

System Rule: Network Activity: P2P File Sharing - Active

This rule detects person-to-person file sharing activity via applications such as KaZaa, Napster, EDonkey, Gnutella, Bearshare etc.

System Rule: Network Activity: Recreational

This rule detects recreational activities such as games, visiting adult web sites etc.

System Rule: Network Activity: Uncommon Traffic

This rule detects traffic that are not common in modern networks, for example (a) uncommon ICMP types - ICMP Router advertisement, ICMP Timestamp request/reply etc., (b) packets with uncommon TCP/IP options such source routing, timestamp etc, (c) standard protocols such as SMTP, HTTP, POP3 running on non-standard ports, (d) uncommon protocols such as FSP.

System: Security Posture Compliance (Cisco NAC)

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Vulnerable Host Found, page E-22](#)
- [System Rule: Security Posture: Audit Server Issue - Network wide, page E-22](#)
- [System Rule: Security Posture: Audit Server Issue - Single Host, page E-22](#)
- [System Rule: Security Posture: Infected - Network wide, page E-22](#)
- [System Rule: Security Posture: Infected - Single Host, page E-22](#)
- [System Rule: Security Posture: Excessive NAC Status Query Failures - Network wide, page E-22](#)
- [System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host, page E-23](#)
- [System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD, page E-23](#)
- [System Rule: Security Posture: Quarantined - Network wide, page E-23](#)
- [System Rule: Security Posture: Quarantined - Single Host, page E-23](#)

System Rule: Vulnerable Host Found

This rule detects vulnerable hosts/devices in the network. Such hosts/devices run services that are vulnerable or not patched properly.

System Rule: Security Posture: Audit Server Issue - Network wide

This rule detects excessive number of logs indicating network wide audit server issues - the indications can come from many hosts staying in TRANSITION posture state for too long or many AAA server reporting Audit Server communication problems. These events may indicate that the audit server is having difficulty in auditing and updating the end host security posture status from TRANSITION state. A host enters the TRANSITION state when it is not running the Cisco Trust Agent (CTA) software and requires an out-of-band audit by an audit server to move it out of TRANSITION state to any one of HEALTHY, INFECTED, QUARANTINE, CHECKUP or UNKNOWN states. A host in a TRANSITION state is likely to have limited or no network access.

System Rule: Security Posture: Audit Server Issue - Single Host

This rule detects excessive number of logs indicating audit server issues for a single host - the indications can come from the host staying in TRANSITION posture state for too long or AAA server reporting Audit Server communication problems for the same host. These events may indicate that the audit server is having difficulty in auditing and updating the end host security posture status from TRANSITION state. A host enters the TRANSITION state when it is not running the Cisco Trust Agent (CTA) software and requires an out-of-band audit by an audit server to move it out of TRANSITION state to any one of HEALTHY, INFECTED, QUARANTINE, CHECKUP or UNKNOWN states. A host in a TRANSITION state is likely to have limited or no network access.

System Rule: Security Posture: Infected - Network wide

This rule detects that many distinct hosts are reporting INFECTED security posture status for an excessive period of time. This implies that a significant number of hosts are having trouble getting cleaned.

System Rule: Security Posture: Infected - Single Host

This rule detects that a particular host is reporting INFECTED security posture status for an excessive period of time. This implies that the host is having trouble getting cleaned.

System Rule: Security Posture: Excessive NAC Status Query Failures - Network wide

This rule detects excessive network-wide NAC status query failures reported by distinct end host, Network Access Device (NAD) combinations. A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. Excessive status query failures reported by distinct NAD and end host combinations may indicate a critical software problem..

System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host

This rule detects excessive NAC status query failures from the same end host. A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. The end host may be compromised; at least this behavior is suspicious.

System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD

This rule detects excessive NAC status query failures from distinct hosts to the same Network Access Device (NAD). A Status query failure indicates a change in posture detected by the Cisco Trust Agent (CTA) after the initial authorization. Excessive status query failures may indicate a sign of end point instability caused by the user enabling or disabling agents. Excessive status query failures from distinct hosts reported by the same NAD may indicate a problem at the NAD.

System Rule: Security Posture: Quarantined - Network wide

This rule detects that many distinct hosts are reporting QUARANTINED security posture status for an excessive period of time. This implies that a significant number of hosts are having trouble getting DAT file updates.

System Rule: Security Posture: Quarantined - Single Host

This rule detects that a particular host is reporting QUARANTINE security posture status for an excessive period of time. This implies that the host is having trouble getting DAT file updates.

System: Server Exploits

This category contains the following system rules:

This section contains the following topics:

- [System Rule: Local Attack - Attempt, page E-24](#)
- [System Rule: Server Attack: Sniffer - Attempt, page E-24](#)
- [System Rule: Server Attack: Sniffer - Success Likely, page E-24](#)
- [System Rule: Local Attack - Success Likely, page E-24](#)
- [System Rule: Server Attack: SCADA Modbus - Attempt, page E-24](#)
- [System Rule: Misc. Attacks: Application Admin Escalation, page E-25](#)
- [System Rule: Misc. Attacks: Evasion, page E-25](#)
- [System Rule: Misc. Attacks: TCP/IP Protocol Anomaly, page E-25](#)
- [System Rule: Misc. Attacks: Replay, page E-25](#)
- [System Rule: Server Attack: Database - Attempt, page E-25](#)
- [System Rule: Server Attack: DNS - Attempt, page E-25](#)
- [System Rule: Server Attack: FTP - Attempt, page E-25](#)
- [System Rule: Server Attack: Login - Attempt, page E-25](#)
- [System Rule: Server Attack: Mail - Attempt, page E-26](#)

- [System Rule: Server Attack: Misc. - Attempt, page E-26](#)
- [System Rule: Server Attack: RPC - Attempt, page E-26](#)
- [System Rule: Server Attack: SNMP - Attempt, page E-26](#)
- [System Rule: Server Attack: Web - Attempt, page E-26](#)
- [System Rule: Misc. Attacks: Access Web Customer Data, page E-26](#)
- [System Rule: Server Attack: Database - Success Likely, page E-26](#)
- [System Rule: Server Attack: DNS - Success Likely, page E-27](#)
- [System Rule: Server Attack: FTP - Success Likely, page E-27](#)
- [System Rule: Server Attack: Login - Success Likely, page E-27](#)
- [System Rule: Server Attack: Mail - Success Likely, page E-27](#)
- [System Rule: Server Attack: Misc. - Success Likely, page E-27](#)
- [System Rule: Server Attack: RPC - Success Likely, page E-27](#)
- [System Rule: Server Attack: SNMP - Success Likely, page E-28](#)
- [System Rule: Server Attack: Web - Success Likely, page E-28](#)

System Rule: Local Attack - Attempt

This correlation rule detects attacks on hosts by logged on users. Such attacks include local buffer overflow attacks, sym link attacks etc.

System Rule: Server Attack: Sniffer - Attempt

This correlation rule detects denial of service attacks on a host in promiscuous host (e.g. a network IDS host).

System Rule: Server Attack: Sniffer - Success Likely

This correlation rule detects denial of service attacks on a host in promiscuous host (e.g. a network IDS host) followed by the destination host reporting functionally anomalous behavior.

System Rule: Local Attack - Success Likely

This correlation rule detects attacks on hosts by locally logged on users followed by the server performing anomalous activities - such activities include excessive denials and scans, connection to backdoors, attempts to propagate worms etc. The presence of such activities may indicate that the host is compromised.

System Rule: Server Attack: SCADA Modbus - Attempt

This correlation rule detects attacks on Modbus servers, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, denial of service attempts etc. Modbus protocol is the defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network, where the Programmable logic controllers (PLCs) act as Modbus servers.

System Rule: Misc. Attacks: Application Admin Escalation

This correlation rule detects attempts by a non-administrative user to perform administrative functions for Web applications by bypassing the required authentication. Several web applications have vulnerabilities that may allow an attacker to do so. These attempts may be preceded by reconnaissance attempts to that host.

System Rule: Misc. Attacks: Evasion

This correlation rule detects generic attempts by an attacker to bypass network IDS systems. The attempts may be preceded by reconnaissance attempts to that host.

System Rule: Misc. Attacks: TCP/IP Protocol Anomaly

This correlation rule detects events that indicate errors in standard TCP/IP headers - these may be caused by broken protocol implementations on the source host or may be malicious attempts by the source host to test the robustness of protocol implementations on the destination host.

System Rule: Misc. Attacks: Replay

This correlation rule detects replay attacks on a host, preceded by reconnaissance attempts to that host, if any. Successful replay attacks may allow the attacker to gain access by bypassing authentication.

System Rule: Server Attack: Database - Attempt

This correlation rule detects attacks on a database server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.

System Rule: Server Attack: DNS - Attempt

This correlation rule detects specific attacks on a DNS host, preceded by reconnaissance attempts targeted to that host, if any. Attacks on a DNS host includes buffer overflow attempts, denial of service attempts.

System Rule: Server Attack: FTP - Attempt

This correlation rule detects attacks on a FTP server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts using FTP server privileges, denial of service attempts.

System Rule: Server Attack: Login - Attempt

This correlation rule detects attacks on login services on a host, preceded by reconnaissance attempts targeted to that host, if any. Login services include Telnet, SSH, R-protocols such as Rsh, Rlogin, Rexec etc. The attacks include buffer overflows, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: Mail - Attempt

This correlation rule detects attacks on mail services (SMTP, POP, IMAP) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks to mail services include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: Misc. - Attempt

This correlation rule detects attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: RPC - Attempt

This correlation rule detects attacks on RPC services on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.

System Rule: Server Attack: SNMP - Attempt

This correlation rule detects attacks on SNMP implementation on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, privilege escalation attempts to become root, etc.

System Rule: Server Attack: Web - Attempt

This correlation rule detects attacks on a web server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, denial of service attempts etc.

System Rule: Misc. Attacks: Access Web Customer Data

This correlation rule detects malicious attempts to access customer data stored by web applications, preceded by reconnaissance attempts to that host, if any. Customer data typically contains sensitive information such as purchasing history, credit card numbers etc.

System Rule: Server Attack: Database - Success Likely

This correlation rule detects specific attacks on a database server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a database server include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.

System Rule: Server Attack: DNS - Success Likely

This correlation rule detects likely successful attacks on a DNS host - an attack is successful if it is followed by suspicious activity on the targeted DNS server. Suspicious activity includes the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host.

System Rule: Server Attack: FTP - Success Likely

This correlation rule detects specific attacks on a FTP server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a FTP server include buffer overflows, remote command execution attempts using FTP server privileges, denial of service attempts.

System Rule: Server Attack: Login - Success Likely

This correlation rule detects specific attacks on login services on a host (e.g. Telnet, SSH, R-protocols such as Rsh, Rlogin, Rexec etc.) followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a login server include buffer overflows, remote command execution attempts using the server privileges, denial of service attempts.

System Rule: Server Attack: Mail - Success Likely

This correlation rule detects specific attacks on mail services (SMTP, POP, IMAP) on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to a mail server include buffer overflows, remote command execution attempts using server privileges, denial of service attempts.

System Rule: Server Attack: Misc. - Success Likely

This correlation rule detects specific attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks include buffer overflows, remote command execution attempts using server privileges, denial of service attempts etc.

System Rule: Server Attack: RPC - Success Likely

This correlation rule detects specific attacks on RPC services on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to RPC services include buffer overflows, remote command execution attempts using system privileges, denial of service attempts.

System Rule: Server Attack: SNMP - Success Likely

This correlation rule detects specific attacks on SNMP implementation on a host followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks to RPC services include buffer overflows, remote command execution attempts using system privileges, denial of service attempts.

System Rule: Server Attack: Web - Success Likely

This correlation rule detects specific attacks on a web server followed by suspicious activity on the targeted host. Suspicious activity may include the host scanning the network, creating excessive firewall deny traffic, a backdoor opening up at the server etc. The attack may be preceded by reconnaissance attempts targeted to that host. The attacks include buffer overflows, remote command execution attempts, denial of service attempts etc.

System Reports by Category

This topic defines the complete list of system reports, organized by category, issued with this release.

This section contains the following topics:

- [System: ASA Botnet Traffic Filter, page E-29](#)
- [System: Access, page E-30](#)
- [System: All Events - Aggregate View, page E-33](#)
- [System: All Exploits - Aggregate View, page E-35](#)
- [System: COBIT DS3.3 - Monitoring and Reporting, page E-36](#)
- [System: COBIT DS5.10: Security Violations, page E-38](#)
- [System: COBIT DS5.19: Malicious software, page E-41](#)
- [System: COBIT DS5.20: Firewall control, page E-42](#)
- [System: COBIT DS5.2: Authentication and Access, page E-44](#)
- [System: COBIT DS5.4: User Account Changes, page E-46](#)
- [System: COBIT DS5.7: Security Surveillance, page E-46](#)
- [System: COBIT DS9.4: Configuraton Control, page E-47](#)
- [System: COBIT DS9.5: Unauthorized Software, page E-48](#)
- [System: CS-MARS Distributed Threat Mitigation \(Cisco DTM\), page E-49](#)
- [System: CS-MARS Incident Response, page E-49](#)
- [System: CS-MARS Issue, page E-50](#)
- [System: Client Exploits, Virus, Worm and Malware, page E-53](#)
- [System: Configuration Changes, page E-55](#)
- [System: Configuration Issue, page E-56](#)
- [System: Database Server Activity, page E-57](#)
- [System: FISMA Compliance Reports, page E-59](#)

- [System: GLBA Compliance Reports, page E-70](#)
- [System: HIPAA Compliance Reports, page E-80](#)
- [System: Host Activity, page E-92](#)
- [System: Network Attacks and DoS, page E-93](#)
- [System: New Malware Outbreak \(Cisco ICS\), page E-94](#)
- [System: Operational Issue, page E-94](#)
- [System: PCI DSS01: Install, Maintain FW, Protect Cardholder Data, page E-96](#)
- [System: PCI DSS02: Do Not Use Default PWD & Security Parameters, page E-101](#)
- [System: PCI DSS03: Protect Store Cardholder Data, page E-103](#)
- [System: PCI DSS04: Encrypt Transmission of Cardholder Data, page E-107](#)
- [System: PCI DSS05: Use and Regularly Update Anti-Virus Software, page E-108](#)
- [System: PCI DSS06: Develop, Maintain Secured System/Application, page E-111](#)
- [System: PCI DSS07: Restrict Access to Cardholder Data, page E-116](#)
- [System: PCI DSS08: Assign Unique ID to Person with Comp Access, page E-118](#)
- [System: PCI DSS09: Restrict Physical Access to Cardholder Data, page E-121](#)
- [System: PCI DSS10: Track, Monitor All Network Access, Card Data, page E-122](#)
- [System: PCI DSS11: Regularly Test Security Systems and Processes, page E-125](#)
- [System: PCI DSS12: Maintain InfoSec Policy for All Personnel, page E-128](#)
- [System: Reconnaissance, page E-131](#)
- [System: Resource Issue, page E-132](#)
- [System: Resource Usage, page E-133](#)
- [System: Restricted Network Traffic, page E-135](#)
- [System: SOX 302\(a\)\(4\)\(A\), page E-136](#)
- [System: SOX 302\(a\)\(4\)\(D\), page E-137](#)
- [System: SOX Compliance Reports, page E-138](#)
- [System: Security Posture Compliance \(Cisco NAC\), page E-148](#)
- [System: Server Exploits, page E-152](#)

System: ASA Botnet Traffic Filter

This category contains the following system reports:

This section contains the following topics:

- [Activity: ASA Botnet Traffic Filter: Phone Home - All Events, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Botnet Sites, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Botnet Ports, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Infected Hosts, page E-55](#)
- [Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events, page E-132](#)

Activity: ASA Botnet Traffic Filter: Phone Home - All Events

This report details all suspicious events related to phone home activity, as reported by ASA Botnet Traffic Filter.

Activity: ASA Botnet Traffic Filter - Top Botnet Sites

This report ranks top botnet sites (black/grey listed sites) for all inbound/outbound sessions as reported by ASA Botnet Traffic Filter.

Activity: ASA Botnet Traffic Filter - Top Botnet Ports

This report ranks top destination ports for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.

Activity: ASA Botnet Traffic Filter - Top Infected Hosts

This report ranks top infected hosts for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.

Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events

This report details all events related to traffic originating from black/grey sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Access

This category contains the following system reports:

This section contains the following topics:

- [Attacks: Password - Top Event Types, page E-31](#)
- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Attacks: Password - Top Destinations, page E-144](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)

- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Attacks: Password: Locked Accounts - All Events, page E-124](#)
- [Attacks: Password: Restricted Times - All Events, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)
- [Activity: CS-MARS Login Failures, page E-91](#)

Attacks: Password - Top Event Types

This report ranks password retrieving and guessing attacks. The password can be system passwords or application passwords.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Passwords attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

System: All Events - Aggregate View

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Destination Ports, page E-102](#)
- [Activity: All - Top Destinations, page E-134](#)
- [Activity: All - Top Event Type Groups, page E-34](#)
- [Activity: All - Top Event Types, page E-47](#)
- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: All - Top Sources, page E-134](#)
- [Activity: All - Top Users, page E-85](#)
- [Activity: All - NAT Connections, page E-34](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: All Sessions - Top Destinations by Bytes, page E-134](#)

- [Detailed NAC Report, page E-35](#)

Activity: All - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Destinations

This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Event Type Groups

This report ranks event type groups by reported events that belong to each group. The event type groups give a general feeling about the type of network activity reported to MARS.

Activity: All - Top Event Types

This report ranks the event types of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: All - Top Sources

This report ranks the session sources of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Users

This report tracks the most frequent logins and other user activity by showing the most active user names.

Activity: All - NAT Connections

This report lists Network Address Translations performed on non-denied sessions as reported to MARS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: All Sessions - Top Destinations by Bytes

This report ranks all destinations by bytes transferred.

Detailed NAC Report

Detailed NAC Report

System: All Exploits - Aggregate View

This category contains the following system reports:

This section contains the following topics:

- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Seen - Top Reporting Devices, page E-141](#)
- [Attacks: All - Top Sources, page E-142](#)
- [Attacks: All - Top Event Type Groups, page E-143](#)
- [Attacks: All - All Events, page E-40](#)
- [Activity: Attacks Seen - Top Event Types, page E-130](#)
- [Attacks: All - Top Destinations, page E-144](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Attacks: All - All Events

This event details details (event type, destination, source) for all attack events.

Activity: Attacks Seen - Top Event Types

This report ranks the top attack event types.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

System: COBIT DS3.3 - Monitoring and Reporting

This category contains the following system reports:

This section contains the following topics:

- [Operational Issues: Network - Top Reporting Devices, page E-143](#)
- [Operational Issues: Server - Top Reporting Devices, page E-143](#)
- [Resource Issues: Network - Top Reporting Devices, page E-143](#)
- [Resource Issues: Server - Top Reporting Devices, page E-143](#)
- [Resource Utilization: Bandwidth: Inbound - Top Interfaces, page E-146](#)
- [Resource Utilization: CPU - Top Devices, page E-146](#)
- [Resource Utilization: Bandwidth: Outbound - Top Interfaces, page E-146](#)
- [Resource Utilization: Concurrent Connections - Top Devices, page E-146](#)
- [Resource Utilization: Errors: Inbound - Top Interfaces, page E-146](#)
- [Resource Utilization: Errors: Outbound - Top Interfaces, page E-146](#)
- [Resource Utilization: Memory - Top Devices, page E-146](#)
- [Activity: Sudden Traffic Increase To Port - All Destinations, page E-93](#)
- [Activity: Sudden Traffic Increase To Port - All Sources, page E-93](#)
- [Operational Issues: Network - All Events, page E-147](#)
- [Operational Issues: Server - All Events, page E-148](#)
- [Resource Issues: Network - All Events, page E-132](#)
- [Resource Issues: Server - All Events, page E-133](#)

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Operational Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate operational issues with servers.

Resource Issues: Network - Top Reporting Devices

This report summarizes the events that represent resource issues with network devices such as firewalls, routers and switches.

Resource Issues: Server - Top Reporting Devices

This report summarizes the events that represent resource issues with servers. These are likely to be Host IDS events.

Resource Utilization: Bandwidth: Inbound - Top Interfaces

This report ranks the inbound bandwidth utilization of the interfaces on the devices managed by PN-MARS.

Resource Utilization: CPU - Top Devices

This report ranks the CPU utilization of the devices managed by PN-MARS.

Resource Utilization: Bandwidth: Outbound - Top Interfaces

This report ranks the outbound bandwidth utilization of interfaces on devices managed by Pn-MARS.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Resource Utilization: Errors: Inbound - Top Interfaces

This report ranks by error rate on the inbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Errors: Outbound - Top Interfaces

This report ranks by error rate on the outbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Memory - Top Devices

This report ranks the memory utilization of the devices managed by PN-MARS.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

Operational Issues: Server - All Events

This report lists details about events that indicate operational errors on hosts or host applications.

Resource Issues: Network - All Events

This report lists event details for all events related to resource issues on network devices such as IDS, routers, firewalls etc.

Resource Issues: Server - All Events

This report lists event details for all resource issues on hosts. These are reported by Host IDS or Operating System logs.

System: COBIT DS5.10: Security Violations

This category contains the following system reports:

This section contains the following topics:

- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: Scans - Top Destination Ports, page E-141](#)
- [Activity: Scans - Top Destinations, page E-141](#)
- [Activity: Stealth Scans - Top Sources, page E-142](#)
- [Attacks: Database Server - Top Event Types, page E-152](#)
- [Attacks: FTP Server - Top Event Types, page E-152](#)
- [Attacks: Identity Spoofing - Top Event Types, page E-153](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Attacks: Mail Server - Top Event Types, page E-153](#)
- [Attacks: Network DoS - Top Event Types, page E-142](#)
- [Attacks: RPC Services - Top Event Types, page E-153](#)
- [Attacks: SNMP - Top Event Types, page E-153](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Attacks: All - Top Event Type Groups, page E-143](#)
- [Attacks: All - All Events, page E-40](#)

- [Attacks: Uncommon or Anomalous Traffic - Top Event Types, page E-153](#)
- [Activity: Database Privileged Command Failures - All Events, page E-145](#)
- [Activity: Database User/Group Change Failures - All Events, page E-145](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: Sudden Traffic Increase To Port - All Destinations, page E-93](#)
- [Activity: Sudden Traffic Increase To Port - All Sources, page E-93](#)
- [Attacks: Password - All Events, page E-147](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: SNMP - Top Event Types

This report ranks SNMP based attacks over the past hour.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Attacks: All - All Events

This event details details (event type, destination, source) for all attack events.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Attacks: Password - All Events

This report details all password attack events.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

System: COBIT DS5.19: Malicious software

This category contains the following system reports:

This section contains the following topics:

- [Activity: Backdoor - Top Event Types, page E-129](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Attacks: Virus/Worms - Top Sources, page E-143](#)
- [Activity: Backdoor - Top Destinations, page E-129](#)
- [Activity: Backdoor - Top Hosts, page E-130](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Activity: Virus/Worms - Top Infected Hosts, page E-145](#)
- [Activity: Virus: Detected - Top Users, page E-145](#)

- [Activity: Virus: Infections - Top Users, page E-145](#)

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

System: COBIT DS5.20: Firewall control

This category contains the following system reports:

This section contains the following topics:

- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Web Usage - Top Sources, page E-43](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Activity: Web Usage - Top Destinations by Bytes, page E-43](#)
- [Activity: Web Usage - Top Destinations by Sessions, page E-43](#)
- [Resource Utilization: Concurrent Connections - Top Devices, page E-146](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Web Usage - Top Sources

This signature ranks source addresses based on web use.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Activity: Web Usage - Top Destinations by Bytes

This report ranks the web servers by bytes transferred.

Activity: Web Usage - Top Destinations by Sessions

This report ranks the top web destinations by session count.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

System: COBIT DS5.2: Authentication and Access

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Admin Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Attacks: Password: Locked Accounts - All Events, page E-124](#)
- [Attacks: Password: Restricted Times - All Events, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)
- [Activity: Database Login Successes - All Events, page E-148](#)
- [Activity: CS-MARS Login Failures, page E-91](#)

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

System: COBIT DS5.4: User Account Changes

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host User/Group Management - All Events, page E-144](#)
- [Activity: Host User/Group Management - Top hosts, page E-144](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Database User/Group Change Successes - Top Users, page E-146](#)

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

System: COBIT DS5.7: Security Surveillance

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Event Types, page E-47](#)
- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Seen - Top Reporting Devices, page E-141](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: Inactive Reporting Device - Top Devices, page E-95](#)

Activity: All - Top Event Types

This report ranks the event types of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Inactive Reporting Device - Top Devices

This report lists devices that are configured to be reporting to CS-MARS but haven't reported any event in the last hour.

System: COBIT DS9.4: Configuration Control

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

System: COBIT DS9.5: Unauthorized Software

This category contains the following system reports:

This section contains the following topics:

- [Activity: IRC - All Events, page E-143](#)
- [Activity: Recreational - All Events, page E-146](#)
- [Activity: Spyware - All Events, page E-147](#)
- [Activity: P2P Filesharing/Chat - All Events, page E-136](#)
- [Activity: Uncommon or Anomalous Traffic - All Events, page E-136](#)

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Activity: Recreational - All Events

This event details all users involved in recreational activities such as games, specific web sites such as gambling etc.

Activity: Spyware - All Events

This event details all spyware events.

Activity: P2P Filesharing/Chat - All Events

This event details all P2P File sharing or Chat event details.

Activity: Uncommon or Anomalous Traffic - All Events

This report details uncommon or anomalous traffic such as unused TCP options, uncommon ICMP traffic, non-standard traffic on standard port, tunneled traffic etc.

System: CS-MARS Distributed Threat Mitigation (Cisco DTM)

This category contains the following system reports:

This section contains the following topics:

- [Activity: IOS IPS DTM Successful Signature Tuning - All Events, page E-50](#)
- [Connectivity Issue: IOS IPS DTM - All Events, page E-96](#)
- [Resource Issues: IOS IPS DTM - Top Devices, page E-133](#)
- [Resource Issues: IOS IPS DTM - All Events, page E-133](#)

Activity: IOS IPS DTM Successful Signature Tuning - All Events

This report lists all successful IOS IPS signature download activities - both addition and deletion. CS-MARS Distributed Threat Mitigation (DTM) turns on ACTIVE IPS signatures on IOS routers.

Connectivity Issue: IOS IPS DTM - All Events

This report lists connectivity issues between CS-MARS and IOS IPS devices. Connectivity issues may prevent CS-MARS from turning on ACTIVE signatures on IOS IPS.

Resource Issues: IOS IPS DTM - Top Devices

This report lists IOS IPS routers that are running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to IOS IPS devices.

Resource Issues: IOS IPS DTM - All Events

This report lists event details that indicate certain IOS IPS routers running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to those IOS IPS devices.

System: CS-MARS Incident Response

This category contains the following system reports:

This section contains the following topics:

- [Activity: CS-MARS Host Mitigation - Failure - All Events, page E-89](#)
- [Activity: CS-MARS Host Mitigation - Success - All Events, page E-89](#)
- [Activity: IOS IPS DTM Successful Signature Tuning - All Events, page E-50](#)
- [Activity: WLAN Successful Mitigations, page E-50](#)

Activity: CS-MARS Host Mitigation - Failure - All Events

This report lists failed CS-MARS mitigation attempts - these can result from improper network connectivity or device access credentials.

Activity: CS-MARS Host Mitigation - Success - All Events

This report lists successful mitigations from CS-MARS.

Activity: IOS IPS DTM Successful Signature Tuning - All Events

This report lists all successful IOS IPS signature download activities - both addition and deletion. CS-MARS Distributed Threat Mitigation (DTM) turns on ACTIVE IPS signatures on IOS routers.

Activity: WLAN Successful Mitigations

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts that were mitigated from accessing the network as reported by a Cisco WLAN Controller

System: CS-MARS Issue

This category contains the following system reports:

This section contains the following topics:

- [Activity: Unknown Events - All Events, page E-51](#)
- [Resource Issues: CS-MARS - All Events, page E-133](#)
- [Resource Utilization: CS-MARS - All Events, page E-96](#)
- [Activity: CS-MARS Accepted New Certificates/Fingerprints, page E-51](#)
- [Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints, page E-51](#)
- [Activity: CS-MARS Detected Conflicting Certificates/Fingerprints, page E-51](#)
- [Activity: CS-MARS Failure Saving Certificates/Fingerprints, page E-96](#)
- [Activity: CS-MARS Device Connectivity Errors, page E-96](#)
- [Activity: CS-MARS Authentication Method Modifications, page E-51](#)
- [Activity: CS-MARS pnaadmin User Password Status, page E-91](#)
- [Activity: CS-MARS Accounts Locked, page E-52](#)
- [Activity: CS-MARS IPS Signature Update Success - All Events, page E-130](#)
- [Activity: CS-MARS Successful Logins, page E-91](#)
- [Activity: CS-MARS IPS Signature Update Failure - All Events, page E-131](#)
- [Activity: CS-MARS Login Failures, page E-91](#)
- [Activity: CS-MARS LC-GC Communication Recovered, page E-52](#)
- [Activity: CS-MARS Accounts Unlocked, page E-52](#)
- [Activity: CS-MARS LC-GC Communication Failures, page E-96](#)

Activity: Unknown Events - All Events

This report tracks the events that are unknown to MARS.

Resource Issues: CS-MARS - All Events

This report lists event details for all events related to resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

Resource Utilization: CS-MARS - All Events

This report lists event details for all events related to CS-MARS resource utilization, e.g. database partitions, etc.

Activity: CS-MARS Accepted New Certificates/Fingerprints

This report lists event details due to CS-MARS accepting new SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints

This report lists event details due to CS-MARS accepting conflicting SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Detected Conflicting Certificates/Fingerprints

This report lists event details due to CS-MARS detecting conflicting SSL certificates or SSH Key Fingerprints when connecting to remote devices.

Activity: CS-MARS Failure Saving Certificates/Fingerprints

This report lists event details due to CS-MARS failure to save new or changed SSL certificates or SSH Key Fingerprints based on explicit user action or automatic accept due to SSL/SSH Settings.

Activity: CS-MARS Device Connectivity Errors

This report lists event details of CS-MARS device connectivity errors due to various reasons (e.g. conflicting SSL certificates or SSH key fingerprints, network timeout etc.). This includes both transient and persisting errors.

Activity: CS-MARS Authentication Method Modifications

This report details events due to CS-MARS LC activity due to authentication method changes from Local DB to AAA or AAA to Local DB

Activity: CS-MARS pnadmin User Password Status

This report details events due to CS-MARS LC 'pnadmin' user account password activity such as change in password or if the password continues to remain factory default which is checked once in 24 hours

Activity: CS-MARS Accounts Locked

This report details events due to CS-MARS LC accounts that are locked due to excessive login failures or explicit admin user action

Activity: CS-MARS IPS Signature Update Success - All Events

This report lists event details of all success events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate success steps in auto update or complete/partial success of updating the CS-MARS database with the downloaded IPS signature package.

Activity: CS-MARS Successful Logins

This report details events due to CS-MARS LC successful logins

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

Activity: CS-MARS LC-GC Communication Recovered

This reports lists event details over the past hour due to all restored communications between CS-MARS Local Controller with its Global Controller that had failed due to various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

Activity: CS-MARS Accounts Unlocked

This report details events due to CS-MARS LC accounts that are unlocked by an admin user

Activity: CS-MARS LC-GC Communication Failures

This reports lists event details over the past hour due to all communication failures between CS-MARS Local Controller with its Global Controller for various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

System: Client Exploits, Virus, Worm and Malware

This category contains the following system reports:

This section contains the following topics:

- [Activity: Backdoor - Top Event Types, page E-129](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Attacks: Virus/Worms - Top Sources, page E-143](#)
- [Activity: Backdoor - Top Destinations, page E-129](#)
- [Activity: Backdoor - Top Hosts, page E-130](#)
- [Attacks: Client Exploits - Top Sources, page E-54](#)
- [Activity: Virus/Worms - Top Infected Hosts, page E-145](#)
- [Activity: Virus: Detected - Top Users, page E-145](#)
- [Activity: Virus: Infections - Top Users, page E-145](#)
- [Activity: New Malware Discovered - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Failure - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Success - All Events, page E-112](#)
- [Activity: New Malware Traffic Match - All Events, page E-113](#)
- [Activity: New Malware Traffic Match - Top Sources, page E-127](#)
- [Activity: Sudden Traffic Increase To Port - All Destinations, page E-93](#)
- [Activity: Sudden Traffic Increase To Port - All Sources, page E-93](#)
- [Activity: ASA Botnet Traffic Filter: Phone Home - All Events, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Botnet Sites, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Botnet Ports, page E-55](#)
- [Activity: ASA Botnet Traffic Filter - Top Infected Hosts, page E-55](#)
- [Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events, page E-132](#)

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Attacks: Client Exploits - Top Sources

This report ranks hosts by the number of exploits originating from each host.

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: New Malware Discovered - All Events

This report lists all the new virus/worm/malware outbreaks discovered by Cisco Incident Control Server.

Activity: New Malware Prevention Deployment Failure - All Events

This report lists all devices to which ACL and signature deployment attempts by a Cisco Incident Control Server, in response to a new virus/worm/malware outbreak, failed.

Activity: New Malware Prevention Deployment Success - All Events

This report lists all destinations (Cisco IOS IPS devices and IPS appliances) to which Cisco Incident Control Server has deployed new ACLs and signatures in response to a new virus/worm/malware outbreak.

Activity: New Malware Traffic Match - All Events

This report details the traffic sources and the enforcing devices that match the ACLs and signatures deployed by the Cisco Incident Control Server in response to a newly discovered malware outbreak.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: ASA Botnet Traffic Filter: Phone Home - All Events

This report details all suspicious events related to phone home activity, as reported by ASA Botnet Traffic Filter.

Activity: ASA Botnet Traffic Filter - Top Botnet Sites

This report ranks top botnet sites (black/grey listed sites) for all inbound/outbound sessions as reported by ASA Botnet Traffic Filter.

Activity: ASA Botnet Traffic Filter - Top Botnet Ports

This report ranks top destination ports for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.

Activity: ASA Botnet Traffic Filter - Top Infected Hosts

This report ranks top infected hosts for traffic originating from infected hosts to black/grey listed sites, for all sessions as seen by MARS.

Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events

This report details all events related to traffic originating from black/grey sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Configuration Changes

This category contains the following system reports:

This section contains the following topics:

- [Configuration Changes: Network - Top Event Types, page E-102](#)
- [Configuration Changes: Server - Top Event Types, page E-98](#)

- [Configuration Changes: Server - Top Reporting Devices, page E-103](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

System: Configuration Issue

This category contains the following system reports:

This section contains the following topics:

- [Configuration Issues: Network - Top Reporting Devices, page E-107](#)
- [Configuration Issues: Server - Top Reporting Devices, page E-75](#)
- [Configuration Issues: Network - All Events, page E-107](#)
- [Configuration Issues: Server - All Events, page E-79](#)

Configuration Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in network devices such as firewalls, routers and switches.

Configuration Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in servers. These are likely to be Host IDS events.

Configuration Issues: Network - All Events

This report lists details for events that indicate configuration error on network devices.

Configuration Issues: Server - All Events

This report lists details for all events that indicate configuration errors on hosts or host applications.

System: Database Server Activity

This category contains the following system reports:

This section contains the following topics:

- [Activity: Database Object Modification Failures - All Events, page E-105](#)
- [Activity: Database Object Modification Failures - Top Users, page E-105](#)
- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Activity: Database Object Modification Successes - Top Users, page E-105](#)
- [Activity: Database Privileged Command Failures - All Events, page E-145](#)
- [Activity: Database Privileged Command Failures - Top Users, page E-145](#)
- [Activity: Database Privileged Command Successes - All Events, page E-138](#)
- [Activity: Database Privileged Command Successes - Top Users, page E-77](#)
- [Activity: Database Regular Command Failures - All Events, page E-145](#)
- [Activity: Database Regular Command Failures - Top Users, page E-145](#)
- [Activity: Database Regular Command Successes - All Events, page E-77](#)
- [Activity: Database Regular Command Successes - Top Users, page E-77](#)
- [Activity: Database User/Group Change Failures - All Events, page E-145](#)
- [Activity: Database User/Group Change Failures - Top Users, page E-145](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Database User/Group Change Successes - Top Users, page E-146](#)

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database Privileged Command Successes - Top Users

This report ranks the users by successful privileged database commands executed.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database Regular Command Successes - All Events

This report lists the event details for all successful non-privileged database command executions.

Activity: Database Regular Command Successes - Top Users

This report ranks the users by successful non-privileged database command executions.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

System: FISMA Compliance Reports

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: P2P Filesharing/Chat - Top Event Types, page E-141](#)
- [Activity: Scans - Top Destination Ports, page E-141](#)
- [Activity: Scans - Top Destinations, page E-141](#)
- [Activity: Stealth Scans - Top Sources, page E-142](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Activity: All - Top Rules Fired, page E-142](#)
- [Attacks: All - Top Sources, page E-142](#)
- [Attacks: Database Server - Top Event Types, page E-152](#)
- [Attacks: FTP Server - Top Event Types, page E-152](#)
- [Attacks: Identity Spoofing - Top Event Types, page E-153](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Attacks: Mail Server - Top Event Types, page E-153](#)
- [Attacks: Network DoS - Top Event Types, page E-142](#)
- [Attacks: RPC Services - Top Event Types, page E-153](#)
- [Attacks: Virus/Worms - Top Sources, page E-143](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Configuration Changes: Network - Top Event Types, page E-102](#)
- [Activity: All - Top Users, page E-85](#)
- [Activity: IRC - All Events, page E-143](#)
- [Attacks: All - Top Event Type Groups, page E-143](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)

- Activity: Host Registry Changes - All Events, page E-144
- Activity: Host Registry Changes - Top Host, page E-112
- Activity: Host Security Policy Changes - Top Host, page E-112
- Attacks: All - Top Destinations, page E-144
- Activity: Host User/Group Management - All Events, page E-144
- Activity: Host User/Group Management - Top hosts, page E-144
- Activity: Network Usage - Top Destination Ports, page E-144
- Attacks: Password - Top Destinations, page E-144
- Attacks: Uncommon or Anomalous Traffic - Top Event Types, page E-153
- Configuration Changes: Server - Top Event Types, page E-98
- Activity: Spyware - Top Hosts, page E-144
- Configuration Changes: Server - Top Reporting Devices, page E-103
- Activity: All Events and Netflow - Top Destination Ports, page E-134
- Activity: Host Privilege Escalation - Top Hosts, page E-145
- Activity: P2P Filesharing/Chat - Top Hosts, page E-145
- Activity: Recreational - Top Sources, page E-136
- Activity: Remote Access Login - Top User, page E-123
- Activity: Virus/Worms - Top Infected Hosts, page E-145
- Activity: Database Login Failures - All Events, page E-123
- Activity: Database Login Failures - Top Servers, page E-123
- Activity: Database Login Successes - Top Servers, page E-123
- Activity: Database Login Successes - Top Users, page E-123
- Activity: Database Object Modification Failures - All Events, page E-105
- Activity: Database Object Modification Failures - Top Users, page E-105
- Activity: Database Object Modification Successes - All Events, page E-137
- Activity: Database Object Modification Successes - Top Users, page E-105
- Activity: Database Privileged Command Failures - All Events, page E-145
- Activity: Virus: Detected - Top Users, page E-145
- Activity: Database Privileged Command Failures - Top Users, page E-145
- Activity: Virus: Infections - Top Users, page E-145
- Activity: Database Regular Command Failures - All Events, page E-145
- Activity: Database Regular Command Failures - Top Users, page E-145
- Activity: Database User/Group Change Failures - All Events, page E-145
- Activity: Database User/Group Change Failures - Top Users, page E-145
- Activity: Database User/Group Change Successes - All Events, page E-146
- Activity: Database User/Group Change Successes - Top Users, page E-146
- Resource Utilization: Concurrent Connections - Top Devices, page E-146
- Activity: Host Login Failures - All Events, page E-146

- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: CS-MARS Host Mitigation - Failure - All Events, page E-89](#)
- [Activity: CS-MARS Host Mitigation - Success - All Events, page E-89](#)
- [Activity: Host Admin Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Attacks: Password - All Events, page E-147](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)
- [Activity: CS-MARS padmin User Password Status, page E-91](#)
- [Activity: CS-MARS Successful Logins, page E-91](#)

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Activity: All - Top Rules Fired

This report ranks rules fired over the past hour by number of incidents. This provides a general feeling about the rule firing activity in the network which includes both attack and non-attack activity. This report is used by pages in the Summary tab.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Activity: All - Top Users

This report tracks the most frequent logins and other user activity by showing the most active user names.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Host User/Group Management - All Events

This report records user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Password attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that install and run on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Activity: All Events and Netflow - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Recreational - Top Sources

This report ranks the source addresses involved in recreational activities such as games, adult web sites, stock sites etc.

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: CS-MARS Host Mitigation - Failure - All Events

This report lists failed CS-MARS mitigation attempts - these can result from improper network connectivity or device access credentials.

Activity: CS-MARS Host Mitigation - Success - All Events

This report lists successful mitigations from CS-MARS.

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Attacks: Password - All Events

This report details all password attack events.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

Activity: CS-MARS pndmin User Password Status

This report details events due to CS-MARS LC 'pndmin' user account password activity such as change in password or if the password continues to remain factory default which is checked once in 24 hours

Activity: CS-MARS Successful Logins

This report details events due to CS-MARS LC successful logins

System: GLBA Compliance Reports

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)

- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: Scans - Top Destination Ports, page E-141](#)
- [Activity: Scans - Top Destinations, page E-141](#)
- [Activity: Stealth Scans - Top Sources, page E-142](#)
- [Activity: All - Top Rules Fired, page E-142](#)
- [Attacks: All - Top Sources, page E-142](#)
- [Attacks: Database Server - Top Event Types, page E-152](#)
- [Attacks: FTP Server - Top Event Types, page E-152](#)
- [Attacks: Identity Spoofing - Top Event Types, page E-153](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Attacks: Mail Server - Top Event Types, page E-153](#)
- [Attacks: Network DoS - Top Event Types, page E-142](#)
- [Attacks: RPC Services - Top Event Types, page E-153](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Configuration Changes: Network - Top Event Types, page E-102](#)
- [Configuration Issues: Network - Top Reporting Devices, page E-107](#)
- [Configuration Issues: Server - Top Reporting Devices, page E-75](#)
- [Activity: IRC - All Events, page E-143](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Attacks: All - Top Destinations, page E-144](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Attacks: Password - Top Destinations, page E-144](#)
- [Configuration Changes: Server - Top Event Types, page E-98](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Configuration Changes: Server - Top Reporting Devices, page E-103](#)
- [Activity: All Events and Netflow - Top Destination Ports, page E-134](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: P2P Filesharing/Chat - Top Hosts, page E-145](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Object Modification Failures - All Events, page E-105](#)
- [Activity: Database Object Modification Failures - Top Users, page E-105](#)
- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Activity: Database Object Modification Successes - Top Users, page E-105](#)

- [Activity: Database Privileged Command Failures - All Events, page E-145](#)
- [Activity: Database Privileged Command Failures - Top Users, page E-145](#)
- [Activity: Database Privileged Command Successes - All Events, page E-138](#)
- [Activity: Database Privileged Command Successes - Top Users, page E-77](#)
- [Activity: Database Regular Command Failures - All Events, page E-145](#)
- [Activity: Database Regular Command Failures - Top Users, page E-145](#)
- [Activity: Database Regular Command Successes - All Events, page E-77](#)
- [Activity: Database Regular Command Successes - Top Users, page E-77](#)
- [Activity: Database User/Group Change Failures - All Events, page E-145](#)
- [Activity: Database User/Group Change Failures - Top Users, page E-145](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Database User/Group Change Successes - Top Users, page E-146](#)
- [Resource Utilization: Concurrent Connections - Top Devices, page E-146](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Spyware - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Attacks: Password - All Events, page E-147](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)
- [Configuration Issues: Network - All Events, page E-107](#)
- [Configuration Issues: Server - All Events, page E-79](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Activity: All - Top Rules Fired

This report ranks rules fired over the past hour by number of incidents. This provides a general feeling about the rule firing activity in the network which includes both attack and non-attack activity. This report is used by pages in the Summary tab.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Configuration Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in network devices such as firewalls, routers and switches.

Configuration Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in servers. These are likely to be Host IDS events.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Passwords attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Activity: All Events and Netflow - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database Privileged Command Successes - Top Users

This report ranks the users by successful privileged database commands executed.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database Regular Command Successes - All Events

This report lists the event details for all successful non-privileged database command executions.

Activity: Database Regular Command Successes - Top Users

This report ranks the users by successful non-privileged database command executions.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Spyware - All Events

This event details all spyware events.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Attacks: Password - All Events

This report details all password attack events.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Configuration Issues: Network - All Events

This report lists details for events that indicate configuration error on network devices.

Configuration Issues: Server - All Events

This report lists details for all events that indicate configuration errors on hosts or host applications.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

System: HIPAA Compliance Reports

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: P2P Filesharing/Chat - Top Event Types, page E-141](#)
- [Activity: Scans - Top Destination Ports, page E-141](#)
- [Activity: Scans - Top Destinations, page E-141](#)
- [Activity: Stealth Scans - Top Sources, page E-142](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Activity: All - Top Rules Fired, page E-142](#)
- [Attacks: All - Top Sources, page E-142](#)
- [Attacks: Database Server - Top Event Types, page E-152](#)
- [Attacks: FTP Server - Top Event Types, page E-152](#)
- [Attacks: Identity Spoofing - Top Event Types, page E-153](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Attacks: Mail Server - Top Event Types, page E-153](#)
- [Attacks: Network DoS - Top Event Types, page E-142](#)
- [Attacks: RPC Services - Top Event Types, page E-153](#)
- [Attacks: Virus/Worms - Top Sources, page E-143](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Configuration Changes: Network - Top Event Types, page E-102](#)

- [Activity: All - Top Users, page E-85](#)
- [Activity: IRC - All Events, page E-143](#)
- [Attacks: All - Top Event Type Groups, page E-143](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Attacks: All - Top Destinations, page E-144](#)
- [Activity: Host User/Group Management - All Events, page E-144](#)
- [Activity: Host User/Group Management - Top hosts, page E-144](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Attacks: Password - Top Destinations, page E-144](#)
- [Attacks: Uncommon or Anomalous Traffic - Top Event Types, page E-153](#)
- [Configuration Changes: Server - Top Event Types, page E-98](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Configuration Changes: Server - Top Reporting Devices, page E-103](#)
- [Activity: All Events and Netflow - Top Destination Ports, page E-134](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: P2P Filesharing/Chat - Top Hosts, page E-145](#)
- [Activity: Recreational - Top Sources, page E-136](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Virus/Worms - Top Infected Hosts, page E-145](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Database Object Modification Failures - All Events, page E-105](#)
- [Activity: Database Object Modification Failures - Top Users, page E-105](#)
- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Activity: Database Object Modification Successes - Top Users, page E-105](#)
- [Activity: Database Privileged Command Failures - All Events, page E-145](#)
- [Activity: Virus: Detected - Top Users, page E-145](#)
- [Activity: Database Privileged Command Failures - Top Users, page E-145](#)
- [Activity: Virus: Infections - Top Users, page E-145](#)
- [Activity: Database Regular Command Failures - All Events, page E-145](#)

- [Activity: Database Regular Command Failures - Top Users, page E-145](#)
- [Activity: Database User/Group Change Failures - All Events, page E-145](#)
- [Activity: Database User/Group Change Failures - Top Users, page E-145](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Database User/Group Change Successes - Top Users, page E-146](#)
- [Resource Utilization: Concurrent Connections - Top Devices, page E-146](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: CS-MARS Host Mitigation - Failure - All Events, page E-89](#)
- [Activity: CS-MARS Host Mitigation - Success - All Events, page E-89](#)
- [Activity: Host Admin Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Attacks: Password - All Events, page E-147](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)
- [Activity: CS-MARS padmin User Password Status, page E-91](#)
- [Activity: CS-MARS Successful Logins, page E-91](#)
- [Activity: CS-MARS Login Failures, page E-91](#)

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Activity: All - Top Rules Fired

This report ranks rules fired over the past hour by number of incidents. This provides a general feeling about the rule firing activity in the network which includes both attack and non-attack activity. This report is used by pages in the Summary tab.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Activity: All - Top Users

This report tracks the most frequent logins and other user activity by showing the most active user names.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Passwords attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Activity: All Events and Netflow - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Recreational - Top Sources

This report ranks the source addresses involved in recreational activities such as games, adult web sites, stock sites etc.

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPsec).

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: CS-MARS Host Mitigation - Failure - All Events

This report lists failed CS-MARS mitigation attempts - these can result from improper network connectivity or device access credentials.

Activity: CS-MARS Host Mitigation - Success - All Events

This report lists successful mitigations from CS-MARS.

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Attacks: Password - All Events

This report details all password attack events.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

Activity: CS-MARS pndmin User Password Status

This report details events due to CS-MARS LC 'pndmin' user account password activity such as change in password or if the password continues to remain factory default which is checked once in 24 hours

Activity: CS-MARS Successful Logins

This report details events due to CS-MARS LC successful logins

Activity: CS-MARS Login Failures

This report details events due to CS-MARS LC login failures

System: Host Activity

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Object Access - All Events, page E-102](#)
- [Activity: Host Privileged Access - All Events, page E-102](#)
- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Activity: Host System Events - All Events, page E-103](#)
- [Activity: Host User/Group Management - All Events, page E-144](#)
- [Activity: Host User/Group Management - Top hosts, page E-144](#)
- [Activity: Host Process Tracking - All Events, page E-103](#)

Activity: Host Object Access - All Events

This report records all Microsoft Windows Object Access events from Windows Event Logs.

Activity: Host Privileged Access - All Events

This report records all Microsoft Windows Host Privileged Access events from Windows Event Logs.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Activity: Host System Events - All Events

This report records the Microsoft Windows system events, e.g. startup, shutdown, LSA registration, audit event discards, etc.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Host Process Tracking - All Events

This report records all Microsoft Windows Detailed Process Tracking events from Windows Event Logs.

System: Network Attacks and DoS

This category contains the following system reports:

This section contains the following topics:

- [Attacks: Network DoS - Top Event Types, page E-142](#)
- [Activity: Sudden Traffic Increase To Port - All Destinations, page E-93](#)
- [Activity: Sudden Traffic Increase To Port - All Sources, page E-93](#)
- [Activity: WLAN DoS Attacks Detected, page E-128](#)
- [Activity: WLAN Probes Detected, page E-128](#)
- [Activity: WLAN Rogue AP or Adhoc Hosts Detected, page E-128](#)

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Destinations

This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: Sudden Traffic Increase To Port - All Sources

This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.

Activity: WLAN DoS Attacks Detected

This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

Activity: WLAN Probes Detected

This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller

Activity: WLAN Rogue AP or Adhoc Hosts Detected

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller

System: New Malware Outbreak (Cisco ICS)

This category contains the following system reports:

This section contains the following topics:

- [Activity: New Malware Discovered - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Failure - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Success - All Events, page E-112](#)
- [Activity: New Malware Traffic Match - All Events, page E-113](#)
- [Activity: New Malware Traffic Match - Top Sources, page E-127](#)

Activity: New Malware Discovered - All Events

This report lists all the new virus/worm/malware outbreaks discovered by Cisco Incident Control Server.

Activity: New Malware Prevention Deployment Failure - All Events

This report lists all devices to which ACL and signature deployment attempts by a Cisco Incident Control Server, in response to a new virus/worm/malware outbreak, failed.

Activity: New Malware Prevention Deployment Success - All Events

This report lists all destinations (Cisco IOS IPS devices and IPS appliances) to which Cisco Incident Control Server has deployed new ACLs and signatures in respond to a new virus/worm/malware outbreak.

Activity: New Malware Traffic Match - All Events

This report details the traffic sources and the enforcing devices that match the ACLs and signatures deployed by the Cisco Incident Control Server in response to a newly discovered malware outbreak.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

System: Operational Issue

This category contains the following system reports:

This section contains the following topics:

- [Operational Issues: Network - Top Reporting Devices, page E-143](#)
- [Operational Issues: Server - Top Reporting Devices, page E-143](#)
- [Resource Utilization: Errors: Inbound - Top Interfaces, page E-146](#)
- [Resource Utilization: Errors: Outbound - Top Interfaces, page E-146](#)
- [Activity: Inactive Reporting Device - Top Devices, page E-95](#)
- [Operational Issues: Network - All Events, page E-147](#)
- [Operational Issues: Server - All Events, page E-148](#)
- [Connectivity Issue: IOS IPS DTM - All Events, page E-96](#)
- [Resource Utilization: CS-MARS - All Events, page E-96](#)
- [Activity: CS-MARS Failure Saving Certificates/Fingerprints, page E-96](#)
- [Activity: CS-MARS Device Connectivity Errors, page E-96](#)
- [Activity: CS-MARS IPS Signature Update Failure - All Events, page E-131](#)
- [Activity: CS-MARS LC-GC Communication Failures, page E-96](#)

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Operational Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate operational issues with servers.

Resource Utilization: Errors: Inbound - Top Interfaces

This report ranks by error rate on the inbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Errors: Outbound - Top Interfaces

This report ranks by error rate on the outbound interfaces of the devices managed by PN-MARS.

Activity: Inactive Reporting Device - Top Devices

This report lists devices that are configured to be reporting to CS-MARS but haven't reported any event in the last hour.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

Operational Issues: Server - All Events

This report lists details about events that indicate operational errors on hosts or host applications.

Connectivity Issue: IOS IPS DTM - All Events

This report lists connectivity issues between CS-MARS and IOS IPS devices. Connectivity issues may prevent CS-MARS from turning on ACTIVE signatures on IOS IPS.

Resource Utilization: CS-MARS - All Events

This report lists event details for all events related to CS-MARS resource utilization, e.g. database partitions, etc.

Activity: CS-MARS Failure Saving Certificates/Fingerprints

This report lists event details due to CS-MARS failure to save new or changed SSL certificates or SSH Key Fingerprints based on explicit user action or automatic accept due to SSL/SSH Settings.

Activity: CS-MARS Device Connectivity Errors

This report lists event details of CS-MARS device connectivity errors due to various reasons (e.g. conflicting SSL certificates or SSH key fingerprints, network timeout etc.). This includes both transient and persisting errors.

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

Activity: CS-MARS LC-GC Communication Failures

This reports lists event details over the past hour due to all communication failures between CS-MARS Local Controller with its Global Controller for various reasons such as connectivity issues, certificate mismatch or incompatible software or data versions

System: PCI DSS01: Install, Maintain FW, Protect Cardholder Data

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Destination Ports, page E-102](#)
- [Activity: P2P Filesharing/Chat - Top Event Types, page E-141](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Configuration Changes: Network - Top Event Types, page E-102](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Configuration Changes: Server - Top Event Types, page E-98](#)
- [Configuration Changes: Server - Top Reporting Devices, page E-103](#)

- [Activity: All Sessions - Top Destination Ports by Bytes, page E-134](#)
- [Activity: P2P Filesharing/Chat - Top Hosts, page E-145](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)
- [Configuration Changes: Network - All Events, page E-147](#)
- [Configuration Changes: Server - All Events, page E-98](#)
- [Activity: Security Posture: Healthy - Top Users, page E-149](#)
- [Activity: Security Posture: NAC - Top NADs, page E-149](#)
- [Activity: Security Posture: NAC - Top Tokens, page E-149](#)
- [Activity: Security Posture: NAC L2IP - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Audit Server Issues - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC L2 802.1x - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top NADs, page E-150](#)
- [Activity: Security Posture: NAC Status Query Failure - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: Security Posture: NAC - Top NADs and Tokens, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Tokens, page E-151](#)
- [Activity: Security Posture: NAC End Host Details - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top NADs, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Hosts, page E-152](#)
- [Activity: Security Posture: NAC Agentless - Top NADs, page E-152](#)

Activity: All - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Configuration Changes: Server - Top Event Types

This report summarizes configuration changes to servers over the past hour.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Activity: All Sessions - Top Destination Ports by Bytes

This report ranks all destination ports by bytes transferred.

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Configuration Changes: Server - All Events

This event details all configuration changes on hosts (reported by OS or Host IDS agents)

Activity: Security Posture: Healthy - Top Users

This report lists the users in a HEALTHY Security Posture State. A Healthy security posture implies that the posture of the host is up to date, policy compliant and does not need attention.

Activity: Security Posture: NAC - Top NADs

This report ranks the network access devices (NADs) handling Network Admission Control transactions.

Activity: Security Posture: NAC - Top Tokens

This report shows the network wide distribution of NAC tokens. The possible token values are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC L2IP - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IP method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Audit Server Issues - All Events

This report ranks the end hosts for which the AAA server is having an issue with obtaining the right security posture token from the audit server. These hosts do not have the Cisco Trust Agent (CTA) running and they depend on an Audit Server for obtaining the proper Security Posture Token.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC L2 802.1x - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IEEE 802.1x method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Static Auth - Top Hosts

This report captures the hosts that are configured as static exceptions on the Network Access Device (NAD). For these hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Static Auth - Top NADs

This report captures the Network Access Device (NAD) that are permitting end hosts into the network as static exceptions. For these end hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: Security Posture: NAC - Top NADs and Tokens

This report displays the Network Access Devices (NADs) handling Network Admission Control transactions along with the tokens assigned by each of them.

Activity: Security Posture: NAC Agentless - Top Tokens

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC End Host Details - All Events

This report details all the NAC related messages from the Network Access Devices (NAD) and AAA servers. Choose a source IP address or user to see the messages for one end host.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Security Posture: NAC Agentless - Top Hosts

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Agentless - Top NADs

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

System: PCI DSS02: Do Not Use Default PWD & Security Parameters

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Destination Ports, page E-102](#)
- [Activity: P2P Filesharing/Chat - Top Event Types, page E-141](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Configuration Changes: Network - Top Event Types, page E-102](#)
- [Activity: Host Object Access - All Events, page E-102](#)
- [Activity: Host Privileged Access - All Events, page E-102](#)
- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Activity: Host System Events - All Events, page E-103](#)
- [Activity: Host User/Group Management - All Events, page E-144](#)
- [Activity: Host User/Group Management - Top hosts, page E-144](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Configuration Changes: Server - Top Reporting Devices, page E-103](#)
- [Activity: P2P Filesharing/Chat - Top Hosts, page E-145](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)
- [Activity: P2P Filesharing/Chat - All Events, page E-136](#)

- [Configuration Changes: Network - All Events, page E-147](#)
- [Activity: Host Process Tracking - All Events, page E-103](#)

Activity: All - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Configuration Changes: Network - Top Event Types

This report summarizes configuration changes to network devices such as firewalls, routers and switches over the past hour.

Activity: Host Object Access - All Events

This report records all Microsoft Windows Object Access events from Windows Event Logs.

Activity: Host Privileged Access - All Events

This report records all Microsoft Windows Host Privileged Access events from Windows Event Logs.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Activity: Host System Events - All Events

This report records the Microsoft Windows system events, e.g. startup, shutdown, LSA registration, audit event discards, etc.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Configuration Changes: Server - Top Reporting Devices

This report summarizes the configuration changes per server over the past hour.

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: P2P Filesharing/Chat - All Events

This event details all P2P File sharing or Chat event details.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Activity: Host Process Tracking - All Events

This report records all Microsoft Windows Detailed Process Tracking events from Windows Event Logs.

System: PCI DSS03: Protect Store Cardholder Data

This category contains the following system reports:

This section contains the following topics:

- [Attacks: SNMP - Top Event Types, page E-153](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Database Object Modification Failures - All Events, page E-105](#)
- [Activity: Database Object Modification Failures - Top Users, page E-105](#)
- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Activity: Database Object Modification Successes - Top Users, page E-105](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top NADs, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)

Attacks: SNMP - Top Event Types

This report ranks SNMP based attacks over the past hour.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Database Object Modification Failures - All Events

This report lists the event details for all failed database object modification attempts.

Activity: Database Object Modification Failures - Top Users

This report ranks the users by the number of failed database object modification attempts.

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Object Modification Successes - Top Users

This report ranks the number of users by the number of successful database object modifications.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

System: PCI DSS04: Encrypt Transmission of Cardholder Data

This category contains the following system reports:

This section contains the following topics:

- [Configuration Issues: Network - Top Reporting Devices, page E-107](#)
- [Operational Issues: Network - Top Reporting Devices, page E-143](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Configuration Issues: Network - All Events, page E-107](#)
- [Operational Issues: Network - All Events, page E-147](#)

Configuration Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate certain configuration related problems in network devices such as firewalls, routers and switches.

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPsec).

Activity: Remote Access Login - All Events

This report details of remote access login events (IPsec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Configuration Issues: Network - All Events

This report lists details for events that indicate configuration error on network devices.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

System: PCI DSS05: Use and Regularly Update Anti-Virus Software

This category contains the following system reports:

This section contains the following topics:

- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Activity: Security Posture: Healthy - Top Users, page E-149](#)
- [Activity: Security Posture: NAC - Top NADs, page E-149](#)
- [Activity: Security Posture: NAC - Top Tokens, page E-149](#)
- [Activity: Security Posture: NAC L2IP - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Audit Server Issues - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC L2 802.1x - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top NADs, page E-150](#)
- [Activity: Security Posture: NAC Status Query Failure - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: Security Posture: NAC - Top NADs and Tokens, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Tokens, page E-151](#)
- [Activity: Security Posture: NAC End Host Details - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top NADs, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Hosts, page E-152](#)
- [Activity: Security Posture: NAC Agentless - Top NADs, page E-152](#)

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Activity: Security Posture: Healthy - Top Users

This report lists the users in a HEALTHY Security Posture State. A Healthy security posture implies that the posture of the host is up to date, policy compliant and does not need attention.

Activity: Security Posture: NAC - Top NADs

This report ranks the network access devices (NADs) handling Network Admission Control transactions.

Activity: Security Posture: NAC - Top Tokens

This report shows the network wide distribution of NAC tokens. The possible token values are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC L2IP - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IP method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Audit Server Issues - All Events

This report ranks the end hosts for which the AAA server is having an issue with obtaining the right security posture token from the audit server. These hosts do not have the Cisco Trust Agent (CTA) running and they depend on an Audit Server for obtaining the proper Security Posture Token.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC L2 802.1x - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IEEE 802.1x method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Static Auth - Top Hosts

This report captures the hosts that are configured as static exceptions on the Network Access Device (NAD). For these hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Static Auth - Top NADs

This report captures the Network Access Device (NAD) that are permitting end hosts into the network as static exceptions. For these end hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: Security Posture: NAC - Top NADs and Tokens

This report displays the Network Access Devices (NADs) handling Network Admission Control transactions along with the tokens assigned by each of them.

Activity: Security Posture: NAC Agentless - Top Tokens

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC End Host Details - All Events

This report details all the NAC related messages from the Network Access Devices (NAD) and AAA servers. Choose a source IP address or user to see the messages for one end host.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Security Posture: NAC Agentless - Top Hosts

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Agentless - Top NADs

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

System: PCI DSS06: Develop, Maintain Secured System/Application

This category contains the following system reports:

This section contains the following topics:

- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Activity: Host Registry Changes - Top Host, page E-112](#)
- [Activity: Host Security Policy Changes - Top Host, page E-112](#)
- [Activity: New Malware Discovered - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Failure - All Events, page E-112](#)
- [Activity: New Malware Prevention Deployment Success - All Events, page E-112](#)
- [Activity: New Malware Traffic Match - All Events, page E-113](#)
- [Activity: New Malware Traffic Match - Top Sources, page E-127](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Security Posture: Healthy - Top Users, page E-149](#)
- [Activity: AAA Based Access - All Events, page E-124](#)
- [Activity: Security Posture: NAC - Top NADs, page E-149](#)
- [Activity: Security Posture: NAC - Top Tokens, page E-149](#)
- [Activity: Security Posture: NAC L2IP - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Audit Server Issues - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)

- [Activity: Security Posture: NAC L2 802.1x - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top NADs, page E-150](#)
- [Activity: Security Posture: NAC Status Query Failure - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: Security Posture: NAC - Top NADs and Tokens, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Tokens, page E-151](#)
- [Activity: Security Posture: NAC End Host Details - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top NADs, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Hosts, page E-152](#)
- [Activity: Security Posture: NAC Agentless - Top NADs, page E-152](#)

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Activity: Host Registry Changes - Top Host

This report ranks hosts by the number of Microsoft Windows registry changes reported.

Activity: Host Security Policy Changes - Top Host

This report ranks hosts by the number of security policy changes on that host.

Activity: New Malware Discovered - All Events

This report lists all the new virus/worm/malware outbreaks discovered by Cisco Incident Control Server.

Activity: New Malware Prevention Deployment Failure - All Events

This report lists all devices to which ACL and signature deployment attempts by a Cisco Incident Control Server, in response to a new virus/worm/malware outbreak, failed.

Activity: New Malware Prevention Deployment Success - All Events

This report lists all destinations (Cisco IOS IPS devices and IPS appliances) to which Cisco Incident Control Server has deployed new ACLs and signatures in respond to a new virus/worm/malware outbreak.

Activity: New Malware Traffic Match - All Events

This report details the traffic sources and the enforcing devices that match the ACLs and signatures deployed by the Cisco Incident Control Server in response to a newly discovered malware outbreak.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Security Posture: Healthy - Top Users

This report lists the users in a HEALTHY Security Posture State. A Healthy security posture implies that the posture of the host is up to date, policy compliant and does not need attention.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Security Posture: NAC - Top NADs

This report ranks the network access devices (NADs) handling Network Admission Control transactions.

Activity: Security Posture: NAC - Top Tokens

This report shows the network wide distribution of NAC tokens. The possible token values are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC L2IP - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IP method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Audit Server Issues - All Events

This report ranks the end hosts for which the AAA server is having an issue with obtaining the right security posture token from the audit server. These hosts do not have the Cisco Trust Agent (CTA) running and they depend on an Audit Server for obtaining the proper Security Posture Token.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC L2 802.1x - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IEEE 802.1x method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Static Auth - Top Hosts

This report captures the hosts that are configured as static exceptions on the Network Access Device (NAD). For these hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Static Auth - Top NADs

This report captures the Network Access Device (NAD) that are permitting end hosts into the network as static exceptions. For these end hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: Security Posture: NAC - Top NADs and Tokens

This report displays the Network Access Devices (NADs) handling Network Admission Control transactions along with the tokens assigned by each of them.

Activity: Security Posture: NAC Agentless - Top Tokens

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC End Host Details - All Events

This report details all the NAC related messages from the Network Access Devices (NAD) and AAA servers. Choose a source IP address or user to see the messages for one end host.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Security Posture: NAC Agentless - Top Hosts

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Agentless - Top NADs

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

System: PCI DSS07: Restrict Access to Cardholder Data

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Attacks: Password: Locked Accounts - All Events, page E-124](#)
- [Attacks: Password: Restricted Times - All Events, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: PCI DSS08: Assign Unique ID to Person with Comp Access

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)

- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Attacks: Password: Locked Accounts - All Events, page E-124](#)
- [Attacks: Password: Restricted Times - All Events, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)
- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: PCI DSS09: Restrict Physical Access to Cardholder Data

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

System: PCI DSS10: Track, Monitor All Network Access, Card Data

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Login Failures - Top Destinations, page E-144](#)
- [Activity: Host Login Failures - Top Users, page E-144](#)
- [Activity: Host Login Success - Top Host, page E-123](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Remote Access Login - Top User, page E-123](#)
- [Activity: Database Login Failures - All Events, page E-123](#)
- [Activity: Database Login Failures - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Servers, page E-123](#)
- [Activity: Database Login Successes - Top Users, page E-123](#)
- [Activity: Host Login Failures - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Privilege Escalation - All Events, page E-147](#)
- [Activity: Remote Access Login - All Events, page E-147](#)
- [Activity: Remote Access Login Failures - All Events, page E-124](#)
- [Activity: AAA Based Access Failure - All Events, page E-124](#)
- [Activity: Accounts Locked - All Events, page E-124](#)
- [Activity: Accounts Locked - Top Hosts, page E-124](#)
- [Attacks: Password: Locked Accounts - All Events, page E-124](#)
- [Attacks: Password: Restricted Times - All Events, page E-124](#)
- [Activity: AAA Based Access - All Events, page E-124](#)

- [Activity: Database Login Failures - Top Users, page E-125](#)
- [Activity: Database Login Successes - All Events, page E-148](#)
- [Activity: WLAN DoS Attacks Detected, page E-128](#)
- [Activity: WLAN Probes Detected, page E-128](#)
- [Activity: WLAN Rogue AP or Adhoc Hosts Detected, page E-128](#)

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Login Success - Top Host

This report ranks hosts by successful logins.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - Top User

This report ranks users by remote access logins (PPP, L2TP, PPTP, IPSec).

Activity: Database Login Failures - All Events

This report lists the event details for all database login failure events.

Activity: Database Login Failures - Top Servers

This report ranks the database servers by the number of login failures.

Activity: Database Login Successes - Top Servers

This report ranks the database server hosts by the number of successful logins.

Activity: Database Login Successes - Top Users

This report ranks the database users by the number of successful logins.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Remote Access Login Failures - All Events

This event details all failed remote access login event details.

Activity: AAA Based Access Failure - All Events

This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco NAC use AAA servers for access control.

Activity: Accounts Locked - All Events

This report details events that indicate locked computer accounts because of excessive login failures.

Activity: Accounts Locked - Top Hosts

This report ranks the hosts by the accounts locked.

Attacks: Password: Locked Accounts - All Events

This report details password attacks on locked/disabled/expired accounts.

Attacks: Password: Restricted Times - All Events

This report details all events that indicate login failures at restricted times - the hosts are specifically configured to disallow access at these hours.

Activity: AAA Based Access - All Events

This report details AAA based access (e.g. to the network or to specific devices).

Activity: Database Login Failures - Top Users

This report ranks the users by the number of login failures.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: WLAN DoS Attacks Detected

This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

Activity: WLAN Probes Detected

This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller

Activity: WLAN Rogue AP or Adhoc Hosts Detected

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller

System: PCI DSS11: Regularly Test Security Systems and Processes

This category contains the following system reports:

This section contains the following topics:

- [Activity: Attacks Seen - Top Reporting Devices, page E-141](#)
- [Activity: Backdoor - Top Event Types, page E-129](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Activity: Backdoor - Top Destinations, page E-129](#)
- [Activity: Attacks Seen - Top Event Types, page E-130](#)
- [Activity: Backdoor - Top Hosts, page E-130](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Virus/Worms - Top Infected Hosts, page E-145](#)
- [Activity: Virus: Detected - Top Users, page E-145](#)
- [Activity: Virus: Infections - Top Users, page E-145](#)
- [Activity: New Malware Traffic Match - Top Sources, page E-127](#)

- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)
- [Activity: CS-MARS IPS Signature Update Success - All Events, page E-130](#)
- [Activity: CS-MARS IPS Signature Update Failure - All Events, page E-131](#)
- [Activity: WLAN DoS Attacks Detected, page E-128](#)
- [Activity: WLAN Probes Detected, page E-128](#)
- [Activity: WLAN Rogue AP or Adhoc Hosts Detected, page E-128](#)

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Attacks Seen - Top Event Types

This report ranks the top attack event types.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: New Malware Traffic Match - Top Sources

This report lists the top sources that match the ACLs or signatures dynamically deployed by Cisco Incident Control Server in response to a new virus/worm/malware outbreak. This indicates that these sources are likely infected.

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

Activity: CS-MARS IPS Signature Update Success - All Events

This report lists event details of all success events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate success steps in auto update or complete/partial success of updating the CS-MARS database with the downloaded IPS signature package.

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

Activity: WLAN DoS Attacks Detected

This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller

Activity: WLAN Probes Detected

This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller

Activity: WLAN Rogue AP or Adhoc Hosts Detected

This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller

System: PCI DSS12: Maintain InfoSec Policy for All Personnel

This category contains the following system reports:

This section contains the following topics:

- [Activity: Attacks Seen - Top Reporting Devices, page E-141](#)
- [Activity: Backdoor - Top Event Types, page E-129](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Activity: Virus/Worms - Top Event Types, page E-142](#)
- [Activity: Backdoor - Top Destinations, page E-129](#)
- [Activity: Attacks Seen - Top Event Types, page E-130](#)

- [Activity: Backdoor - Top Hosts, page E-130](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Activity: Host Privilege Escalation - Top Hosts, page E-145](#)
- [Activity: Virus/Worms - Top Infected Hosts, page E-145](#)
- [Activity: Virus: Detected - Top Users, page E-145](#)
- [Activity: Virus: Infections - Top Users, page E-145](#)
- [Activity: Attacks Prevented by Cisco IPS - All Events, page E-130](#)
- [Activity: Attacks Prevented by Cisco IPS - Top Event Types, page E-130](#)
- [Activity: CS-MARS IPS Signature Update Success - All Events, page E-130](#)
- [Activity: CS-MARS IPS Signature Update Failure - All Events, page E-131](#)

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Activity: Backdoor - Top Event Types

This report ranks the events that detect some form of backdoor activity. A backdoor may be created by an attacker on a compromised host. A backdoor event can be either an attempt to connect to a backdoor or a response from a server running a backdoor.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Activity: Backdoor - Top Destinations

This report ranks the hosts that respond to backdoor connection attempts.

Activity: Attacks Seen - Top Event Types

This report ranks the top attack event types.

Activity: Backdoor - Top Hosts

This report ranks the hosts that respond to backdoor connection attempts. This means that the hosts are likely infected and running backdoors.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: Attacks Prevented by Cisco IPS - All Events

This report contains all Cisco IPS events for which attacks (or attempts) were prevented.

Activity: Attacks Prevented by Cisco IPS - Top Event Types

This report ranks the top Cisco IPS event types for which attacks (or attempts) were prevented

Activity: CS-MARS IPS Signature Update Success - All Events

This report lists event details of all success events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate success steps in auto update or complete/partial success of updating the CS-MARS database with the downloaded IPS signature package.

Activity: CS-MARS IPS Signature Update Failure - All Events

This report lists event details of all failure events that occur during auto update of an IPS signature package in CS-MARS. The included events indicate intermediate errors such as failing to add or update one or more CS-MARS event types corresponding to some IPS signature as well as complete failure to download/parse/update (or partial update) the CS-MARS database with the signature package.

System: Reconnaissance

This category contains the following system reports:

This section contains the following topics:

- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: Scans - Top Destination Ports, page E-141](#)
- [Activity: Scans - Top Destinations, page E-141](#)
- [Activity: Scans - Top Sources, page E-132](#)
- [Activity: Stealth Scans - Top Sources, page E-142](#)
- [Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events, page E-132](#)

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Sources

This report ranks an attack sources by the total number of events detecting scanning activity for certain services. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Attacks: ASA Botnet Traffic Filter: Malicious Traff - All Events

This report details all events related to traffic originating from black/grey sites/IPs, as reported by ASA Botnet Traffic Filter.

System: Resource Issue

This category contains the following system reports:

This section contains the following topics:

- [Resource Issues: Network - Top Reporting Devices, page E-143](#)
- [Resource Issues: Server - Top Reporting Devices, page E-143](#)
- [Resource Issues: Network - All Events, page E-132](#)
- [Resource Issues: Server - All Events, page E-133](#)
- [Resource Issues: IOS IPS DTM - Top Devices, page E-133](#)
- [Resource Issues: IOS IPS DTM - All Events, page E-133](#)
- [Resource Issues: CS-MARS - All Events, page E-133](#)

Resource Issues: Network - Top Reporting Devices

This report summarizes the events that represent resource issues with network devices such as firewalls, routers and switches.

Resource Issues: Server - Top Reporting Devices

This report summarizes the events that represent resource issues with servers. These are likely to be Host IDS events.

Resource Issues: Network - All Events

This report lists event details for all events related to resource issues on network devices such as IDS, routers, firewalls etc.

Resource Issues: Server - All Events

This report lists event details for all resource issues on hosts. These are reported by Host IDS or Operating System logs.

Resource Issues: IOS IPS DTM - Top Devices

This report lists IOS IPS routers that are running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to IOS IPS devices.

Resource Issues: IOS IPS DTM - All Events

This report lists event details that indicate certain IOS IPS routers running low on memory for CS-MARS Distributed Threat Mitigation (DTM). Because of low memory, CS-MARS may not be able to download and activate the complete set of ACTIVE IPS signatures to those IOS IPS devices.

Resource Issues: CS-MARS - All Events

This report lists event details for all events related to resource issues with the CS-MARS device, e.g. dropped events or netflow, etc.

System: Resource Usage

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Destinations, page E-134](#)
- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: All - Top Sources, page E-134](#)
- [Activity: All - Top Reporting Device Types, page E-143](#)
- [Activity: Network Usage - Top Destination Ports, page E-144](#)
- [Activity: All Events and Netflow - Top Destination Ports, page E-134](#)
- [Activity: All Sessions - Top Destination Ports by Bytes, page E-134](#)
- [Activity: All Sessions - Top Destinations by Bytes, page E-134](#)
- [Resource Utilization: Bandwidth: Inbound - Top Interfaces, page E-146](#)
- [Resource Utilization: CPU - Top Devices, page E-146](#)
- [Resource Utilization: Bandwidth: Outbound - Top Interfaces, page E-146](#)
- [Resource Utilization: Concurrent Connections - Top Devices, page E-146](#)
- [Resource Utilization: Memory - Top Devices, page E-146](#)
- [Activity: Network Usage - Top Destination Ports By Bytes, page E-147](#)

Activity: All - Top Destinations

This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: All - Top Sources

This report ranks the session sources of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Activity: All Events and Netflow - Top Destination Ports

This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.

Activity: All Sessions - Top Destination Ports by Bytes

This report ranks all destination ports by bytes transferred.

Activity: All Sessions - Top Destinations by Bytes

This report ranks all destinations by bytes transferred.

Resource Utilization: Bandwidth: Inbound - Top Interfaces

This report ranks the inbound bandwidth utilization of the interfaces on the devices managed by PN-MARS.

Resource Utilization: CPU - Top Devices

This report ranks the CPU utilization of the devices managed by PN-MARS.

Resource Utilization: Bandwidth: Outbound - Top Interfaces

This report ranks the outbound bandwidth utilization of interfaces on devices managed by Pn-MARS.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Resource Utilization: Memory - Top Devices

This report ranks the memory utilization of the devices managed by PN-MARS.

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

System: Restricted Network Traffic

This category contains the following system reports:

This section contains the following topics:

- [Activity: P2P Filesharing/Chat - Top Event Types, page E-141](#)
- [Activity: IRC - All Events, page E-143](#)
- [Activity: Spyware - Top Hosts, page E-144](#)
- [Activity: P2P Filesharing/Chat - Top Hosts, page E-145](#)
- [Activity: Recreational - Top Sources, page E-136](#)
- [Activity: Recreational - All Events, page E-146](#)
- [Activity: Spyware - All Events, page E-147](#)
- [Activity: P2P Filesharing/Chat - All Events, page E-136](#)
- [Activity: Uncommon or Anomalous Traffic - All Events, page E-136](#)

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Recreational - Top Sources

This report ranks the source addresses involved in recreational activities such as games, adult web sites, stock sites etc.

Activity: Recreational - All Events

This event details all users involved in recreational activities such as games, specific web sites such as gambling etc.

Activity: Spyware - All Events

This event details all spyware events.

Activity: P2P Filesharing/Chat - All Events

This event details all P2P File sharing or Chat event details.

Activity: Uncommon or Anomalous Traffic - All Events

This report details uncommon or anomalous traffic such as unused TCP options, uncommon ICMP traffic, non-standard traffic on standard port, tunneled traffic etc.

System: SOX 302(a)(4)(A)

This category contains the following system reports:

This section contains the following topics:

- [Activity: Database Object Modification Successes - All Events, page E-137](#)
- [Activity: Database Privileged Command Successes - All Events, page E-138](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Admin Login Success - All Events, page E-147](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: Database Login Successes - All Events, page E-148](#)

Activity: Database Object Modification Successes - All Events

This report lists the event details for all successful database object modification attempts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: SOX 302(a)(4)(D)

This category contains the following system reports:

This section contains the following topics:

- [Activity: Host Registry Changes - All Events, page E-144](#)
- [Activity: Host User/Group Management - All Events, page E-144](#)
- [Activity: Database Privileged Command Successes - All Events, page E-138](#)
- [Activity: Database User/Group Change Successes - All Events, page E-146](#)
- [Activity: Host Login Success - All Events, page E-147](#)
- [Activity: Host Admin Login Success - All Events, page E-147](#)
- [Activity: Host Security Policy Changes - All Events, page E-148](#)
- [Activity: Database Login Successes - All Events, page E-148](#)

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Database Privileged Command Successes - All Events

This report lists the event details for all successful privileged database commands executed.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

System: SOX Compliance Reports

This category contains the following system reports:

This section contains the following topics:

- [Activity: All - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Prevented - Top Reporting Devices, page E-141](#)
- [Activity: Attacks Seen - Top Reporting Devices, page E-141](#)
- [Activity: Denies - Top Destination Ports, page E-141](#)
- [Activity: Denies - Top Destinations, page E-141](#)
- [Activity: Denies - Top Sources, page E-141](#)
- [Activity: IDS Evasion - Top Event Types, page E-152](#)

- Activity: P2P Filesharing/Chat - Top Event Types, page E-141
- Activity: Scans - Top Destination Ports, page E-141
- Activity: Scans - Top Destinations, page E-141
- Activity: Stealth Scans - Top Sources, page E-142
- Activity: Virus/Worms - Top Event Types, page E-142
- Activity: All - Top Rules Fired, page E-142
- Attacks: All - Top Sources, page E-142
- Attacks: Database Server - Top Event Types, page E-152
- Attacks: FTP Server - Top Event Types, page E-152
- Attacks: Identity Spoofing - Top Event Types, page E-153
- Attacks: Login Services - Top Event Types, page E-153
- Attacks: Mail Server - Top Event Types, page E-153
- Attacks: Network DoS - Top Event Types, page E-142
- Attacks: RPC Services - Top Event Types, page E-153
- Attacks: Virus/Worms - Top Sources, page E-143
- Attacks: Web Server/App - Top Event Types, page E-153
- Operational Issues: Network - Top Reporting Devices, page E-143
- Operational Issues: Server - Top Reporting Devices, page E-143
- Resource Issues: Network - Top Reporting Devices, page E-143
- Resource Issues: Server - Top Reporting Devices, page E-143
- Activity: IRC - All Events, page E-143
- Attacks: All - Top Event Type Groups, page E-143
- Activity: All - Top Reporting Device Types, page E-143
- Activity: Host Login Failures - Top Destinations, page E-144
- Activity: Host Login Failures - Top Users, page E-144
- Activity: Host Registry Changes - All Events, page E-144
- Attacks: All - Top Destinations, page E-144
- Activity: Host User/Group Management - All Events, page E-144
- Activity: Host User/Group Management - Top hosts, page E-144
- Activity: Network Usage - Top Destination Ports, page E-144
- Attacks: Password - Top Destinations, page E-144
- Attacks: Uncommon or Anomalous Traffic - Top Event Types, page E-153
- Activity: Spyware - Top Hosts, page E-144
- Activity: Host Privilege Escalation - Top Hosts, page E-145
- Activity: P2P Filesharing/Chat - Top Hosts, page E-145
- Activity: Virus/Worms - Top Infected Hosts, page E-145
- Activity: Database Privileged Command Failures - All Events, page E-145
- Activity: Virus: Detected - Top Users, page E-145

- Activity: Database Privileged Command Failures - Top Users, page E-145
- Activity: Virus: Infections - Top Users, page E-145
- Activity: Database Regular Command Failures - All Events, page E-145
- Activity: Database Regular Command Failures - Top Users, page E-145
- Activity: Database User/Group Change Failures - All Events, page E-145
- Activity: Database User/Group Change Failures - Top Users, page E-145
- Activity: Database User/Group Change Successes - All Events, page E-146
- Activity: Database User/Group Change Successes - Top Users, page E-146
- Activity: Recreational - All Events, page E-146
- Resource Utilization: Bandwidth: Inbound - Top Interfaces, page E-146
- Resource Utilization: CPU - Top Devices, page E-146
- Resource Utilization: Bandwidth: Outbound - Top Interfaces, page E-146
- Resource Utilization: Concurrent Connections - Top Devices, page E-146
- Resource Utilization: Errors: Inbound - Top Interfaces, page E-146
- Resource Utilization: Errors: Outbound - Top Interfaces, page E-146
- Resource Utilization: Memory - Top Devices, page E-146
- Activity: Host Login Failures - All Events, page E-146
- Activity: Spyware - All Events, page E-147
- Activity: Host Login Success - All Events, page E-147
- Activity: Host Admin Login Success - All Events, page E-147
- Activity: Host Privilege Escalation - All Events, page E-147
- Activity: Network Usage - Top Destination Ports By Bytes, page E-147
- Activity: Remote Access Login - All Events, page E-147
- Activity: Vulnerable Host Found via VA Scanner, page E-149
- Activity: Vulnerable Host Found, page E-149
- Attacks: Password - All Events, page E-147
- Configuration Changes: Network - All Events, page E-147
- Operational Issues: Network - All Events, page E-147
- Operational Issues: Server - All Events, page E-148
- Activity: Host Security Policy Changes - All Events, page E-148
- Activity: Database Login Successes - All Events, page E-148
- Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150
- Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150
- Activity: Security Posture: NAC Status Query Failure - Top Hosts, page E-150
- Activity: Security Posture: Not Healthy - All Events, page E-151

Activity: All - Top Reporting Devices

This report ranks security devices by the total number of events reported by each device. This report is used by pages in the Summary tab.

Activity: Attacks Prevented - Top Reporting Devices

This report ranks security devices by the number of attacks prevented.

Activity: Attacks Seen - Top Reporting Devices

This report ranks security devices by the number of attack events logged. The security devices can be firewalls, NIDS and HIDS.

Activity: Denies - Top Destination Ports

This report ranks the destination ports to which attacks have been targetted but denied.

Activity: Denies - Top Destinations

This report ranks the destination hosts to which attacks have been targeted but denied.

Activity: Denies - Top Sources

This report ranks attack sources by the number of denied connection attempts.

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Activity: P2P Filesharing/Chat - Top Event Types

This event ranks events detecting person-to-person file sharing protocol and chat protocol activity. File sharing protocols such as KaZaa, Napster, EDonkey and chat protocols such as IRC, Hotline and instant messaging protocols may not be suitable in business environments.

Activity: Scans - Top Destination Ports

This report ranks destination ports by the total number of events detecting scanning activity for that port. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Scans - Top Destinations

This report ranks hosts by the total number of events detecting scanning activity directed to that host. Scans involve activities such as searching for alive hosts, open services on such hosts and detecting host configuration and application settings.

Activity: Stealth Scans - Top Sources

This report ranks attackers by the amount of stealth scanning activity. Such activities include sending crafted packets to detect host operating systems and other vulnerabilities. Vulnerability scanners may generate such events.

Activity: Virus/Worms - Top Event Types

This report ranks the events that detect virus or worm activity in the network.

Activity: All - Top Rules Fired

This report ranks rules fired over the past hour by number of incidents. This provides a general feeling about the rule firing activity in the network which includes both attack and non-attack activity. This report is used by pages in the Summary tab.

Attacks: All - Top Sources

This report ranks the sources of attack events seen by MARS over the past hour.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: Network DoS - Top Event Types

This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: Virus/Worms - Top Sources

This report ranks addresses that are the source of virus/worm propagation attempts.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Operational Issues: Network - Top Reporting Devices

This report summarizes the events that may indicate operational issues with network devices such as routers, firewalls and Network IDS systems.

Operational Issues: Server - Top Reporting Devices

This report summarizes the events that may indicate operational issues with servers.

Resource Issues: Network - Top Reporting Devices

This report summarizes the events that represent resource issues with network devices such as firewalls, routers and switches.

Resource Issues: Server - Top Reporting Devices

This report summarizes the events that represent resource issues with servers. These are likely to be Host IDS events.

Activity: IRC - All Events

This report lists all IRC activities. Typically, worms deposit executables on infected hosts that initiate IRC connections.

Attacks: All - Top Event Type Groups

This report ranks event type groups that appear in fired correlation rules. The event type groups give a general feeling about the network activity classified as part of an attack by MARS.

Activity: All - Top Reporting Device Types

This report ranks security device types by the number events reported by devices of each particular type.

Activity: Host Login Failures - Top Destinations

This report ranks hosts by the number of logon failures recorded.

Activity: Host Login Failures - Top Users

This report ranks host users by failed login attempts.

Activity: Host Registry Changes - All Events

This report records the events signalling Microsoft Windows registry changes.

Attacks: All - Top Destinations

This report ranks hosts by the number of attacks targetted at each host.

Activity: Host User/Group Management - All Events

This report recordss user group management events reported by hosts.

Activity: Host User/Group Management - Top hosts

This report ranks hosts by user group management events reported.

Activity: Network Usage - Top Destination Ports

This report ranks destination ports by number of network sessions. This report requires that the syslog level of routers or firewalls be set to high to be able to capture session events. This report provides a general usage pattern of the network.

Attacks: Password - Top Destinations

This report ranks hosts by the number of password attacks attempted on them. Passwords attacks include attempts to (a) capture passwords, either remotely or locally and (b) guess passwords. Password guessing attempts are recorded as authentication failures by IDS and hosts.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.

Activity: Spyware - Top Hosts

This report ranks the hosts running spyware applications. Spywares are malicious applications that installs and runs on hosts, collect the username, passwords, and credit card information and send this information to the spyware writers.

Activity: Host Privilege Escalation - Top Hosts

This report records ranks the hosts by access privilege escalation attempts attempted against them. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: P2P Filesharing/Chat - Top Hosts

This report ranks hosts involved in P2P Filesharing and chat protocol activity. Such protocols may not be suitable in business environments.

Activity: Virus/Worms - Top Infected Hosts

This report ranks hosts that are propagating virus and worms via SMTP, POP, IMAP, network shares etc.

Activity: Database Privileged Command Failures - All Events

This report lists event details for all privileged database command execution failures.

Activity: Virus: Detected - Top Users

This report ranks users/workstations by viruses detected.

Activity: Database Privileged Command Failures - Top Users

This report ranks the users by failed privileged database command execution attempts.

Activity: Virus: Infections - Top Users

This report ranks users/workstations by viruses detected and not cleaned.

Activity: Database Regular Command Failures - All Events

This report lists the event details for all failed non-privileged database command execution attempts.

Activity: Database Regular Command Failures - Top Users

This report ranks the users by the number of non-privileged database command execution attempts.

Activity: Database User/Group Change Failures - All Events

This report lists the event details for all failed database user/group modification attempts.

Activity: Database User/Group Change Failures - Top Users

This report ranks the users by the number of failed database user/group modification attempts.

Activity: Database User/Group Change Successes - All Events

This report lists the event details for all successful database user/group modifications.

Activity: Database User/Group Change Successes - Top Users

This report ranks the users by the successful database user/group modifications performed.

Activity: Recreational - All Events

This event details all users involved in recreational activities such as games, specific web sites such as gambling etc.

Resource Utilization: Bandwidth: Inbound - Top Interfaces

This report ranks the inbound bandwidth utilization of the interfaces on the devices managed by PN-MARS.

Resource Utilization: CPU - Top Devices

This report ranks the CPU utilization of the devices managed by PN-MARS.

Resource Utilization: Bandwidth: Outbound - Top Interfaces

This report ranks the outbound bandwidth utilization of interfaces on devices managed by Pn-MARS.

Resource Utilization: Concurrent Connections - Top Devices

This report ranks the number of concurrent connections established through the devices managed by PN-MARS.

Resource Utilization: Errors: Inbound - Top Interfaces

This report ranks by error rate on the inbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Errors: Outbound - Top Interfaces

This report ranks by error rate on the outbound interfaces of the devices managed by PN-MARS.

Resource Utilization: Memory - Top Devices

This report ranks the memory utilization of the devices managed by PN-MARS.

Activity: Host Login Failures - All Events

This report records all host login failure details.

Activity: Spyware - All Events

This event details all spyware events.

Activity: Host Login Success - All Events

This report details all host login success event details

Activity: Host Admin Login Success - All Events

This report details successful administrative login events to hosts.

Activity: Host Privilege Escalation - All Events

This report provides details for events that represent an user attempting to increase access rights on a particular host. Such attempts can happen remotely or from the local console and can be reported by Network or Host IDS devices or the hosts themselves

Activity: Network Usage - Top Destination Ports By Bytes

This report ranks the top destination ports by bytes sent and transmitted.

Activity: Remote Access Login - All Events

This report details of remote access login events (IPSec, SSLVPN, PPP, L2TP etc)

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Attacks: Password - All Events

This report details all password attack events.

Configuration Changes: Network - All Events

This event details all the configuration changes in network devices.

Operational Issues: Network - All Events

This report lists details about all operational issues on network devices.

Operational Issues: Server - All Events

This report lists details about events that indicate operational errors on hosts or host applications.

Activity: Host Security Policy Changes - All Events

This report lists all policy changes on a host affecting host security. These events are typically reported by Host IDS and host agents.

Activity: Database Login Successes - All Events

This report lists event details for all successful database login events.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

System: Security Posture Compliance (Cisco NAC)

This category contains the following system reports:

This section contains the following topics:

- [Activity: Vulnerable Host Found via VA Scanner, page E-149](#)
- [Activity: Vulnerable Host Found, page E-149](#)
- [Activity: Security Posture: Healthy - Top Users, page E-149](#)

- [Activity: Security Posture: NAC - Top NADs, page E-149](#)
- [Activity: Security Posture: NAC - Top Tokens, page E-149](#)
- [Activity: Security Posture: NAC L2IP - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Audit Server Issues - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - All Events, page E-150](#)
- [Activity: Security Posture: NAC Infected/Quarantine - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC L2 802.1x - Top Tokens, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top Hosts, page E-150](#)
- [Activity: Security Posture: NAC Static Auth - Top NADs, page E-150](#)
- [Activity: Security Posture: NAC Status Query Failure - Top Hosts, page E-150](#)
- [Activity: Security Posture: Not Healthy - All Events, page E-151](#)
- [Activity: Security Posture: NAC - Top NADs and Tokens, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Tokens, page E-151](#)
- [Activity: Security Posture: NAC End Host Details - All Events, page E-151](#)
- [Activity: AAA Failed Auth - All Events, page E-151](#)
- [Activity: AAA Failed Auth - Top NADs, page E-151](#)
- [Activity: AAA Failed Auth - Top Users, page E-151](#)
- [Activity: Security Posture: NAC Agentless - Top Hosts, page E-152](#)
- [Activity: Security Posture: NAC Agentless - Top NADs, page E-152](#)

Activity: Vulnerable Host Found via VA Scanner

This report lists vulnerable hosts and associated vulnerabilities found by importing information from Vulnerability Analysis (VA) scanners.

Activity: Vulnerable Host Found

This host lists all vulnerable hosts found by IDS or VA scanners

Activity: Security Posture: Healthy - Top Users

This report lists the users in a HEALTHY Security Posture State. A Healthy security posture implies that the posture of the host is up to date, policy compliant and does not need attention.

Activity: Security Posture: NAC - Top NADs

This report ranks the network access devices (NADs) handling Network Admission Control transactions.

Activity: Security Posture: NAC - Top Tokens

This report shows the network wide distribution of NAC tokens. The possible token values are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC L2IP - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IP method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Audit Server Issues - All Events

This report ranks the end hosts for which the AAA server is having an issue with obtaining the right security posture token from the audit server. These hosts do not have the Cisco Trust Agent (CTA) running and they depend on an Audit Server for obtaining the proper Security Posture Token.

Activity: Security Posture: NAC Infected/Quarantine - All Events

This report reports the event details for the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC Infected/Quarantine - Top Hosts

This report details the hosts that are in an INFECTED or QUARANTINE state. The QUARANTINE hosts must do Anti-virus DAT file updates before network access and the INFECTED hosts must be cleaned before network access.

Activity: Security Posture: NAC L2 802.1x - Top Tokens

This report captures the distribution of NAC tokens for end hosts that use Layer 2 IEEE 802.1x method to validate their posture. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Static Auth - Top Hosts

This report captures the hosts that are configured as static exceptions on the Network Access Device (NAD). For these hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Static Auth - Top NADs

This report captures the Network Access Device (NAD) that are permitting end hosts into the network as static exceptions. For these end hosts, the NAD directly permits network access without consulting the posture validation server.

Activity: Security Posture: NAC Status Query Failure - Top Hosts

This report details the top hosts that failed the status queries from the Network Access Devices (NAD). Such failures occur after initial authorization whenever there is a change in posture detected by the Cisco Trust Agent (CTA) on the end host. Such failures may be caused by user frequently enabling or disabling CTA agents.

Activity: Security Posture: Not Healthy - All Events

This report lists the detailed events for users whose security posture is not up to date, ie. in either a CHECKUP, QUARANTINE or INFECTED state. The software on these hosts need to be upgraded. The CHECKUP hosts may need DAT file updates, the QUARANTINE hosts must do DAT file updates before network access and the INFECTED hosts must be remediated before network access.

Activity: Security Posture: NAC - Top NADs and Tokens

This report displays the Network Access Devices (NADs) handling Network Admission Control transactions along with the tokens assigned by each of them.

Activity: Security Posture: NAC Agentless - Top Tokens

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC End Host Details - All Events

This report details all the NAC related messages from the Network Access Devices (NAD) and AAA servers. Choose a source IP address or user to see the messages for one end host.

Activity: AAA Failed Auth - All Events

This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top NADs

This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: AAA Failed Auth - Top Users

This report ranks the users based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.

Activity: Security Posture: NAC Agentless - Top Hosts

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

Activity: Security Posture: NAC Agentless - Top NADs

This report captures the distribution of NAC tokens for end hosts that do not have Cisco Trust Agent (CTA) software. In this case, the posture validation is done either locally by the Network Access Device or via the Audit Server. The possible NAC tokens values in this report are HEALTHY, CHECKUP, INFECTED, QUARANTINE, UNKNOWN. The TRANSITION token is excluded since it is an intermediate state.

System: Server Exploits

This category contains the following system reports:

This section contains the following topics:

- [Activity: IDS Evasion - Top Event Types, page E-152](#)
- [Attacks: Database Server - Top Event Types, page E-152](#)
- [Attacks: FTP Server - Top Event Types, page E-152](#)
- [Attacks: Identity Spoofing - Top Event Types, page E-153](#)
- [Attacks: Login Services - Top Event Types, page E-153](#)
- [Attacks: Mail Server - Top Event Types, page E-153](#)
- [Attacks: RPC Services - Top Event Types, page E-153](#)
- [Attacks: SNMP - Top Event Types, page E-153](#)
- [Attacks: Web Server/App - Top Event Types, page E-153](#)
- [Attacks: Uncommon or Anomalous Traffic - Top Event Types, page E-153](#)

Activity: IDS Evasion - Top Event Types

This report ranks the events that detect an attempt by an attacker to evade detection by Network IDS systems. This may be web-based obfuscation attacks, fragmentation attacks or TCP/IP based attacks.

Attacks: Database Server - Top Event Types

This report ranks attacks on database servers such as MS SQL Server, Oracle and Sybase.

Attacks: FTP Server - Top Event Types

This report ranks attacks on FTP servers.

Attacks: Identity Spoofing - Top Event Types

This report ranks events that represent attempts by an attacker to spoof his/her identity over the past hour.

Attacks: Login Services - Top Event Types

This report ranks attacks on servers providing login services and remote shells. Examples include Telnet, SSH and Berkeley r-protocols.

Attacks: Mail Server - Top Event Types

This report ranks attacks on Mail servers (SMTP, POP, IMAP).

Attacks: RPC Services - Top Event Types

This report ranks attacks on RPC based applications.

Attacks: SNMP - Top Event Types

This report ranks SNMP based attacks over the past hour.

Attacks: Web Server/App - Top Event Types

This report ranks attacks on web servers or applications built on top of web servers over the past hour.

Attacks: Uncommon or Anomalous Traffic - Top Event Types

This report ranks the events that represent uncommon or anomalous traffic. Uncommon traffic involves ICMP types and TCP/IP options not in common usage or standard traffic on non-standard ports. Anomalous traffic includes traffic that violate IETF or other well known protocol specifications.



INDEX

Numerics

- 5-tuple data
 - low-latency event query [11-9](#)

A

- AAA authentication
 - and Cisco Secure ACS
 - for policy lookup [11-16](#)
- AAA server
 - add [14-9](#)
 - delete [14-16](#)
 - servers supported [14-1](#)
- access rule lookup [11-4](#)
 - device software versions
 - supported for [11-15](#)
 - devices with multiple contexts [11-4](#)
 - issues [11-8](#)
 - overview [11-5](#)
 - syslog messages supported
 - by IOS routers [11-7](#)
- access rules
 - looking up
 - from MARS events (procedure) [11-24](#)
- Accounts
 - expired
 - unlocking [14-4](#)
- ACS
 - See also Cisco Secure ACS
 - configuring user names [14-9](#)
- Activate button [4-15, 4-16, 4-18, 4-20, 6-1](#)
 - activating reporting devices [3-17](#)
 - explanation [7-11](#)
 - what it does [3-17](#)
 - when multiple users are logged in [7-12](#)
 - when to use [3-17](#)
- Activation Settings page [7-12](#)
- adding
 - cell phone number [6-14](#)
 - drop rules [4-19](#)
 - event groups [6-3](#)
 - inspection rules [4-16](#)
 - IP groups [6-4](#)
 - pager number [6-14](#)
 - service [6-10](#)
 - service provider [6-14](#)
 - user [5-13, 6-12](#)
 - user group [6-15](#)
- addresses [14-9](#)
- admin roles, see user management [6-11](#)
- Adobe SVG [7-18](#)
- alert action [4-12](#)
- alerts [5-1](#)
- anomaly detection
 - See NetFlow
- archive server
 - retrieving raw messages [13-3](#)
- ASA devices
 - supported software versions
 - for policy and events lookup [11-15](#)
 - with multiple contexts [11-4](#)
- attack diagram [7-18](#)
- attack paths
 - L2 [9-6](#)
 - L3 [9-6](#)

audit trail
 viewing [13-2](#)
 authentication settings
 policy table lookup
 allow saving of credentials [11-19](#)

B

Banner configuration [7-9](#)
 bootstrapping
 devices [2-5](#)
 Security Manager server
 for communication with MARS [11-16](#)
 Botnet Traffic Filter
 syslog and SNMP notification limitation [5-4](#)
 botnet traffic filter
 deleting botnet sites [12-14](#)
 Events [12-12](#)
 notifications [12-11](#)
 query criteria [12-3](#)
 query result format
 All Matching Events [12-6](#)
 site ranking [12-5](#)
 site management [12-14](#)
 System Reports [12-8](#)
 System Rules [12-11](#)

C

case management
 case report [10-7](#)
 editing cases [10-6](#)
 emailing case [10-7](#)
 overview [10-1](#)
 Catalyst 6500 Series switches
 supported software versions
 for policy and events lookup [11-15](#)
 cautions

 significance of [i-xlvii](#)
 cell phone paging
 adding [5-15, 6-14](#)
 certificate
 monitor status [13-9](#)
 upgrading from expired or fingerprint [13-9](#)
 certificates
 presented by Security Manager
 compared by MARS during policy lookup [11-10](#)
 changing
 drop rule status [4-18](#)
 inspection rule status [4-14](#)
 charts
 improving refresh time [7-21](#)
 Cisco IOS routers
 supported software versions
 for policy and events lookup [11-15](#)
 Cisco Secure ACS
 access settings for
 MARS appliance [11-16](#)
 configuring user names [14-9](#)
 roles for
 policy table lookup [11-16](#)
 Common Services
 AAA authentication for
 MARS appliance [11-16](#)
 Common Vulnerabilities and Exposures [6-2](#)
 configuration
 NetFlow [3-20](#)
 connection teardown messages [11-13](#)
 realtime event viewer [11-13](#)
 connectivity test
 between MARS and Security Manager [11-19](#)
 conventions [i-xlvi](#)
 creating
 report [8-30](#)
 custom device type parser
 selecting traffic type [15-19](#)
 custom log parser

- selecting traffic type [15-20](#)
- custom signatures
 - unknown device event type [11-33](#)
- CVE [6-2](#)

D

- database
 - cardinality calculation [13-14](#)
 - indexing [13-11](#)
 - tuning [13-11](#)
- data reduction [7-17](#)
- default certificate response
 - change [13-8](#)
- default fingerprint response
 - change [13-8](#)
- default password
 - change [13-7](#)
- deleting service [6-10](#)
- device event types
 - create new [15-8](#)
 - define
 - overview [15-6](#)
 - defined [15-1](#)
 - override defined patterns [15-17](#)
- devices
 - bootstrap overview [2-5](#)
 - define
 - overview [2-6](#)
 - deleting [3-14](#)
 - deleting all displayed [3-15](#)
 - edit [3-13](#)
 - in MARS
 - time synchronization, recommendation [11-14](#)
 - lookup [11-4](#)
 - managed by MARS and Security Manager
 - running compatible software version [11-14](#)
 - management traffic
 - between MARS and [11-14](#)
 - mitigation
 - monitored by MARS [11-14](#)
 - notification traffic
 - between MARS and [11-14](#)
 - policy lookup from MARS [11-5](#)
 - re-adding [3-14](#)
 - reporting
 - monitored by MARS [11-14](#)
 - software versions
 - supported by MARS and Security Manager [11-15](#)
 - versions supported for policy lookup
 - by MARS and Security Manager [11-10](#)
 - with multiple contexts [11-4](#)
- device support
 - define custom devices [15-3](#)
- device support framework
 - definition of [15-3](#)
- device support package
 - checksum protection [15-23](#)
 - define a device type [15-7](#)
 - defined [15-2](#)
 - events about [15-28](#)
 - export [15-24](#)
 - overview [15-6](#)
 - import [15-20](#)
 - password protection [15-27](#)
 - provider definition [15-5](#)
 - provider information
 - define [15-4](#)
 - remove [15-28](#)
 - reports about [15-28](#)
- device type
 - create custom [15-7](#)
 - custom
 - overview [15-5](#)
 - defined [15-1](#)
 - edit custom/local [15-17](#)
 - extend existing [15-18](#)
 - add event types [15-18](#)

- derive from [15-18](#)
- device types
 - override existing
 - edit parser [15-17](#)
- diagrams
 - attack [7-18](#)
- discovering networks
 - automatic [3-31](#)
- discovery
 - scheduling [3-31](#)
 - updating [3-31](#)
- display format
 - query [8-4](#)
- displays
 - refreshing [7-21](#)
- documentation
 - conventions [i-xlvi](#)
- drop rule
 - activate and inactive [4-18](#)
- drop rules
 - adding [4-19](#)
 - editing [4-19](#)
- drop rule status
 - changing [4-18](#)
- dynamic information [9-12](#)
- dynamic vulnerability scanning [3-19](#)

E

- editing
 - drop rules [4-19](#)
 - host information [6-7](#)
 - inspection rules [4-15](#)
 - IP groups [6-4](#)
 - service [6-10](#)
 - user [6-15](#)
- error messages
 - policy table lookup from MARS
 - connection setup syslog unavailable [11-13](#)

- connection teardown events in realtime viewer [11-13](#)
- event action filter
 - saving as a local policy [11-35](#)
- event groups [6-3](#)
- event management [6-2](#)
 - editing [6-2](#)
- expired
 - accounts [14-4](#)
- expired certificate [13-9](#)

F

- false positives
 - tuning [9-6](#)
 - types [9-9](#)
- fingerprint validation [13-7](#)
- FWSM
 - supported software versions
 - for policy and events lookup [11-15](#)
 - with multiple contexts [11-4](#)

G

- gateways
 - intermediate
 - allowing flows between MARS and devices [11-14](#)
- Global Controller
 - adding Security Manager to [11-16](#)
 - and Local Controllers [4-1, 4-4, 7-1](#)
 - Network Summary page [7-1](#)
 - queries [8-2](#)
 - rules [4-1, 4-4](#)
 - user management [6-12](#)

H

- hosts

- adding [6-5](#)
- editing [6-7](#)
- Hot Spot Graph [7-18](#)

I

- ICMP connection-related messages
 - access rule lookup from MARS [11-6](#)
- idle session timeout
 - of Security Manager
 - authentication of MARS [11-11](#)
 - policy table lookup [11-11](#)
- IDS/IPS modules
 - supported software versions
 - for policy and events lookup [11-15](#)
- Incident Details page [9-4](#)
- incidents [7-16](#)
 - defined [9-1](#)
 - incident path [9-4](#)
 - incident vector [9-4](#)
 - instances [9-7](#)
 - mitigation [9-11](#)
 - page [9-2](#)
- incident table [9-6](#)
- inspection rule
 - activate and inactive [4-14](#)
- inspection rules
 - adding [4-16](#)
 - editing [4-15](#)
- inspection rule status
 - changing [4-14](#)
- Internet Explorer
 - accessing MARS GUI using
 - for signature policy lookup [11-34](#)
- IOS IPS sensors
 - supported software versions
 - for policy and events lookup [11-15](#)
- IP groups
 - adding [6-4](#)

- editing [6-4](#)
- IP management [6-3](#)
 - adding
 - hosts [6-5](#)
 - IP range [6-5](#)
 - network [6-5](#)
 - variable [6-5](#)
 - filter list [6-4](#)
- IPS
 - Global Correlation Score [8-10](#)
 - Risk Rating [8-10](#)
 - Threat Rating [8-10](#)
- IPS sensors
 - supported software versions
 - for policy and events lookup [11-15](#)
- IPS signature
 - policy lookup [11-39](#)
- IPS signature policy
 - go to from MARS events [11-28](#)
- IPS signature policy lookup
 - device lookup query [11-5](#)
 - device software versions
 - supported for [11-15](#)
 - issues [11-8](#)
 - looking up devices in MARS [11-4](#)
 - overview [11-8](#)

L

- L2 attack path [9-6](#)
- L3 attack path [9-6](#)
- Local Controller [4-1, 4-4, 7-1](#)
 - adding Security Manager to (procedure) [11-20](#)
 - queries [8-2](#)
 - Security Manager not added to
 - user credential fields [11-20](#)
- Local User Setup page
 - defining
 - MARS user account [11-22](#)

- log files
 - viewing [13-2](#)
- logging levels [13-1](#)
- logging traffic
 - between MARS and monitored devices
 - enabling [11-14](#)
- login credentials
 - of Security Manager
 - saved in MARS during policy lookup [11-11](#)
- Login Failure
 - procedure to unlock [14-16](#)
- log keyword
 - output details [11-7](#)
- Logon Banner [7-9](#)
- log template
 - See device event type

M

- management
 - events [6-2](#)
 - IP [6-3](#)
 - service [6-8](#)
 - user [6-11](#)
- management traffic
 - between MARS and monitored devices
 - enabling [11-14](#)
- MARS
 - audit trail [13-2](#)
 - devices
 - identifying for policy lookup [11-14](#)
 - running supported software for lookup [11-14](#)
 - device software versions
 - supported for policy lookup [11-10](#)
 - integration with Security Manager [11-1](#)
 - log files [13-2](#)
- MARS appliance
 - time synchronization
 - recommendation [11-14](#)

- MARS events
 - for connection teardown
 - in realtime event viewer [11-13](#)
 - generated by management traffic [11-13](#)
- Matched Rule [9-4](#)
- matching rules
 - not found
 - during policy lookup [11-13](#)
- MIB
 - MARS format [3-44](#)
- mitigation
 - definition [9-11](#)
- mitigation policy
 - suggested content [2-2](#)
- monitoring policy
 - suggested content [2-2](#)

N

- NAC
 - See Network Admission Control
- navigating
 - to other MARS pages
 - from read-only access rule table [11-36](#)
- NetFlow
 - bootstrap reporting devices [3-22](#)
 - configuration [3-20](#)
 - description of use [3-21](#)
 - enable processing [3-23](#)
 - store ASA NetFlow [3-25](#)
- Netflow
 - supported versions [3-21](#)
- NetFlow Security Event Logging [3-21, 11-3, 11-5](#)
- Network Admission Control (NAC)
 - configuring [3-39](#)
- network discovery
 - auto-populate MARS [3-27](#)
 - exceptions to discovery [3-28](#)
 - how it works [3-28](#)

restricting list [3-30](#)

SNMP [3-28](#)

work around exceptions [3-28](#)

Network Status tab

Incidents [7-20](#)

Top Destinations [7-21](#)

Top Event Types [7-21](#)

Top Sources [7-21](#)

notification traffic

between MARS and monitored devices

enabling [11-14](#)

NSEL [3-21](#)

O

optimizing queries [13-11](#)

Order/Rank By [8-6](#)

order by [8-6](#)

P

pager [6-14](#)

adding [5-15](#)

parser template

defined [15-1](#)

password

change default [13-7](#)

device support package protection [15-27](#)

pattern

key [15-11](#)

value [15-11](#)

PIX firewalls

supported software versions

for policy and events lookup [11-15](#)

pnadmin [6-11](#)

policy query login dialog box

saving Security Manager credentials [11-11](#)

policy table lookup [11-1, 11-2](#)

checklist for [11-14](#)

device lookup query [11-5](#)

devices with multiple contexts [11-4](#)

issues [11-8](#)

provider configuration

define custom values [15-4](#)

public networks [3-30](#)

Q

queries

action

ANY [8-12](#)

display format [8-4](#)

use only firing events [8-7](#)

filter by time [8-6](#)

interface [8-2](#)

of Security Manager policies from MARS events [11-1](#)

operation

AND [4-11](#)

FOLLOWED-BY [4-11](#)

none [4-11](#)

OR [4-11](#)

optimizing [13-11](#)

rank by [8-6](#)

reporting device ranking [3-16](#)

rule [8-12](#)

ANY [8-12](#)

service

ANY [8-9](#)

defined services [8-9](#)

service variables [8-9](#)

types of [8-3](#)

Query page [8-1](#)

R

raw messages

- archive folder location [13-3](#)
- file name format [13-4](#)
- maximum size stored [13-3](#)
- retrieving from archive server [13-3](#)
- read-only access rule table
 - [11-35](#)
 - navigating to Access Rules page [11-36](#)
 - navigating to other MARS pages [11-36](#)
- realtime event viewer
 - access rule lookup
 - for connection teardown events [11-13](#)
- remediation policy
 - suggested content [2-2](#)
- removing
 - user [6-15](#)
- reporting device
 - custom [15-1](#)
 - device type [15-5](#)
 - custom appliance definition [15-18](#)
 - custom software definition [15-19](#)
 - unsupported [15-1](#)
 - receiving events from [15-2](#)
- reporting devices
 - custom [15-3](#)
- reports
 - adding [8-29, 8-30](#)
 - charts and graphs [8-29](#)
 - delete [8-31](#)
 - duplicate [8-32](#)
 - edit [8-31](#)
 - new [8-29, 8-30](#)
 - type views [8-27](#)
 - csv [8-28](#)
 - peak [8-28](#)
 - recent [8-28](#)
 - total [8-28](#)
 - viewing [8-21, 8-31](#)
- rules
 - destination IP
 - ANY [4-7](#)
 - devices [4-7](#)
 - DISTINCT [4-7](#)
 - IP addresses [4-7](#)
 - IP ranges [4-7](#)
 - Network Groups [4-7](#)
 - networks [4-7](#)
 - SAME [4-7](#)
 - variables [4-7](#)
 - device [4-10](#)
 - ANY [4-9](#)
 - Unknown Reporting Device [4-9](#)
 - variables [4-9](#)
 - event type grouping [4-9](#)
 - event types [4-9](#)
 - ANY [4-9](#)
 - variables [4-9](#)
 - reported user
 - ANY [4-10](#)
 - Invalid User Name [4-10](#)
 - NONE [4-10](#)
 - variables [4-10](#)
 - service
 - ANY [4-8](#)
 - defined groups [4-8](#)
 - defined services [4-8](#)
 - service variables [4-8](#)
 - severity
 - ANY [4-11](#)
 - green [4-11](#)
 - red [4-11](#)
 - yellow [4-11](#)
 - source IP
 - devices [4-7](#)
 - IP addresses [4-7](#)
 - IP ranges [4-7](#)
 - Network Groups [4-7](#)
 - networks [4-7](#)
 - variables [4-7](#)

runtime logging [13-1](#)

S

scheduling

discovery [3-31](#)

security policies

objectives of [2-1](#)

security policy

suggested content [2-1](#)

see CVE 25-2 [6-2](#)

See syslog messages

service

adding [6-10](#)

deleting [6-10](#)

editing [6-10](#)

editing groups [6-9](#)

service group

adding [6-9](#)

service management [6-8](#)

service provider

adding [5-15, 6-14](#)

services

adding group [6-9](#)

setting

runtime logging levels [13-1](#)

Severity icons [9-4](#)

Short Message Service

See SMS

signature ID

parsed from IPS event messages

for signature policy lookup from MARS [11-8](#)

signature policy lookup

from MARS events (procedure) [11-29](#)

signature policy lookup page [11-40](#)

signatures

looking up from events [11-29](#)

modifying [11-8](#)

Simple Network Management Protocol

See SNMP

SNMP [3-28](#)

SNMP RO, unsupported characters [3-8, 3-18](#)

SNMPv1

RO community string [3-11, 3-29](#)

SNMPv3

authentication protocol [3-11, 3-29](#)

context name [3-11, 3-30](#)

privacy protocol [3-11, 3-29](#)

security level [3-11, 3-29](#)

SSH

fingerprint validation [13-7](#)

SSL

certificate validation [13-7](#)

stacked charts [7-21](#)

static information [9-12](#)

subsignature ID

parsed from IPS event messages

for signature policy lookup from MARS [11-8](#)

syslog

alert forwarding [3-41](#)

disable relay [3-43](#)

enable relay [3-42](#)

forwarding

status reports [3-43](#)

mapping to policy [11-1](#)

message forwarding [3-41](#)

troubleshoot relay [3-44](#)

syslog messages

changing the severity level [11-7](#)

format [11-7](#)

for Packet Data events [11-8](#)

IDs [11-7](#)

system log messages

T

Threat Category [12-2](#)

Threat Level [12-2](#)

Timeout Interval, setting for GUI and CLI [7-7](#)

Topology

toggle device display [7-20](#)

traffic flows

between MARS and devices

enabling [11-14](#)

identify and enable [2-4](#)

troubleshooting

cannot add device [3-15](#)

cannot re-add a device [3-14](#)

tuning

false positives [9-6, 9-10](#)

U

Unknown Device Event Type

custom signatures and [11-8](#)

unlock

after login failure [14-16](#)

CLI command

after login failure [14-4](#)

use only firing events [8-7](#)

user

adding [5-13, 6-12](#)

editing [6-15](#)

removing [6-15](#)

user credentials

Reporting Applications tab of MARS

different from those in User Configuration
page [11-10](#)

user group

adding [6-15](#)

user management [6-11](#)

roles defined [6-11](#)

user roles

for policy lookup from MARS [11-16](#)

V

validation

fingerprint [13-7](#)

valid networks [3-30](#)

variables [4-7](#)

viewing

security incidents [11-1](#)

W

warnings

significance of [i-xlvi](#)