



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 [11-9](#)
 - overview [11-5](#)
 - syslog messages supported
 - by IOS routers [11-7](#)
- access rules
 - looking up
 - from MARS events (procedure) [11-23](#)
- 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](#)

BBanner 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 [12-13](#)

- Events [12-11](#)

- notifications [12-10](#)

- query criteria [12-3](#)

- query result format

- All Matching Events [12-6](#)

- site ranking [12-4](#)

- site management [12-12](#)

- System Reports [12-8](#)

- System Rules [12-10](#)

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 [11-16](#)

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](#)community strings [3-28](#)

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 [11-32](#)

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](#)

Device Resource Usage [3-32](#)

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 [3-15](#)

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](#)
- device usage parameters [3-32](#)
- diagrams
 - attack [7-18](#)
- discovering networks
 - automatic [3-30](#)
- discovery
 - scheduling [3-30](#)
 - updating [3-30](#)
- 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 [11-34](#)
- 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 [11-16](#)
 - with multiple contexts [11-4](#)

G

- gateways
 - intermediate
 - allowing flows between MARS and devices [11-14](#)
- Global Controller
 - adding Security Manager to [11-17](#)
 - 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](#)

IDSM-2 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 [11-33](#)

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 [11-38](#)

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 [11-9](#)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 [11-14](#)
 - MIB
 - MARS format [3-42](#)
 - 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 [11-35](#)
 - NetFlow
 - bootstrap reporting devices [3-22](#)
 - configuration [3-20](#)
 - description of use [3-21](#)
 - enable processing [3-24](#)
 - 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 [3-37](#)
 - network discovery

- auto-populate MARS [3-27](#)
- exceptions to discovery [3-27](#)
- how it works [3-27](#)
- restricting list [3-29](#)
- work around exceptions [3-27](#)

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](#)

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 [11-9](#)
- provider configuration
 - define custom values [15-4](#)
- public networks [3-29](#)

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

[11-34](#)

- navigating to Access Rules page [11-35](#)
- navigating to other MARS pages [11-35](#)

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](#)

Resource Monitoring [3-32](#)

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 [3-30](#)

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 [11-39](#)

signatures

- looking up from events [11-28](#)
- modifying [11-8](#)

Simple Network Management Protocol

- See SNMP

SNMP OIDs [3-34](#)

SNMP RO, unsupported characters [3-9, 3-19](#)

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 [3-39](#)
- disable relay [3-41](#)
- enable relay [3-40](#)
- forwarding
 - status reports [3-41](#)
- mapping to policy [11-1](#)
- message forwarding [3-39](#)
- troubleshoot relay [3-42](#)

syslog messages

- changing the severity level [11-7](#)
- format [11-7](#)
- for Packet Data events [11-8](#)
- IDs [11-7](#)

system log messages

T

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 [3-15](#)
- tuning
 - false positives [9-6, 9-10](#)

- security incidents [11-1](#)

W

- warnings
 - significance of [i-xlvii](#)

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 [11-11](#)
- 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 [3-29](#)
- variables [4-7](#)
- viewing