INDEX

A

AAA server
- add 3-8
- delete 3-15
- servers supported 3-1

Accounts
- expired
  - unlocking 3-4

ACS
- configuring user names 3-8

Action 6-3

Activate button 8-17, 8-18, 8-20, 10-1
- explanation 4-7
- when multiple users are logged in 4-8

Activation Settings page 4-9

adding
- cell phone number 9-11, 10-9
- devices 2-15
  - manually 2-15
- event groups 10-3
- inspection rules 8-18
- pager number 9-11, 10-9
- service 10-6
- user 9-10, 10-7
- user group 10-10

adding IP groups 10-4

adding service provider 9-11, 10-9

admin roles, see user management 10-7

Adobe SVG 4-15

alert
- action 8-14
  - Distributed Threat Management 8-14
  - Email 8-14
  - NONE 8-14
  - Page 8-14
  - SMS 8-14
  - SNMP 8-14
  - Syslog 8-14

alerts 9-1

all matching event raw messages 7-8

all matching events 7-8

all matching sessions 7-7

attack diagram 4-14

attack paths
- L2 6-5
- L3 6-5

audit trail 11-3

B

bytes transmitted 7-8

C

cell phone paging 9-11, 10-9

certificate
- monitor status 11-6
- upgrading from expired or fingerprint 11-6

changing
- inspection rule status 8-16

Cisco Secure ACS
- configuring user names 3-8

Collapse All 6-5

Common Vulneratbilities and Exposures 10-2

creating

report 7-22
CVE 10-2

D

data reduction 4-14
default certificate response
change 11-6
default fingerprint response
change 11-6
default password
change 11-4
deleting service 10-6
destination IP address ranking 7-7
destination network group ranking 7-7
destination network ranking 7-7
destination ranking 7-7
diagrams
attack 4-14
display format
query 7-6

E

editing
inspection rules 8-17
IP groups 10-4
service 10-6
user 10-10
event groups 10-3
event management 10-1
editing 10-2
Event Type 6-3
event type group ranking 7-6
event type ranking 7-6
Expand All 6-5
expired
accounts 3-4
expired certificate 11-6

F

false positives
tuning 6-5
fingerprint validation 11-4

G

Global Controller i-xxv
adding Local Controllers to 2-3
and Local Controllers 2-14, 4-1, 6-1, 7-1, 8-1, 8-3, 10-7
Network Summary page 4-1
queries 7-1
rules 8-1, 8-3
user interface i-xxv
user management 10-7
Global Controller
overview 1-1

H

hardware maintenance
MARS 100, 100E, 200, GCM, GC 11-8
Hot Spot Graph 4-14

I

incident count 7-8
Incident Details page 6-4
Incident ID 6-3
Incident Path 6-3
incidents 4-13
action 6-3
event type 6-3
incident ID 6-3
incident path 6-3

incident vector 6-3
instances 6-6
matched rule 6-3
severity 6-3
time 6-3
time ranges 6-4
incidents table
navigation 6-3
incident table 6-5
Incident Vector 6-3
inspection rule
activate and inactive 8-16
inspection rules
adding 8-18
editing 8-17
inspection rule status
changing 8-16
instances
incidents 6-6
interoperability
local controllers and global controllers 2-2
IP groups
adding 10-4
editing 10-4
IP management 10-3
adding
IP range 10-4
network 10-4
variable 10-4

L

L2 attack path 6-5
L3 attack path 6-5
Local Controller 2-14, 4-1, 6-1, 7-1, 8-1, 8-3, 10-7
log files 11-2
Login Failure
procedure to unlock 3-15

M

MAC address report 7-8
management
events 10-1
IP 10-3
service 10-5
user 10-6
MARS
audit trail 11-3
log files 11-2
matched incident ranking 7-7
Matched Rule 6-3
matched rule ranking 7-7
mitigate 6-5

N

NAT connection report 7-8
network group ranking 7-6
network ranking 7-6
Network Status tab
Incidents 4-17
Top Destinations 4-18
Top Event Types 4-17
Top Sources 4-18

O

Order/Rank By 7-8
order by 7-8
bytes transmitted 7-8
incident count 7-8
session count 7-8
time 7-8

P

pager 9-11, 10-9
password
  change default 11-4
post NAT destination addresses 7-11
post NAT source addresses 7-11
pre NAT destination addresses 7-11
pre NAT source addresses 7-11
protocol ranking 7-7

Q

queries
  action
    ANY 7-13
  actions 7-13
  destination IP 7-11
    ANY 7-11
    devices 7-12
    IP addresses 7-11
    IP ranges 7-11
    networks 7-11
    post NAT destination addresses 7-11
    pre NAT destination addresses 7-11
  devices 7-12
  display format
    all matching event raw messages 7-8
    all matching events 7-8
    all matching sessions 7-7
    destination IP address ranking 7-7
    destination ranking 7-7
    event type group ranking 7-6
    MAC address report 7-8
    matched incident ranking 7-7
    matched rule ranking 7-7
    NAT connection report 7-8
    protocol ranking 7-7
    reporting device ranking 7-7
    reporting device type ranking 7-7
    source IP address ranking 7-6
    source port ranking 7-7
    unknown event report 7-8
    use only firing events 7-9
  event type grouping 7-12
  event types 7-12
    ANY 7-12
  operation
    AND 7-13, 8-12
    FOLLOWED-BY 7-13, 8-12
    none 7-13, 8-12
    OR 7-13, 8-12
  result format
    destination network group ranking 7-7
    destination network ranking 7-7
    event type ranking 7-6
    network group ranking 7-6
    network ranking 7-6
    reported user ranking 7-7
    source network group ranking 7-6
    source network ranking 7-6
  rule 7-13
    ANY 7-13
  save as
    reports 7-13
    rules 7-13
  service
    ANY 7-12
    defined services 7-12
    service variables 7-12
  severity
    ANY 7-12
    green 7-12
    red 7-12
    yellow 7-12
  source IP
    ANY 7-11
    devices 7-11

IP addresses 7-11
IP ranges 7-11
networks 7-11
post NAT source addresses 7-11
pre NAT source addresses 7-11
variables 7-11
time range
last 7-8
start and end times 7-8
zone 7-12
query
display format 7-6
Query page 7-1

R

rank by 7-8
bytes transmitted 7-8
incident count 7-8
session count 7-8
time 7-8
removing
user 10-10
report
adding 7-22
delete 7-23
edit 7-23
new 7-22
reported user ranking 7-7
reporting device ranking 7-7
reporting device type ranking 7-7
reports
viewing 7-16, 7-22
reports, view type, CSV 7-21
reports, view type, recent 7-21
reports,view type, total 7-21
report views, CSV 7-21
report views, peak, reports, view type, peak 7-21
report views, recent 7-21
report views, total 7-21
rules
destination IP
ANY 8-7
devices 8-7
DISTINCT 8-7
IP addresses 8-7
IP ranges 8-7
Network Groups 8-7
networks 8-7
SAME 8-7
variables 8-7
device 8-10
ANY 8-10
Unknown Reporting Device 8-10
variables 8-10
event type grouping 8-9
event types 8-9
ANY 8-9
variables 8-9
reported user
ANY 8-10
Invalid User Name 8-10
NONE 8-10
variables 8-10
service
ANY 8-8
defined groups 8-9
defined services 8-9
service variables 8-8
severity
ANY 8-11
green 8-11
red 8-11
yellow 8-11
source IP
devices 8-6
IP addresses 8-6
IP ranges 8-6

Network Groups 8-6
networks 8-6
variables 8-6
runtime logging 11-1

S

see CVE 10-2
service
adding 10-6
deleting 10-6
editing 10-6
editing groups 10-5
service group
adding 10-5
service management 10-5
service provider
adding 9-11, 10-9
services
adding group 10-5
session count 7-8
setting
runtime logging levels 11-1
Severity icons 6-3
Short Message Service
See SMS. 8-14
Simple Network Management Protocol
See SNMP. 8-14
source IP address ranking 7-6
source network group ranking 7-6
source network ranking 7-6
source port ranking 7-7
SSH
fingerprint validation 11-4
SSL
certificate validation 11-4
stacked charts 4-18

T

table
incidents 6-5
Time 6-3
Timeout Interval, setting for GUI and CLI 4-6
time ranges
incidents 6-4
Topology
toggle device display 4-17
tuning
false positives 6-5

U

unknown event report 7-8
unlock
after login failure 3-15
CLI command
after login failure 3-4
use only firing events 7-9
user
adding 9-10, 10-7
editing 10-10
removing 10-10
user group
adding 10-10
user management 10-6
roles defined 10-7

V

validation
fingerprint 11-4
variables 7-11, 8-6, 8-7