INDEX

A

adding
- an entry to the known hosts table 87
- a public key 84
- a trusted host 91

Administrators
- privileges 1

alerts
- viewing 55

application partition
- reimaging 39

applying
- service packs 94
- signature updates 94

attacker IP address
- removing from list of denied IP addresses 5

B

banner login
- describing 3
- examples 3
- syntax 3
- using 3

banner message
- creating 3

block requests
- viewing 55

C

capturing
- live traffic 31

changing the password 34

clear denied-attackers
- describing 5
- examples 5
- using 5

clear events
- describing 6
- examples 6
- using 6

clear line
- describing 7
- examples 7
- syntax 7
- using 7

CLI
- command line editing 4
- command modes 5
- default keywords 8
- error messages 1
- generic commands 7
- regular expression syntax 5

CLI behavior 2
- case sensitivity 3
- display options 3
- help 2
- prompts 2
- recall 3
- tab completion 3

clock set
- describing 9
- examples 9
- syntax 9

using 9
closing an active terminal session 18
command line editing (table) 4
command modes 5
event action rules configuration 5
EXEC 5
global configuration 5
privileged EXEC 5
service mode configuration 5
signature definition configuration 5
command platform dependencies 2
commands
deprecated 1
platform dependencies 2
viewing list of most recently used 59
configure
describing 10
examples 10
syntax 10
using 10
conventions vii
copy
describing 11
examples 12
syntax 11
using 11
copying
configuration files 11
iplogs 11
creating
banner message 3
users 96
Ctrl-N 3
Ctrl-P 3

D

default keywords
using 8
deleting a logical file 17
denied attackers
removing 5
deprecated commands 1
directing output to the serial connection 14
display
specifying number of lines on screen 89
displaying
current level of privilege 65
current system status 76
interface statistics 62
IP log contents 21
IP packet route 93
known hosts table 72
live traffic 31
local event log contents 55
PEP information 64
public RSA keys 69
sensor trusted hosts 79
server TLS certificate fingerprint 78
SSH server's host key 71
statistics 73
system clock 52
user information 80
version information 82
display-serial
describing 14
examples 14
using 14
downgrade
describing 15
examples 15

E

end
describing 16
examples 16
entering

global configuration 10
service configuration mode 41
erase
describing 17
examples 17
syntax 17
using 17
error events
viewing 55
error messages 1
event log
viewing contents of 55
events
clearing 6
deleting 6
Event Store
clearing events 6
exit
describing 18
examples 18
using 18
exiting
configuration mode 16, 18
submodes 16

G

generating
server host key 86
X.509 certificate 90
generic commands 7

H

help
question mark 2
using 2

I

initializing the sensor 44
iplog
describing 19
examples 20
syntax 19
using 19
iplog-status
describing 21
examples 21
using 21
IP packet
display route 93

K

keywords
default 8
no 8

M

modifying
privilege level 38
terminal properties for a login session 89
monitoring
Viewer privileges 2
more exclude
describing 27
examples 27
syntax 27
using 27
more include
describing 29

N

network connectivity
testing for 36

O

Operators
privileges 2
output
clearing current line 3
displaying 3
setting number of lines to display 89

P

packet
describing 31
examples 32
syntax 31
using 32
password
changing 34
describing 34
examples 35
syntax 34
updating 34
using 34
ping
describing 36
examples 36
syntax 36
using 36
privilege
describing 38
examples 38
modifying 38
syntax 38
prompts
default input 2

R

recall
help and tab completion 3
using 3
recover
describing 39
examples 39
syntax 39
using 39
regular expression syntax 5
regular expression syntax (table) 6
removing the most recent upgrade 15
reset
describing 40
examples 40
syntax 40
using 40
route
displaying for IP packet 93

S

Service
privileges 2
service
analysis-engine 41
authentication 41
certificate-authority 41
describing 41
event-action-rules 41
examples 42
host 41
interface 41
logger 41
network-access 41

notification 41
signature-definition 41
ssh-known-hosts 41
syntax 41
trusted-certificate 41
using 42
web-server 41
service account
privileges 2
service event-action-rules
using 42
service role 2
setting the system clock 9
setup
clock setting parameters (table) 45
describing 44
examples 46
using 45
show begin
describing 50
examples 50
syntax 50
using 50
show clock
authoritative flags 52
describing 52
examples 52
syntax 52
using 52
show events
describing 55
examples 56
syntax 55
using 56
show exclude
describing 57
examples 57
syntax 57
using 57
show history
describing 59
examples 59
using 59
show include
describing 60
examples 60
using 60
show interfaces
describing 62
examples 62
syntax 62
using 62
show inventory
describing 64
examples 64
using 64
show privilege
describing 65
examples 65
using 65
show settings
describing 66
examples 66
syntax 66
show ssh authorized-keys
describing 69
examples 69
syntax 69
using 69
show ssh host-keys
describing 72
examples 72
syntax 72
using 72
show ssh server-key
describing 71
examples 71
show statistics

describing 73
syntax 73
show tech-support
describing 76
examples 77
using 76
show tls-fingerprint
describing 78
examples 78
show tls trusted-hosts
describing 79
examples 79
syntax 79
using 79
show users
describing 80
examples 80
syntax 80
using 80
show version
describing 82
examples 82
using 82
ssh authorized-key
describing 84
examples 84
syntax 84
using 84
ssh generate-key
describing 86
examples 86
using 86
ssh host-key
describing 87
examples 88
syntax 87
using 87
starting IP logging 19
statistics
clearing 73
viewing 73
status events
viewing 55
syntax
case sensitivity 3
system
viewing status 76
System Configuration Dialog 45
system information
exporting to FTP or SCP server 76

T

tab completion
using 3
tech support
viewing
control transaction responses 76
current configuration information 76
debug logs 76
version 76
terminal
describing 89
examples 89
syntax 89
using 89
terminating a CLI session 7
tls generate-key
describing 90
examples 90
tls trusted-host
describing 91
examples 91
syntax 91
using 91
trace
describing 93
examples 93

using 93

U

updating the password 34
upgrade
describing 94
examples 95
syntax 94
using 94
upgrading the system 94
username
describing 96
examples 96
syntax 96
using 96
user roles
Administrator 1, 2
Operator 1, 2
Service 1, 2
Viewer 1, 2

V

Viewers
privileges 2
viewing
alerts 55
block requests 55
error events 55
IPS processes 82
operating system 82
signature packages 82
status events 55