



## INDEX

---

### A

- adding
  - an entry to the known hosts table [2-88](#)
  - a public key [2-85](#)
  - a trusted host [2-92](#)
- Administrators
  - privileges [1-1](#)
- alerts
  - viewing [2-56](#)
- application partition
  - reimaging [2-39](#)
- applying
  - service packs [2-95](#)
  - signature updates [2-95](#)
- attacker IP address
  - removing from list of denied IP addresses [2-5](#)

---

### B

- banner login
  - describing [2-3](#)
  - examples [2-3](#)
  - syntax [2-3](#)
  - using [2-3](#)
- banner message
  - creating [2-3](#)
- block requests
  - viewing [2-56](#)

---

### C

- capturing
  - live traffic [2-31](#)
- changing the password [2-34](#)
- clear denied-attackers
  - describing [2-5](#)
  - examples [2-5](#)
  - using [2-5](#)
- clear events
  - describing [2-6](#)
  - examples [2-6](#)
  - using [2-6](#)
- clear line
  - describing [2-7](#)
  - examples [2-7](#)
  - syntax [2-7](#)
  - using [2-7](#)
- CLI
  - command line editing [1-4](#)
  - command modes [1-5](#)
  - default keywords [1-8](#)
  - error messages [B-1](#)
  - generic commands [1-7](#)
  - regular expression syntax [1-5](#)
- CLI behavior [1-2](#)
  - case sensitivity [1-3](#)
  - display options [1-3](#)
  - help [1-2](#)
  - prompts [1-2](#)
  - recall [1-3](#)
  - tab completion [1-3](#)

clock set

- describing [2-9](#)
- examples [2-9](#)
- syntax [2-9](#)
- using [2-9](#)

closing an active terminal session [2-18](#)

command line editing (table) [1-4](#)

command modes [1-5](#)

- event action rules configuration [1-5](#)
- EXEC [1-5](#)
- global configuration [1-5](#)
- privileged EXEC [1-5](#)
- service mode configuration [1-5](#)
- signature definition configuration [1-5](#)

command platform dependencies [A-2](#)

commands

- deprecated [A-1](#)
- platform dependencies [A-2](#)
- viewing list of most recently used [2-60](#)

configure

- describing [2-10](#)
- examples [2-10](#)
- syntax [2-10](#)
- using [2-10](#)

conventions [i-vii](#)

copy

- describing [2-11](#)
- examples [2-12](#)
- syntax [2-11](#)
- using [2-11](#)

copying

- configuration files [2-11](#)
- iplogs [2-11](#)

creating

- banner message [2-3](#)
- users [2-97](#)

Ctrl-N [1-3](#)

Ctrl-P [1-3](#)

---

## D

default keywords

- using [1-8](#)

deleting a logical file [2-17](#)

denied attackers

- removing [2-5](#)

deprecated commands [A-1](#)

directing output to the serial connection [2-14](#)

display

- specifying number of lines on screen [2-90](#)

displaying

- current level of privilege [2-66](#)
- current system status [2-77](#)
- interface statistics [2-63](#)
- IP log contents [2-21](#)
- IP packet route [2-94](#)
- known hosts table [2-73](#)
- live traffic [2-31](#)
- local event log contents [2-56](#)
- PEP information [2-65](#)
- public RSA keys [2-70](#)
- sensor trusted hosts [2-80](#)
- server TLS certificate fingerprint [2-79](#)
- SSH server's host key [2-72](#)
- statistics [2-74](#)
- system clock [2-53](#)
- user information [2-81](#)
- version information [2-83](#)

display-serial

- describing [2-14](#)
- examples [2-14](#)
- using [2-14](#)

downgrade

- describing [2-15](#)
- examples [2-15](#)

---

**E**

end

describing [2-16](#)examples [2-16](#)

entering

global configuration [2-10](#)service configuration mode [2-42](#)

erase

describing [2-17](#)examples [2-17](#)syntax [2-17](#)using [2-17](#)

error events

viewing [2-56](#)error messages [B-1](#)

event log

viewing contents of [2-56](#)

events

clearing [2-6](#)deleting [2-6](#)

Event Store

clearing events [2-6](#)

exit

describing [2-18](#)examples [2-18](#)using [2-18](#)

exiting

configuration mode [2-16, 2-18](#)submodes [2-16](#)

---

**G**

generating

server host key [2-87](#)X.509 certificate [2-91](#)generic commands [1-7](#)

---

**H**

help

question mark [1-2](#)using [1-2](#)

---

**I**initializing the sensor [2-45](#)

iplog

describing [2-19](#)examples [2-20](#)syntax [2-19](#)using [2-19](#)

iplog-status

describing [2-21](#)examples [2-21](#)using [2-21](#)

IP packet

display route [2-94](#)

---

**K**

keywords

default [1-8](#)no [1-8](#)

---

**M**

modifying

privilege level [2-38](#)terminal properties for a login session [2-90](#)

monitoring

Viewer privileges [1-2](#)

more exclude

describing [2-27](#)examples [2-27](#)syntax [2-27](#)

using [2-27](#)

more include

describing [2-29](#)

---

## N

network connectivity

testing for [2-36](#)

---

## O

Operators

privileges [1-2](#)

output

clearing current line [1-3](#)

displaying [1-3](#)

setting number of lines to display [2-90](#)

---

## P

packet

describing [2-31](#)

examples [2-32](#)

syntax [2-31](#)

using [2-32](#)

password

changing [2-34](#)

describing [2-34](#)

examples [2-35](#)

syntax [2-34](#)

updating [2-34](#)

using [2-34](#)

ping

describing [2-36](#)

examples [2-36](#)

syntax [2-36](#)

using [2-36](#)

privilege

describing [2-38](#)

examples [2-38](#)

modifying [2-38](#)

syntax [2-38](#)

prompts

default input [1-2](#)

---

## R

recall

help and tab completion [1-3](#)

using [1-3](#)

recover

describing [2-39](#)

examples [2-39](#)

syntax [2-39](#)

using [2-39](#)

regular expression syntax [1-5](#)

regular expression syntax (table) [1-6](#)

removing the most recent upgrade [2-15](#)

reset

describing [2-41](#)

examples [2-41](#)

syntax [2-41](#)

using [2-41](#)

route

displaying for IP packet [2-94](#)

---

## S

Service

privileges [1-2](#)

service

analysis-engine [2-42](#)

authentication [2-42](#)

certificate-authority [2-42](#)

describing [2-42](#)

- event-action-rules [2-42](#)
- examples [2-43](#)
- host [2-42](#)
- interface [2-42](#)
- logger [2-42](#)
- network-access [2-42](#)
- notification [2-42](#)
- signature-definition [2-42](#)
- ssh-known-hosts [2-42](#)
- syntax [2-42](#)
- trusted-certificate [2-42](#)
- using [2-43](#)
- web-server [2-42](#)
- service account
  - privileges [1-2](#)
- service event-action-rules
  - using [2-43](#)
- service role [1-2](#)
- setting the system clock [2-9](#)
- setup
  - clock setting parameters (table) [2-46](#)
  - describing [2-45](#)
  - examples [2-47](#)
  - using [2-46](#)
- show begin
  - describing [2-51](#)
  - examples [2-51](#)
  - syntax [2-51](#)
  - using [2-51](#)
- show clock
  - authoritative flags [2-53](#)
  - describing [2-53](#)
  - examples [2-53](#)
  - syntax [2-53](#)
  - using [2-53](#)
- show events
  - describing [2-56](#)
  - examples [2-57](#)
  - syntax [2-56](#)
  - using [2-57](#)
- show exclude
  - describing [2-58](#)
  - examples [2-58](#)
  - syntax [2-58](#)
  - using [2-58](#)
- show history
  - describing [2-60](#)
  - examples [2-60](#)
  - using [2-60](#)
- show include
  - describing [2-61](#)
  - examples [2-61](#)
  - using [2-61](#)
- show interfaces
  - describing [2-63](#)
  - examples [2-63](#)
  - syntax [2-63](#)
  - using [2-63](#)
- show inventory
  - describing [2-65](#)
  - examples [2-65](#)
  - using [2-65](#)
- show privilege
  - describing [2-66](#)
  - examples [2-66](#)
  - using [2-66](#)
- show settings
  - describing [2-67](#)
  - examples [2-67](#)
  - syntax [2-67](#)
- show ssh authorized-keys
  - describing [2-70](#)
  - examples [2-70](#)
  - syntax [2-70](#)
  - using [2-70](#)
- show ssh host-keys
  - describing [2-73](#)
  - examples [2-73](#)

- syntax [2-73](#)
    - using [2-73](#)
  - show ssh server-key
    - describing [2-72](#)
    - examples [2-72](#)
  - show statistics
    - describing [2-74](#)
    - syntax [2-74](#)
  - show tech-support
    - describing [2-77](#)
    - examples [2-78](#)
    - using [2-77](#)
  - show tls-fingerprint
    - describing [2-79](#)
    - examples [2-79](#)
  - show tls trusted-hosts
    - describing [2-80](#)
    - examples [2-80](#)
    - syntax [2-80](#)
    - using [2-80](#)
  - show users
    - describing [2-81](#)
    - examples [2-81](#)
    - syntax [2-81](#)
    - using [2-81](#)
  - show version
    - describing [2-83](#)
    - examples [2-83](#)
    - using [2-83](#)
  - ssh authorized-key
    - describing [2-85](#)
    - examples [2-85](#)
    - syntax [2-85](#)
    - using [2-85](#)
  - ssh generate-key
    - describing [2-87](#)
    - examples [2-87](#)
    - using [2-87](#)
  - ssh host-key
    - describing [2-88](#)
    - examples [2-89](#)
    - syntax [2-88](#)
    - using [2-88](#)
  - starting IP logging [2-19](#)
  - statistics
    - clearing [2-74](#)
    - viewing [2-74](#)
  - status events
    - viewing [2-56](#)
  - syntax
    - case sensitivity [1-3](#)
  - system
    - viewing status [2-77](#)
  - System Configuration Dialog [2-46](#)
  - system information
    - exporting to FTP or SCP server [2-77](#)
- 
- T**
- tab completion
    - using [1-3](#)
  - tech support
    - viewing
      - control transaction responses [2-77](#)
      - current configuration information [2-77](#)
      - debug logs [2-77](#)
      - version [2-77](#)
  - terminal
    - describing [2-90](#)
    - examples [2-90](#)
    - syntax [2-90](#)
    - using [2-90](#)
  - terminating a CLI session [2-7](#)
  - tls generate-key
    - describing [2-91](#)
    - examples [2-91](#)
  - tls trusted-host
    - describing [2-92](#)

examples [2-92](#)

syntax [2-92](#)

using [2-92](#)

trace

describing [2-94](#)

examples [2-94](#)

using [2-94](#)

signature packages [2-83](#)

status events [2-56s](#)

---

## U

updating the password [2-34](#)

upgrade

describing [2-95](#)

examples [2-96](#)

syntax [2-95](#)

using [2-95](#)

upgrading the system [2-95](#)

username

describing [2-97](#)

examples [2-97](#)

syntax [2-97](#)

using [2-97](#)

user roles

Administrator [1-1, 1-2](#)

Operator [1-1, 1-2](#)

Service [1-1, 1-2](#)

Viewer [1-1, 1-2](#)

---

## V

Viewers

privileges [1-2](#)

viewing

alerts [2-56](#)

block requests [2-56](#)

error events [2-56](#)

IPS processes [2-83](#)

operating system [2-83](#)

