



INDEX

A

adding
 an entry to the known hosts table [2-136](#)
 a public key [2-133](#)
 a trusted host [2-140](#)
administrator privileges [1-1](#)
alerts viewing [2-97](#)
anomaly detection file
 loading [2-4](#)
 saving [2-5](#)
 using [2-5](#)
anomaly-detection load
 described [2-4](#)
 examples [2-4](#)
 syntax [2-4](#)
anomaly-detection name described [2-68](#)
anomaly-detection save
 described [2-5](#)
 examples [2-5](#)
 syntax [2-5](#)
application partition reimaging [2-64](#)
applying
 service packs [2-143](#)
 signature updates [2-143](#)
attacker IP address removing [2-15](#)
attemptLimit
 described [2-6](#)
 examples [2-6](#)
 related commands [2-6](#)
 syntax [2-6](#)
 using [2-6](#)

B

banner login
 described [2-7](#)
 examples [2-7](#)
 using [2-7](#)
banner message creating [2-7](#)
block requests viewing [2-97](#)

C

capturing live traffic [2-56](#)
changing the password [2-59](#)
clear denied-attackers
 described [2-15](#)
 examples [2-15, 2-30](#)
 syntax [2-15, 2-29](#)
 using [2-15, 2-29](#)
clear events
 described [2-17](#)
 examples [2-17, 2-102](#)
 using [2-17, 2-102](#)
clear line
 described [2-18](#)
 examples [2-18](#)
 syntax [2-18](#)
 using [2-18](#)
clear os-identification
 described [2-20](#)
 examples [2-20](#)
 syntax [2-20](#)
 using [2-20](#)

CLI

- command line editing [1-4](#)
- command modes [1-5](#)
- default keywords [1-8](#)
- error messages [A-1](#)
- generic commands [1-7](#)
- regular expression syntax [1-5](#)

CLI behavior

- case sensitivity [1-3](#)
- described [1-2](#)
- display options [1-3](#)
- help [1-2](#)
- prompts [1-2](#)
- recall [1-3](#)
- tab completion [1-3](#)

clock set

- described [2-21](#)
- examples [2-21](#)
- syntax [2-21](#)
- using [2-21](#)

closing an active terminal session [2-38](#)command line editing (table) [1-4](#)

command modes

- described [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 [1-8](#)

commands

- platform dependencies [1-8](#)
- viewing list of most recently used [2-103](#)

configure

- described [2-22](#)
- examples [2-22](#)
- syntax [2-22](#)
- using [2-22](#)

copy

- described [2-23](#)
- examples [2-24](#)
- syntax [2-23](#)
- using [2-23](#)

copy ad-knowledge-base

- described [2-26](#)
- examples [2-27](#)
- syntax [2-26](#)
- using [2-26](#)

copying

- configuration files [2-23](#)
- iplogs [2-23](#)

copy instance

- described [2-28](#)
- examples [2-28](#)
- syntax [2-28](#)
- using [2-28](#)

creating

- banner message [2-7](#)
- users [2-146](#)

Ctrl-N [1-3](#)Ctrl-P [1-3](#)

Ddefault keywords using [1-8](#)deleting a logical file [2-34](#)denied attackers removing [2-15](#)directing output to the serial connection [2-31](#)

displaying

- current level of privilege [2-114](#)
- current system status [2-125](#)
- interface statistics [2-109](#)
- IP log contents [2-41](#)
- IP packet route [2-142](#)
- known hosts table [2-121](#)
- live traffic [2-56](#)
- local event log contents [2-97](#)

- PEP information [2-111](#)
- public RSA keys [2-118](#)
- sensor trusted hosts [2-128](#)
- server TLS certificate fingerprint [2-127](#)
- specific number of lines on screen [2-138](#)
- SSH server host key [2-120](#)
- statistics [2-122](#)
- system clock [2-94](#)
- user information [2-129](#)
- version information [2-131](#)
- display-serial
 - described [2-31](#)
 - examples [2-31](#)
 - using [2-31](#)
- downgrade
 - described [2-32](#)
 - examples [2-32](#)
 - related commands [2-32](#)

E

- end
 - described [2-33](#)
 - examples [2-33](#)
- entering
 - global configuration [2-22](#)
 - service configuration mode [2-68](#)
- erase
 - described [2-34](#)
 - examples [2-34](#)
 - syntax [2-34](#)
 - using [2-34](#)
- erase ad-knowledge-base
 - described [2-35](#)
 - examples [2-35](#)
 - syntax [2-35](#)
 - using [2-35](#)
- erase license-key
 - described [2-37](#)

- examples [2-37](#)
- using [2-37](#)
- error events viewing [2-97](#)
- error messages
 - described [A-1](#)
 - validation [A-4](#)
- event-action-rules name described [2-68](#)
- event log viewing contents of [2-97](#)
- events
 - clearing [2-17](#)
 - deleting [2-17](#)
- Event Store clearing events [2-17, 2-102](#)
- exit
 - described [2-38](#)
 - examples [2-38](#)
 - using [2-38](#)
- exiting
 - configuration mode [2-33, 2-38](#)
 - submodes [2-33](#)

F

- files
 - anomaly detection
 - loading [2-4](#)
 - saving [2-5](#)

G

- generating
 - server host key [2-135](#)
 - X.509 certificate [2-139](#)
- generic commands [1-7](#)

H

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

using [1-2](#)

I

initializing the sensor [2-72](#)

iplog

described [2-39](#)

examples [2-40](#)

related commands [2-40](#)

syntax [2-39](#)

using [2-39](#)

iplog-status

described [2-41](#)

examples [2-42](#)

syntax [2-41](#)

using [2-41](#)

IP packet display route [2-142](#)

K

keywords

default [1-8](#)

no [1-8](#)

L

limitations for concurrent CLI sessions [1-1](#)

list component-configurations

described [2-43](#)

examples [2-43](#)

using [2-43](#)

locking user accounts [2-6](#)

M

modifying

privilege level [2-63](#)

terminal properties for a login session [2-138](#)

monitoring viewer privileges [1-2](#)

more exclude

described [2-50](#)

examples [2-50](#)

related commands [2-53](#)

syntax [2-50](#)

using [2-50](#)

more include

described [2-54](#)

related commands [2-55](#)

syntax [2-54](#)

N

network connectivity testing for [2-61](#)

O

operator privileges [1-2](#)

output

clearing current line [1-3](#)

displaying [1-3](#)

setting number of lines to display [2-138](#)

P

packet

described [2-56](#)

examples [2-57](#)

related commands [2-58](#)

syntax [2-56](#)

using [2-57](#)

password

changing [2-59](#)

described [2-59](#)

examples [2-60](#)

related commands [2-60](#)

syntax [2-59](#)

- updating [2-59](#)
- using [2-59](#)
- ping
 - described [2-61](#)
 - examples [2-61](#)
 - syntax [2-61](#)
 - using [2-61](#)
- platforms concurrent CLI sessions [1-1](#)
- privilege
 - described [2-63](#)
 - examples [2-63](#)
 - modifying [2-63](#)
 - related commands [2-63](#)
 - syntax [2-63](#)
- prompts default input [1-2](#)

R

- recall
 - help and tab completion [1-3](#)
 - using [1-3](#)
- recover
 - described [2-64](#)
 - examples [2-64](#)
 - syntax [2-64](#)
 - using [2-64](#)
- regular expression syntax
 - described [1-5](#)
 - table [1-6](#)
- removing
 - service packs [2-32](#)
 - signature updates [2-32](#)
- rename ad-knowledge-base
 - described [2-66](#)
 - examples [2-66](#)
 - syntax [2-66](#)
 - using [2-66](#)
- reset
 - described [2-67](#)

- examples [2-67](#)
- syntax [2-67](#)
- using [2-67](#)
- route displaying IP packet [2-142](#)

S

- service
 - analysis-engine [2-68](#)
 - anomaly-detection name [2-68](#)
 - authentication [2-68](#)
 - described [2-68](#)
 - event-action-rules name [2-68](#)
 - examples [2-70](#)
 - external-product-interface [2-68](#)
 - host [2-68](#)
 - interface [2-68](#)
 - logger [2-68](#)
 - network-access [2-68](#)
 - notification [2-68](#)
 - privileges [1-2](#)
 - role [1-2](#)
 - signature-definition name [2-68](#)
 - ssh-known-hosts [2-68](#)
 - syntax [2-68](#)
 - trusted-certificate [2-68](#)
 - using [1-2, 2-70](#)
 - web-server [2-68](#)
- setting the system clock [2-21](#)
- setup
 - clock setting parameters (table) [2-74](#)
 - described [2-72](#)
 - examples [2-74](#)
 - using [2-73](#)
- show begin
 - described [2-92](#)
 - examples [2-92](#)
 - syntax [2-92](#)
 - using [2-92](#)

- show clock
 - authoritative flags [2-94](#)
 - described [2-94](#)
 - examples [2-94](#)
 - syntax [2-94](#)
 - using [2-94](#)
- show events
 - described [2-97](#)
 - examples [2-98](#)
 - syntax [2-97](#)
 - using [2-98](#)
- show exclude
 - described [2-99](#)
 - examples [2-99](#)
 - related commands [2-101](#)
 - syntax [2-99](#)
 - using [2-99](#)
- show history
 - described [2-103](#)
 - examples [2-103](#)
 - using [2-103](#)
- show include
 - described [2-104](#)
 - examples [2-104](#)
 - related commands [2-104](#)
 - using [2-104](#)
- show inspection-load
 - described [2-106](#)
 - examples [2-106](#)
 - using [2-106](#)
- show interfaces
 - described [2-109](#)
 - examples [2-110](#)
 - syntax [2-109](#)
 - using [2-109](#)
- show inventory
 - described [2-111](#)
 - examples [2-111](#)
 - using [2-111](#)
- show privilege
 - described [2-114](#)
 - examples [2-114](#)
 - related commands [2-114](#)
 - using [2-114](#)
- show settings
 - described [2-115](#)
 - examples [2-115](#)
 - syntax [2-115](#)
- show ssh authorized-keys
 - described [2-118](#)
 - examples [2-118](#)
 - related commands [2-119](#)
 - syntax [2-118](#)
 - using [2-118](#)
- show ssh host-keys
 - described [2-121](#)
 - examples [2-121](#)
 - related commands [2-121](#)
 - syntax [2-121](#)
 - using [2-121](#)
- show ssh server-key
 - described [2-120](#)
 - examples [2-120](#)
 - related commands [2-120](#)
- show statistics
 - described [2-122](#)
 - syntax [2-122](#)
- show tech-support
 - described [2-125](#)
 - examples [2-126](#)
 - syntax [2-125](#)
 - using [2-125](#)
- show tls fingerprint
 - described [2-127](#)
 - examples [2-127](#)
 - related commands [2-127](#)
- show tls trusted-hosts
 - described [2-128](#)

- examples [2-128](#)
- related commands [2-128](#)
- syntax [2-128](#)
- using [2-128](#)
- show users
 - described [2-129](#)
 - examples [2-129](#)
 - related commands [2-130](#)
 - syntax [2-129](#)
 - using [2-129](#)
- show version
 - described [2-131](#)
 - examples [2-131](#)
 - using [2-131](#)
- signature-definition name described [2-68](#)
- ssh authorized-key
 - described [2-133](#)
 - examples [2-133](#)
 - related commands [2-134](#)
 - syntax [2-133](#)
 - using [2-133](#)
- ssh generate-key
 - described [2-135](#)
 - examples [2-135](#)
 - related commands [2-135](#)
 - using [2-135](#)
- ssh host-key
 - described [2-136](#)
 - examples [2-137](#)
 - related commands [2-137](#)
 - syntax [2-136](#)
 - using [2-136](#)
- starting IP logging [2-39](#)
- statistics
 - clearing [2-122](#)
 - viewing [2-122](#)
- status events viewing [2-97](#)
- syntax case sensitivity [1-3](#)
- System Configuration Dialog [2-73](#)

- system information exporting to FTP or SCP server [2-125](#)
- system viewing status [2-125](#)

T

- tab completion using [1-3](#)
- tech support
 - viewing
 - control transaction responses [2-125](#)
 - current configuration information [2-125](#)
 - debug logs [2-125](#)
 - version [2-125](#)
- terminal
 - described [2-138](#)
 - examples [2-138](#)
 - syntax [2-138](#)
 - using [2-138](#)
- terminating a CLI session [2-18](#)
- tls generate-key
 - described [2-139](#)
 - examples [2-139](#)
 - related commands [2-139](#)
- tls trusted-host
 - described [2-140](#)
 - examples [2-140](#)
 - related commands [2-141](#)
 - syntax [2-140](#)
 - using [2-140](#)
- trace
 - described [2-142](#)
 - examples [2-142](#)
 - using [2-142](#)

U

- unlocking user accounts [2-145](#)
- unlock user
 - described [2-145](#)

- examples [2-145](#)
 - related commands [2-145](#)
 - syntax [2-145](#)
 - using [2-145](#)
- updating the password [2-59](#)
- upgrade
 - described [2-143](#)
 - examples [2-144](#)
 - syntax [2-143](#)
 - using [2-143](#)
- upgrading the system [2-143](#)
- username
 - described [2-146](#)
 - examples [2-146](#)
 - related commands [2-147](#)
 - syntax [2-146](#)
 - using [2-146](#)
- user roles
 - administrator [1-1](#)
 - operator [1-1](#)
 - service [1-1](#)
 - viewer [1-1](#)
- using
 - anomaly detection file [2-5](#)
 - banner login [2-7](#)
 - clear denied-attackers [2-15, 2-29](#)
 - clear os-identification [2-20](#)
 - copy ad-knowledge-base [2-26](#)
 - copy instance [2-28](#)
 - erase ad-knowledge-base [2-35](#)
 - erase license-key [2-37](#)
 - list component-configurations [2-43](#)
 - rename ad-knowledge-base [2-66](#)
 - show inspection-load [2-106](#)
- viewing
 - alerts [2-97](#)
 - block requests [2-97](#)
 - error events [2-97](#)
 - IPS processes [2-131](#)
 - operating system [2-131](#)
 - signature packages [2-131](#)
 - status events [2-97](#)

V

- validation error messages described [A-4](#)
- viewer privileges [1-2](#)