



INDEX

A

adding

- an entry to the known hosts table [2-123](#)
- a public key [2-120](#)
- a trusted host [2-127](#)

administrator privileges [1-1](#)

alerts viewing [2-88](#)

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 [2-61](#)

anomaly-detection save

- described [2-5](#)
- examples [2-5](#)
- syntax [2-5](#)

application partition reimaging [2-57](#)

applying

- service packs [2-130](#)
- signature updates [2-130](#)

attacker IP address deleting [2-13](#)

using [2-6](#)

banner message creating [2-6](#)

block requests viewing [2-88](#)

C

capturing

live traffic [2-49](#)

changing the password [2-52](#)

clear denied-attackers

- described [2-13](#)
- examples [2-13, 2-27](#)
- syntax [2-13, 2-27](#)
- using [2-13, 2-27](#)

clear events

- described [2-15](#)
- examples [2-15, 2-92](#)
- using [2-92](#)

clear line

- described [2-16](#)
- examples [2-16](#)
- syntax [2-16](#)
- using [2-16](#)

clear os-identification

- described [2-18](#)
- examples [2-18](#)
- syntax [2-18](#)
- using [2-18](#)

CLI

command line editing [1-4](#)

command modes [1-5](#)

default keywords [1-8](#)

error messages [A-1](#)

B

banner login

- described [2-6](#)
- examples [2-6](#)
- syntax [2-6](#)

- 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 [2-19](#)
 - examples [2-19](#)
 - syntax [2-19](#)
 - using [2-19](#)
- closing an active terminal session [2-35](#)
- 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 [2-93](#)
- configure
 - described [2-20](#)
 - examples [2-20](#)
 - syntax [2-20](#)
 - using [2-20](#)
- copy
 - described [2-21](#)
 - examples [2-22](#)
 - syntax [2-21](#)
 - using [2-21](#)

- copy ad-knowledge-base
 - described [2-24](#)
 - examples [2-25](#)
 - syntax [2-24](#)
 - using [2-24](#)
- copying
 - configuration files [2-21](#)
 - iplogs [2-21](#)
- copy instance
 - described [2-26](#)
 - examples [2-26](#)
 - syntax [2-26](#)
 - using [2-26](#)
- creating
 - banner message [2-6](#)
 - users [2-132](#)
- Ctrl-N [1-3](#)
- Ctrl-P [1-3](#)

D

- default keywords using [1-8](#)
- deleting a logical file [2-32](#)
- denied attackers deleting [2-13](#)
- directing output to the serial connection [2-29](#)
- displaying
 - current level of privilege [2-101](#)
 - current system status [2-112](#)
 - interface statistics [2-96](#)
 - IP log contents [2-38](#)
 - IP packet route [2-129](#)
 - known hosts table [2-108](#)
 - live traffic [2-49](#)
 - local event log contents [2-88](#)
 - PEP information [2-98](#)
 - public RSA keys [2-105](#)
 - sensor trusted hosts [2-115](#)
 - server TLS certificate fingerprint [2-114](#)
 - specific number of lines on screen [2-125](#)

- SSH server's host key [2-107](#)
- statistics [2-109](#)
- system clock [2-85](#)
- user information [2-116](#)
- version information [2-118](#)

display-serial

- described [2-29](#)
- examples [2-29](#)
- using [2-29](#)

downgrade

- described [2-30](#)
- examples [2-30](#)
- related commands [2-30](#)

E

end

- described [2-31](#)
- examples [2-31](#)

entering

- global configuration [2-20](#)
- service configuration mode [2-61](#)

erase

- described [2-32](#)
- examples [2-32](#)
- syntax [2-32](#)
- using [2-32](#)

erase ad-knowledge-base

- described [2-33](#)
- examples [2-33](#)
- syntax [2-33](#)
- using [2-33](#)

error events viewing [2-88](#)

error messages

- described [A-1](#)
- validation [A-4](#)

event-action-rules name described [2-61](#)

event log viewing contents [2-88](#)

events

- clearing [2-15](#)
- deleting [2-15](#)

Event Store

- clearing events [2-15](#)

Event Store clearing events [2-15, 2-92](#)

exit

- described [2-35](#)
- examples [2-35](#)
- using [2-35](#)

exiting

- configuration mode [2-31, 2-35](#)
- submodes [2-31](#)

F

files

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

G

generating

- server host key [2-122](#)
- X.509 certificate [2-126](#)

generic commands [1-7](#)

H

help

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

I

initializing the sensor [2-64](#)

iplog
 described [2-36](#)
 examples [2-37](#)
 related commands [2-37](#)
 syntax [2-36](#)
 using [2-36](#)

iplog-status
 described [2-38](#)
 examples [2-39](#)
 syntax [2-38](#)
 using [2-38](#)

IP packet display route [2-129](#)

K

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

L

limitations for concurrent CLI sessions [1-1](#)
 list component-configurations
 described [2-40](#)
 examples [2-40](#)
 using [2-40](#)

M

modifying
 privilege level [2-56](#)
 terminal properties for a login session [2-125](#)
 monitoring viewer privileges [1-2](#)
 more exclude
 described [2-45](#)
 examples [2-45](#)
 related commands [2-46](#)
 syntax [2-45](#)

using [2-45](#)
 more include
 described [2-47](#)
 related commands [2-48](#)
 syntax [2-47](#)

N

network connectivity testing [2-54](#)

O

operator privileges [1-2](#)
 output
 clearing current line [1-3](#)
 displaying [1-3](#)
 setting number of lines to display [2-125](#)

P

packet
 described [2-49](#)
 examples [2-50](#)
 related commands [2-51](#)
 syntax [2-49](#)
 using [2-50](#)
 password
 changing [2-52](#)
 described [2-52](#)
 examples [2-53](#)
 related commands [2-53](#)
 syntax [2-52](#)
 updating [2-52](#)
 using [2-52](#)
 ping
 described [2-54](#)
 examples [2-54](#)
 syntax [2-54](#)

- using [2-54](#)
- platforms concurrent CLI sessions [1-1](#)
- privilege
 - described [2-56](#)
 - examples [2-56](#)
 - modifying [2-56](#)
 - related commands [2-56](#)
 - syntax [2-56](#)
- prompts default input [1-2](#)

R

- recall
 - help and tab completion [1-3](#)
 - using [1-3](#)
- recover
 - described [2-57](#)
 - examples [2-57](#)
 - syntax [2-57](#)
 - using [2-57](#)
- regular expression syntax
 - described [1-5](#)
 - table [1-6](#)
- removing
 - service packs [2-30](#)
 - signature updates [2-30](#)
- rename ad-knowledge-base
 - described [2-59](#)
 - examples [2-59](#)
 - syntax [2-59](#)
 - using [2-59](#)
- reset
 - described [2-60](#)
 - examples [2-60](#)
 - syntax [2-60](#)
 - using [2-60](#)
- route of IP packet [2-129](#)

S

- service
 - analysis-engine [2-61](#)
 - anomaly-detection name [2-61](#)
 - authentication [2-61](#)
 - described [2-61](#)
 - event-action-rules name [2-61](#)
 - examples [2-63](#)
 - external-product-interface [2-61](#)
 - host [2-61](#)
 - interface [2-61](#)
 - logger [2-61](#)
 - network-access [2-61](#)
 - notification [2-61](#)
 - privileges [1-2](#)
 - role [1-2](#)
 - signature-definition name [2-61](#)
 - ssh-known-hosts [2-61](#)
 - syntax [2-61](#)
 - trusted-certificate [2-61](#)
 - using [1-2, 2-62](#)
 - web-server [2-61](#)
- service account privileges [1-2](#)
- setting the system clock [2-19](#)
- setup
 - clock setting parameters (table) [2-65](#)
 - described [2-64](#)
 - examples [2-66](#)
 - using [2-65](#)
- show begin
 - described [2-83](#)
 - examples [2-83](#)
 - syntax [2-83](#)
 - using [2-83](#)
- show clock
 - authoritative flags [2-85](#)
 - described [2-85](#)
 - examples [2-85](#)

- syntax [2-85](#)
- using [2-85](#)
- show events
 - described [2-88](#)
 - examples [2-89](#)
 - syntax [2-88](#)
 - using [2-89](#)
- show exclude
 - described [2-90](#)
 - examples [2-90](#)
 - related commands [2-91](#)
 - syntax [2-90](#)
 - using [2-90](#)
- show history
 - described [2-93](#)
 - examples [2-93](#)
 - using [2-93](#)
- show include
 - described [2-94](#)
 - examples [2-94](#)
 - related commands [2-94](#)
 - using [2-94](#)
- show interfaces
 - described [2-96](#)
 - examples [2-97](#)
 - syntax [2-96](#)
 - using [2-96](#)
- show inventory
 - described [2-98](#)
 - examples [2-98](#)
 - using [2-98](#)
- show privilege
 - described [2-101](#)
 - examples [2-101](#)
 - related commands [2-101](#)
 - using [2-101](#)
- show settings
 - described [2-102](#)
 - examples [2-102](#)
- syntax [2-102](#)
- show ssh authorized-keys
 - described [2-105](#)
 - examples [2-105](#)
 - related commands [2-106](#)
 - syntax [2-105](#)
 - using [2-105](#)
- show ssh host-keys
 - described [2-108](#)
 - examples [2-108](#)
 - related commands [2-108](#)
 - syntax [2-108](#)
 - using [2-108](#)
- show ssh server-key
 - described [2-107](#)
 - examples [2-107](#)
 - related commands [2-107](#)
- show statistics
 - described [2-109](#)
 - syntax [2-109](#)
- show tech-support
 - described [2-112](#)
 - examples [2-113](#)
 - syntax [2-112](#)
 - using [2-112](#)
- show tls fingerprint
 - described [2-114](#)
 - examples [2-114](#)
 - related commands [2-114](#)
- show tls trusted-hosts
 - described [2-115](#)
 - examples [2-115](#)
 - related commands [2-115](#)
 - syntax [2-115](#)
 - using [2-115](#)
- show users
 - described [2-116](#)
 - examples [2-116](#)
 - related commands [2-117](#)

- syntax [2-116](#)
 - using [2-116](#)
- show version
 - described [2-118](#)
 - examples [2-118](#)
 - using [2-118](#)
- signature-definition name described [2-61](#)
- ssh authorized-key
 - described [2-120](#)
 - examples [2-120](#)
 - related commands [2-121](#)
 - syntax [2-120](#)
 - using [2-120](#)
- ssh generate-key
 - described [2-122](#)
 - examples [2-122](#)
 - related commands [2-122](#)
 - using [2-122](#)
- ssh host-key
 - described [2-123](#)
 - examples [2-124](#)
 - related commands [2-124](#)
 - syntax [2-123](#)
 - using [2-123](#)
- starting IP logging [2-36](#)
- statistics
 - clearing [2-109](#)
 - viewing [2-109](#)
- status events viewing [2-88](#)
- syntax case sensitivity [1-3](#)
- System Configuration Dialog [2-65](#)
- system information exporting to FTP or SCP server [2-112](#)
- system viewing status [2-112](#)

T

- tab completion using [1-3](#)
- tech support
 - viewing
 - control transaction responses [2-112](#)
 - current configuration information [2-112](#)
 - debug logs [2-112](#)
 - version [2-112](#)
- terminal
 - described [2-125](#)
 - examples [2-125](#)
 - syntax [2-125](#)
 - using [2-125](#)
- terminating a CLI session [2-16](#)
- tls generate-key
 - described [2-126](#)
 - examples [2-126](#)
 - related commands [2-126](#)
- tls trusted-host
 - described [2-127](#)
 - examples [2-127](#)
 - related commands [2-128](#)
 - syntax [2-127](#)
 - using [2-127](#)
- trace
 - described [2-129](#)
 - examples [2-129](#)
 - using [2-129](#)

U

- updating the password [2-52](#)
- upgrade
 - described [2-130](#)
 - examples [2-131](#)
 - syntax [2-130](#)
 - using [2-130](#)
- upgrading the system [2-130](#)

username

- described [2-132](#)
- examples [2-132](#)
- related commands [2-133](#)
- syntax [2-132](#)
- using [2-132](#)

user roles

- administrator [1-1](#)
- operator [1-1, 1-2](#)
- service [1-1](#)
- viewer [1-1](#)

using

- anomaly detection file [2-5](#)
- banner login [2-6](#)
- clear denied-attackers [2-13, 2-27](#)
- clear os-identification [2-18](#)
- copy ad-knowledge-base [2-24](#)
- copy instance [2-26](#)
- erase ad-knowledge-base [2-33](#)
- list component-configurations [2-40](#)
- rename ad-knowledge-base [2-59](#)

V

validation error messages

- described [A-4](#)

viewer privileges [1-2](#)

viewing

- alerts [2-88](#)
- block requests [2-88](#)
- error events [2-88](#)
- IPS processes [2-118](#)
- operating system [2-118](#)
- signature packages [2-118](#)
- status events [2-88](#)