



A

access

- allowing all hosts [2-5](#)
- creating user accounts [2-22](#)
- default 10.0.0.0 networks [2-5](#)
- permitting host or network access [2-4](#)

Administration tab [5-1](#)

advisory

- cryptographic products [1-1](#)

alarm channels

event filters

- configuring [3-6](#)
- described [3-6](#)

Event Filters page [3-6](#)

system variables

- configuring [3-3](#)
- described [3-3](#)

System Variables page [3-3](#)

alarms

- associated with an event [6-41](#)
- deleting [6-49](#)
- including notes with [6-43](#)
- status
 - acknowledged [6-42](#)

assigned [6-42](#)

closed [6-42](#)

deleted [6-42](#)

new [6-42](#)

tasks

accessing NSDB [6-41](#)

adding notes [6-41](#)

setting status [6-41](#)

viewing alarms [6-41](#)

viewing attack details [6-41](#)

viewing context [6-41](#)

viewing

average number received [6-35](#)

context data [6-43](#)

Allowed Hosts page [2-4, 3-31, 3-33](#)

Application Settings panel [6-28, 6-29](#)

archival

configuring [6-23](#)

ATOMIC.ARP engine

described [A-18](#)

parameters [A-18](#)

ATOMIC.ICMP engine

described [A-17](#)

parameters [A-19](#)

ATOMIC.IPOPTIONS engine

described [A-18](#)parameters [A-20](#)

ATOMIC.L3.IP engine

described [A-17](#)parameters [A-20](#)

ATOMIC.TCP engine

described [A-18](#)parameters [A-21](#)

ATOMIC.UDP engine

described [A-17](#)parameters [A-22](#)

ATOMIC engines

configuration restrictions [A-22](#)described [A-17](#)

authorized keys

defining [2-9](#)Authorized Keys page [2-9](#)Auto Update page [3-35](#)

B

blocking

ACL modification [3-26](#)

configuring

blocking devices [3-26](#)blocking forwarding sensors [3-33](#)logical devices [3-24](#)master blocking sensors [3-31](#)properties [3-21](#)router blocking interfaces [3-28](#)switch blocking interfaces [3-30](#)

manually blocking

hosts [5-7](#)networks [5-10](#)specifying addresses to never block [3-22](#)tasks required to configure [3-20](#)Blocking Devices page [3-26](#)

blocking forwarding sensors

configuring [3-33](#)described [3-33](#)Blocking Properties page [3-21](#)

CCat 6K Blocking Device Interfaces page [3-30](#)Certificate Information panel [6-9](#)

certificates

adding for trusted hosts [2-15](#)generating X.509 [2-17](#)Internet Explorer [1-13](#)Netscape [1-11](#)

columns

hiding [6-32](#)viewing all [6-32](#)

communication parameters

See Network Settings page

configuration
 restoring default settings [3-38](#)

Configuration tab [3-1](#)

connecting

IDS Device Manager [1-7](#)

control transaction

See CT

cookies

IDS Device Manager [1-8](#)

CT

setConfig [A-5](#)

D

data

configuring archival [6-23](#)

exporting tables to ASCII file [6-47](#)

importing [6-45](#)

sorting in tables [6-33](#)

database

managing event data [6-44](#)

default settings

restoring [3-38](#)

deleting hosts [2-4](#)

Device Properties panel [6-7](#)

Device Status panel [6-10](#)

Device tab [2-1](#)

diagnostics

generating [5-1](#)

viewing [5-1](#)

Diagnostics page [5-1](#)

E

error messages

CTs [A-16](#)

IDAPI [A-16](#)

service submode [A-15](#)

signature engines [A-15](#)

Ethereal

described [6-40](#)

moving the executable file [6-27](#)

event data

deleting [6-44](#)

exporting [6-44](#)

filtering [6-12](#)

importing [6-44](#)

specifying a source [6-31](#)

tasks for viewing [6-30](#)

viewing

in IDS Event Viewer [6-17](#)

in real time [6-37](#)

events

associated signature [6-34](#)

configuring display [4-2](#)

correcting the time [2-22](#)

graphical view [6-34](#)

viewing details [6-34](#)

Events page [4-2](#)

EventStore

described [A-4](#)

Export Database Tables panel [6-47](#)

F

Filter Properties panel [6-13](#)

filters

changing defined filters [6-16](#)

creating [6-13](#)

deleting [6-17](#)

fingerprints

viewing X.509 certificate [2-18](#)

FLOOD.HOST.ICMP engine

described [A-23](#)

parameters [A-24](#)

FLOOD.HOST.UDP engine

described [A-23](#)

parameters [A-24](#)

FLOOD.NET engine

described [A-23](#)

parameters [A-25](#)

FLOOD engines

configuration restrictions [A-26](#)

described [A-23](#)

FTP servers [3-37](#)

supported servers [3-37](#)

G

Generate Host Certificate page [2-17](#)

Generate Key page [2-11](#)

graphs

described [6-30](#)

GUI elements

IDS Device Manager [1-2](#)

H

Host Manual Blocks page [5-7](#)

hosts

adding [2-4](#)

deleting [2-4](#)

editing [2-4](#)

HTTP deobfuscation

alarms [A-30](#)

ASCII normalization [A-26](#)

characters not converted [A-27](#)

decode variations [A-27](#)

described [A-26](#)

error conditions [A-29](#)

supported decodings [A-29](#)

https

connection protocol for IDS Event
Viewer [6-9](#)

IDS Device Manager

accessing from IDS Event Viewer [6-12](#)

applications

starting [1-9](#)

stopping [1-9](#)

certificates [1-9](#)

connecting [1-7](#)

cookies [1-8](#)

GUI elements [1-2](#)

initializing sensors [1-7](#)

installing [1-6](#)

introducing [1-2](#)

system requirements [1-6](#)

validating

Internet Explorer certificate
fingerprints [1-13](#)

Netscape certificate fingerprints [1-11](#)

IDS Event Viewer

applications

specifying Ethernet location [6-27](#)

specifying NSDB folder location [6-28](#)

specifying web browser location [6-25](#)

installing [6-4](#)

introducing [6-1](#)

Import Log Files panel [6-45](#)

initializing sensors [1-7](#)

IDS Device Manager [1-7](#)

installing

IDS Device Manager [1-6](#)

IDS Event Viewer [6-4](#)

Internet Explorer

validating certificate fingerprints [1-13](#)

IP logging

configuring sensors to log IP traffic [5-5](#)

IP Logging page [5-5](#)

IP logs

downloading from IDS Device Manager [4-1](#)

IP Logs page [4-1](#)

K

Key Modulus Length

definition of [2-14](#)

keys

defining authorized keys [2-9](#)

SSH host [2-11](#)

known hosts tables

updating with new keys [2-12](#)

L

log files

importing into IDS Event Viewer [6-45](#)

logging in

restrictions in IDS Device Manager [2-22](#)

user accounts [2-22](#)

using a service account to bypass CLI [2-23](#)

logical devices

- configuring [3-24](#)
- described [3-24](#)

Logical Devices page [3-24](#)

M

master blocking sensors

- configuring [3-31](#)
- described [3-31](#)

MASTER engine

- configuration restrictions [A-5](#)
- parameters [A-5](#), [A-9](#)

Monitoring tab [4-1](#)

N

NAC

- role in blocking [3-21](#)

Netscape

- validating certificate fingerprints [1-11](#)

Network Access Controller

- See NAC

Network Manual Blocks page [5-10](#)

Network Security Database

- See NSDB

Network Settings page [2-2](#)

Never Block Addresses page [3-22](#)

notes

- adding to alarm data [6-43](#)

NSDB

- accessing [6-44](#)
- moving location of files [6-28](#)

O

OTHER engine

- described [A-30](#)
- parameters [A-32](#)
- signature list [A-31](#)

P

powering down the sensor [5-12](#)

Preferences panel [6-21](#)

R

Realtime Dashboard

- clearing events from [6-38](#)
- configuring [6-39](#)
- viewing events from [6-38](#)

Realtime Dashboard Properties panel [6-39](#)

Realtime Graph

- (figure) [6-35](#)
- described [6-35](#)

- refresh
 - specifying refresh cycles [6-21](#)
 - Refresh Cycle tab [6-21](#)
 - Regex
 - patterns [A-14](#)
 - syntax [A-13](#)
 - Regular Expression
 - See [Regex](#)
 - remote access
 - disabling Telnet [2-8](#)
 - enabling Telnet [2-8](#)
 - Remote Access page [2-8](#)
 - resetting the sensor [5-12](#)
 - Restore Defaults page [3-38](#)
 - Router Blocking Device Interfaces page [3-28](#)
 - RSA authentication
 - generation tool [2-9](#)
-
- S
- Secure Shell
 - See [SSH](#)
 - Sensing Engine page [3-1](#)
 - sensors
 - allowing host or network access to [2-4](#)
 - changing
 - communication parameters [2-2](#)
 - settings used in IDS Event Viewer [6-10](#)
 - configuring automatic updates [3-36](#)
 - determining status in IDS Event Viewer [6-10](#)
 - establishing connection to view events [6-7](#)
 - initializing [2-1](#)
 - powering down [5-12](#)
 - removing from list of monitored devices [6-10](#)
 - resetting [5-12](#)
 - unable to connect to IDS Event Viewer [6-9](#)
 - updating [5-4](#)
 - Server Certificate page [2-18](#)
 - SERVICE.DNS engine
 - described [A-34](#)
 - parameters [A-34](#)
 - SERVICE.FTP engine
 - described [A-34](#)
 - parameters [A-35](#)
 - SERVICE.GENERIC engine
 - described [A-34](#), [A-36](#)
 - parameters [A-36](#)
 - SERVICE.HTTP engine
 - described [A-37](#)
 - HTTP field sections [A-38](#)
 - limitations and restrictions [A-40](#)
 - parameters [A-41](#)
 - Regex [A-37](#)
 - string match length [A-39](#)
 - SERVICE.IDENT engine
 - described [A-34](#), [A-42](#)
 - parameters [A-42](#)

- SERVICE.MSSQL engine
 - described [A-43](#)
 - parameters [A-43](#)
 - SERVICE.NTP engine
 - described [A-44](#)
 - parameters [A-44](#)
 - SERVICE.RPC engine
 - described [A-44](#)
 - parameters [A-44](#)
 - SERVICE.SMB engine
 - described [A-46](#)
 - parameters [A-46](#)
 - signature list [A-46](#)
 - SERVICE.SMTP engine
 - transitions [A-54](#)
 - SERVICE.SNMP engine
 - described [A-47](#)
 - limitations [A-48](#)
 - parameters [A-48](#)
 - SERVICE.SSH engine
 - described [A-34, A-49](#)
 - parameters [A-49](#)
 - SERVICE engines
 - configuration restrictions [A-34](#)
 - described [A-33](#)
 - service packs
 - applying [5-4](#)
 - signature 993
 - description [3-19](#)
 - parameters [3-19](#)
 - signature engines
 - ATOMIC.ARP [A-18](#)
 - parameters [A-18](#)
 - ATOMIC.ICMP [A-17](#)
 - parameters [A-19](#)
 - ATOMIC.IPOPTIONS [A-18](#)
 - parameters [A-20](#)
 - ATOMIC.L3.IP [A-17](#)
 - parameters [A-20](#)
 - ATOMIC.TCP [A-18](#)
 - parameters [A-21](#)
 - ATOMIC.UDP [A-17](#)
 - parameters [A-22](#)
 - configuration parsing [A-5](#)
 - described [A-2](#)
 - error messages [A-15](#)
 - CTs [A-16](#)
 - IDAPI [A-16](#)
 - service submode [A-15](#)
- FLOOD [A-23](#)
- FLOOD.HOST.ICMP [A-23](#)
 - parameters [A-24](#)
- FLOOD.HOST.UDP [A-23](#)
 - parameters [A-24](#)
- FLOOD.NET [A-23](#)
 - parameters [A-25](#)
- handling alarms [A-4](#)
- MASTER [A-9](#)

- OTHER
 - described [A-30](#)
 - parameters [A-32](#)
 - signature list [A-31](#)
- Regex
 - patterns [A-14](#)
 - syntax [A-13](#)
- SERVICE
 - described [A-33](#)
- SERVICE.DNS
 - described [A-34](#)
 - parameters [A-34](#)
- SERVICE.FTP
 - described [A-34](#)
 - parameters [A-35](#)
- SERVICE.GENERIC
 - described [A-34](#), [A-36](#)
 - parameters [A-36](#)
- SERVICE.HTTP
 - described [A-37](#)
 - field sections [A-38](#)
 - limitations and restrictions [A-40](#)
 - parameters [A-41](#)
 - Regex [A-37](#)
 - string match length [A-39](#)
- SERVICE.IDENT
 - described [A-34](#), [A-42](#)
 - parameters [A-42](#)
- SERVICE.MSSQL
 - described [A-43](#)
 - parameters [A-43](#)
- SERVICE.NTP
 - described [A-44](#)
 - parameters [A-44](#)
- SERVICE.RPC
 - described [A-44](#)
 - parameters [A-44](#)
- SERVICE.SMB
 - described [A-46](#)
 - parameters [A-46](#)
 - signature list [A-46](#)
- SERVICE.SMTP
 - transitions [A-54](#)
- SERVICE.SNMP
 - described [A-47](#)
 - limitations [A-48](#)
 - parameters [A-48](#)
- SERVICE.SSH
 - described [A-34](#), [A-49](#)
 - parameters [A-49](#)
- STATE.STRING
 - described [A-50](#)
 - limitations [A-52](#)
 - parameters [A-52](#)
- STATE.STRING.CISCOLOGIN
 - transitions [A-55](#)

- STATE.STRING.LPRFORMAT
 - transitions [A-56](#)
- STATE machine engines
 - predefined state machines [A-53](#)
 - transition parameters [A-54](#)
- STRING
 - described [A-56](#)
 - limitations [A-58](#)
 - parameters [A-57](#)
 - Regex [A-56](#)
 - string match length [A-57](#)
- Summarizer [A-6](#)
- SWEEP
 - configuration restrictions [A-60](#)
 - described [A-59](#)
- SWEEP.HOST.ICMP
 - parameters [A-60](#)
- SWEEP.HOST.TCP
 - parameters [A-61](#)
- SWEEP.MULTI
 - described [A-59](#)
 - parameters [A-61](#)
- SWEEP.OTHER.TCP
 - described [A-59](#)
 - parameters [A-62](#)
- SWEEP.PORT.TCP
 - parameters [A-63](#)
- SWEEP.PORT.UDP
 - parameters [A-64](#)
- SYSLOG
 - described [A-64](#)
 - parameters [A-64](#)
- TRAFFIC.ICMP
 - described [A-65](#)
 - parameters [A-66](#)
- TROJAN
 - described [A-65](#)
- signatures
 - about [3-2](#)
 - applying signature updates [5-4](#)
 - automatic updates [3-35](#)
 - built-in [3-3](#)
 - custom [3-3](#)
 - disabling [3-13](#)
 - editing [3-13](#)
 - enabling [3-13](#)
 - false positives [3-2](#)
 - groups [3-12](#)
 - subsignatures [3-3](#)
 - tuned [3-3](#)
 - tuning [3-12](#)
 - viewing [3-12](#)
 - viewing descriptions of [6-44](#)
- signature updates
 - applying [5-4](#)
- SSH
 - connecting to sensor [1-12](#)

- SSH keys
 - configuring [2-12](#)
 - generated on startup [2-11](#)
 - generating [2-11](#)
- SSH Known Host Keys page [2-12](#)
- starting applications
 - IDS Device Manager [1-9](#)
- starting the software
 - IDS Event Viewer [6-6](#)
- STATE.STRING.CISCOLOGIN engine
 - transitions [A-55](#)
- STATE.STRING.LPRFORMAT engine
 - transitions [A-56](#)
- STATE.STRING engine
 - described [A-50](#)
 - limitations [A-52](#)
 - parameters [A-52](#)
- STATE machine engines
 - predefined state machines [A-53](#)
 - transition parameters [A-54](#)
- Statistical Graph
 - (figure) [6-36](#)
 - described [6-35](#)
- statistics
 - list [4-4](#)
 - viewing in IDS Device Manager [4-4](#)
- Statistics page [4-4](#)
- stopping applications
 - IDS Device Manager [1-9](#)
- STRING engines
 - described [A-56](#)
 - limitations [A-58](#)
 - parameters [A-57](#)
 - Regex [A-56](#)
 - string match length [A-57](#)
- Summarizer
 - event aggregation [A-6](#)
- SWEEP.HOST.ICMP engine
 - parameters [A-60](#)
- SWEEP.HOST.TCP engine
 - parameters [A-61](#)
- SWEEP.MULTI engine
 - described [A-59](#)
 - parameters [A-61](#)
- SWEEP.OTHER.TCP engine
 - described [A-59](#)
 - parameters [A-62](#)
- SWEEP.PORT.TCP engine
 - parameters [A-63](#)
- SWEEP.PORT.UDP engine
 - parameters [A-64](#)
- sweep attack
 - viewing details [6-43](#)
- SWEEP engines
 - configuration restrictions [A-60](#)
 - described [A-59](#)
- SYSLOG engine
 - described [A-64](#)

- parameters [A-64](#)
- System Control page [5-12](#)
- system information
 - viewing
 - interface information [5-3](#)
 - resource usage [5-3](#)
 - software version [5-3](#)
 - status of applications [5-3](#)
 - TAC contact information [5-3](#)
- System Information page [5-3](#)
- system requirements
 - IDS Device Manager [1-6](#)
 - IDS Event Viewer [6-2](#)

T

- tables
 - described [6-30](#)
 - exporting from IDS Event Viewer [6-47](#)
 - removing from list of data sources [6-48](#)
 - sorting columns [6-33](#)
- task list
 - alarms [6-41](#)
 - application settings [6-25](#)
 - database administration [6-44](#)
 - devices [6-6](#)
 - event data [6-30](#)
 - filters [6-12](#)
 - IDS Event Viewer [6-2](#)

- refreshes [6-21](#)
- views [6-17](#)
- TCP
 - viewing binary traffic for alarm [6-43](#)
- Telnet
 - enabling access sensors [2-8](#)
- time
 - defining for the sensor [2-19](#)
 - event timestamps [2-22](#)
 - incorrect setting [2-22](#)
- Time page [2-19](#)
- TLS
 - certificates [1-9](#)
 - described [1-9, 2-4](#)
 - enabling [2-3](#)
 - handshaking [1-10](#)
- TRAFFIC.ICMP engine
 - described [A-65](#)
 - parameters [A-66](#)
- traffic oversubscription [3-19](#)
- Transport Layer Security
 - See TLS
- TROJAN engines
 - described [A-65](#)
- troubleshooting
 - accessing Cisco Technical Support website [5-3](#)
 - viewing sensor diagnostics [5-1](#)
- Trusted Hosts page [2-15](#)

U

uninstalling IDS Event Viewer 3.1 [6-5](#)

Update page [5-4](#)

updates

 automatic [3-35](#)

 downloading to FTP server [5-4](#)

upgrading from 3.1

 uninstalling 3.1 [6-5](#)

 warning [6-4](#)

users

 types of access [2-23](#)

Users Page [2-22](#)

V

views

 changing defined views [6-20](#)

 closing [6-33](#)

 creating [6-18](#)

 displaying several [6-33](#)

 refreshing

 after change [6-29](#)

 view contents [6-21](#)

 removing defined views [6-21](#)

View Wizard [6-18](#)

Virtual Sensor Configuration

 Sensor Configuration Mode page [3-12](#)

 System Variables page [3-9](#)

virtual sensors

 configuring [3-12](#)

 description [3-12](#)

 system variables

 configuring [3-9](#)

 description [3-9](#)

W

web server port

 default for IDS Device Manager [2-4](#)

X

X.509 [2-17](#)

