



INDEX

Numerics

- 4GE bypass interface card
 - configuration restrictions [5-10](#)
 - described [5-10](#)
- 802.1q encapsulation
 - VLAN groups [5-15](#)

A

- accessing IPS software [19-2](#)
- access lists
 - misconfiguration [C-29](#)
 - necessary hosts [3-3](#)
- ACLs
 - adding [3-3](#)
 - described [12-2](#)
 - Post-Block [12-17, 12-18](#)
 - Pre-Block [12-17, 12-18](#)
- Active Host Blocks pane
 - field descriptions [16-6](#)
 - user roles [16-6](#)
- ad0 pane
 - default [10-10](#)
 - described [10-10](#)
 - tabs [10-10](#)
- Add ACL Entry dialog box field descriptions [3-3](#)
- Add Active Host Block dialog box field descriptions [16-7](#)
- Add Allowed Host dialog box
 - field descriptions [4-5](#)
 - user roles [4-4](#)
- Add Authorized Key dialog box
 - field descriptions [11-3](#)
 - user roles [11-2](#)
- Add Blocking Device dialog box
 - field descriptions [12-15](#)
 - user roles [12-14](#)
- Add Cat 6K Blocking Device Interface dialog box
 - field descriptions [12-23](#)
 - user roles [12-21](#)
- Add Configured OS Map dialog box
 - field descriptions [6-24, 9-26](#)
 - user roles [6-23, 9-23](#)
- Add Destination Port dialog box field descriptions [10-16](#)
- Add Device Login Profile dialog box
 - field descriptions [12-12](#)
 - user roles [12-12](#)
- Add Event Action Filter dialog box
 - field descriptions [6-14, 9-16](#)
 - user roles [6-13, 9-15](#)
- Add Event Action Override dialog box
 - field descriptions [6-11, 9-13](#)
 - user roles [6-11, 9-13](#)
- Add Event Variable dialog box
 - field descriptions [6-27, 9-29](#)
 - user roles [6-26, 9-28](#)
- Add External Product Interface dialog box
 - field descriptions [14-6](#)
 - user roles [14-5](#)
- Add Histogram dialog box field descriptions [10-17](#)
- adding
 - ACLs [3-3](#)
 - a host never to be blocked [12-11](#)
 - anomaly detection policies [10-9](#)
 - CSA MC interfaces [14-7](#)
 - dashboards [2-1](#)

- denied attackers [16-5](#)
- event action filters [6-15, 9-17](#)
- event action overrides [9-14](#)
- event action rules policies [9-12](#)
- event variables [6-28, 9-29](#)
- external product interfaces [14-7](#)
- gadgets [2-1](#)
- host blocks [16-7](#)
- IPv4 target value rating [6-18, 9-20](#)
- IPv6 target value rating [6-20, 9-22](#)
- network blocks [16-9](#)
- OS maps [6-25, 9-27](#)
- risk categories [6-30, 9-32](#)
- signature definition policies [7-2](#)
- signatures [7-13](#)
- signature variables [7-27](#)
- virtual sensors [3-12, 6-11](#)
- Add Inline VLAN Pair dialog box field descriptions [3-9, 5-22](#)
- Add Interface Pair dialog box field descriptions [5-20](#)
- Add IP Logging dialog box field descriptions [16-13](#)
- Add Known Host Key dialog box
 - field descriptions [11-5](#)
 - user roles [11-4](#)
- Add Master Blocking Sensor dialog box
 - field descriptions [12-25](#)
 - user roles [12-24](#)
- Add Network Block dialog box field descriptions [16-9](#)
- Add Never Block Address dialog box
 - field descriptions [12-10](#)
 - user roles [12-7](#)
- Add Policy dialog box field descriptions [7-2, 9-11, 10-9](#)
- Add Posture ACL dialog box field descriptions [14-7](#)
- Add Protocol Number dialog box field descriptions [10-18, 10-25](#)
- Add Rate Limit dialog box
 - field descriptions [16-11](#)
 - user role [16-10](#)
- Address Resolution Protocol. See ARP.
- Add Risk Level dialog box field descriptions [6-30, 9-32](#)
- Add Router Blocking Device Interface dialog box
 - field descriptions [12-19](#)
 - user roles [12-17](#)
- Add Signature dialog box field descriptions [7-7](#)
- Add Signature Variable dialog box
 - field descriptions [7-27](#)
 - user roles [7-26](#)
- Add SNMP Trap Destination dialog box field descriptions [13-4](#)
- Add Trusted Host dialog box
 - field descriptions [11-9](#)
 - user roles [11-9](#)
- Add User dialog box
 - field descriptions [4-16](#)
 - user roles [4-16](#)
- Add Virtual Sensor dialog box
 - described [3-11, 6-9](#)
 - field descriptions [3-11, 6-9](#)
- Add VLAN Group dialog box field descriptions [5-24](#)
- Advanced Alert Behavior Wizard
 - Alert Dynamic Response Fire All window field descriptions [8-25](#)
 - Alert Dynamic Response Fire Once window field descriptions [8-26](#)
 - Alert Dynamic Response Summary window field descriptions [8-26](#)
 - Alert Summarization window field descriptions [8-25](#)
 - Event Count and Interval window field descriptions [8-24](#)
 - Global Summarization window field descriptions [8-27](#)
- AIC
 - policy [7-38](#)
 - signatures (example) [7-38](#)
- AIC engine
 - AIC FTP [B-11](#)
 - AIC FTP engine parameters (table) [B-12](#)
 - AIC HTTP [B-11](#)
 - AIC HTTP engine parameters (table) [B-11](#)

- described [B-11](#)
- features [B-11](#)
- signature categories [7-30](#)
- AIC policy enforcement
 - default configuration [7-31, B-11](#)
 - described [7-31, B-10](#)
 - sensor oversubscription [7-31, B-11](#)
- AIM-IPS
 - initializing [17-12](#)
 - installing system image [20-22](#)
 - logging in [18-5](#)
 - reimaging [20-22](#)
 - session command [18-5](#)
 - sessioning [18-4, 18-5](#)
 - setup command [17-12](#)
 - time sources [4-7, C-18](#)
- AIP SCC-5
 - Normalizer engine [B-38](#)
- AIP SSC-5
 - bypass mode [5-27](#)
 - password recovery [15-6, C-10](#)
 - resetting the password [15-7, C-11](#)
- AIP-SSC-5
 - initializing [17-6](#)
 - logging in [18-6](#)
 - reimaging [20-25](#)
 - session command [18-6](#)
- AIP SSM
 - bypass mode [5-27](#)
 - Deny Connection Inline [9-10, C-73](#)
 - Deny Packet Inline [9-10, C-73](#)
 - Normalizer engine [B-38, C-72](#)
 - password recovery [15-8, C-12](#)
 - Reset TCP Connection [9-10, C-73](#)
 - resetting the password [15-8, C-13](#)
 - TCP reset packets [9-10, C-73](#)
- AIP-SSM
 - initializing [17-15](#)
 - installing system image [20-25](#)
 - logging in [18-6](#)
 - recovering [C-69](#)
 - reimaging [20-25](#)
 - resetting [C-68](#)
 - session command [18-6](#)
 - setup command [17-15](#)
 - time sources [4-7, C-19](#)
- Alarm Channel [9-6, A-26](#)
- alert and log actions (list) [9-8](#)
- alert behavior normal [8-24](#)
- alert frequency
 - aggregation [7-19](#)
 - configuring [7-19](#)
 - controlling [7-19](#)
 - modes [B-6](#)
- Allowed Hosts/Networks pane
 - configuring [4-5](#)
 - described [4-4](#)
 - field descriptions [4-5](#)
- alternate TCP reset interface [5-8](#)
- Analysis Engine
 - described [6-2](#)
 - error messages [C-26](#)
 - IDM exits [C-58](#)
 - verify it is running [C-23](#)
 - virtual sensors [6-2](#)
- anomaly detection
 - asymmetric traffic [10-2, 10-34](#)
 - caution [10-2, 10-34](#)
 - configuration sequence [10-5](#)
 - default configuration (example) [10-4](#)
 - described [10-2](#)
 - detect mode [10-4](#)
 - disabling [C-22](#)
 - event actions [10-6, B-66](#)
 - inactive mode [10-4](#)
 - learning accept mode [10-3](#)
 - learning process [10-3](#)
 - limiting false positives [10-13, 16-16](#)

- operation settings [10-11](#)
 - protocols [10-3](#)
 - signatures (table) [10-6, B-67](#)
 - turning off [10-34](#)
 - worms
 - attacks [10-12, 16-16](#)
 - described [10-3](#)
 - zones [10-4](#)
- Anomaly Detection pane
- button functions [16-16](#)
 - described [16-15](#)
 - field descriptions [16-16](#)
 - user roles [16-15](#)
- anomaly detection policies
- ad0 [10-8](#)
 - adding [10-9](#)
 - cloning [10-9](#)
 - default policy [10-8](#)
 - deleting [10-9](#)
- Anomaly Detections pane
- described [10-8](#)
 - field descriptions [10-9](#)
 - user roles [10-8](#)
- appliances
- application partition image [20-11](#)
 - GRUB menu [15-4, C-8](#)
 - initializing [17-7](#)
 - logging in [18-2](#)
 - password recovery [15-4, C-8](#)
 - terminal servers
 - described [18-3, 20-13](#)
 - setting up [18-3, 20-13](#)
 - time sources [4-7, C-18](#)
 - upgrading recovery partition [20-6](#)
- Application Inspection and Control. See AIC.
- application partition
- described [A-3](#)
 - recovering image [20-11](#)
- application policy enforcement
- described [7-31, B-10](#)
 - disabled (default) [7-31, B-11](#)
- applications XML format [A-2](#)
- applying software updates [C-55](#)
- ARC
- ACLs [12-18, A-13](#)
 - authentication [A-14](#)
 - blocking
 - application [12-1](#)
 - connection-based [A-16](#)
 - not occurring for signature [C-44](#)
 - unconditional blocking [A-16](#)
 - block response [A-13](#)
- Catalyst 6000 series switch
- VACL commands [A-18](#)
 - VACLs [A-18](#)
- Catalyst switches
- VACLs [A-15](#)
 - VLANs [A-15](#)
- checking status [12-3, 12-4](#)
- described [A-3](#)
- design [12-2](#)
- device access issues [C-42](#)
- enabling SSH [C-44](#)
- features [A-13](#)
- firewalls
- AAA [A-17](#)
 - connection blocking [A-17](#)
 - NAT [A-18](#)
 - network blocking [A-17](#)
 - postblock ACL [A-15](#)
 - preblock ACL [A-15](#)
 - shun command [A-17](#)
 - TACACS+ [A-18](#)
- formerly Network Access Controller [12-1, 12-3](#)
- functions [12-1](#)
- illustration [A-12](#)
- inactive state [C-40](#)

- interfaces [A-13](#)
- maintaining states [A-16](#)
- managed devices [12-7](#)
- master blocking sensors [A-13](#)
- maximum blocks [12-2](#)
- misconfigured master blocking sensor [C-45](#)
- nac.shun.txt file [A-16](#)
- NAT addressing [A-14](#)
- number of blocks [A-14](#)
- postblock ACL [A-15](#)
- preblock ACL [A-15](#)
- prerequisites [12-5](#)
- rate limiting [12-4](#)
- responsibilities [A-12](#)
- single point of control [A-14](#)
- SSH [A-13](#)
- supported devices [12-5, A-15](#)
- Telnet [A-13](#)
- troubleshooting [C-39](#)
- VACLs [A-13](#)
- verifying device interfaces [C-43](#)
- verifying status [C-39](#)
- ARP
 - Layer 2 signatures [B-13](#)
 - protocol [B-13](#)
- ARP spoof tools
 - dsniff [B-13](#)
 - ettercap [B-13](#)
- ASDM resetting passwords [15-8, 15-10, C-12, C-14](#)
- assigning actions to signatures [7-17](#)
- asymmetric traffic
 - anomaly detection [10-2, 10-34](#)
 - disabling anomaly detection [C-22](#)
- Atomic ARP engine
 - described [B-13](#)
 - parameters (table) [B-13](#)
- Atomic IP Advanced engine
 - described [B-15](#)
 - restrictions [B-16](#)
- Atomic IP engine
 - described [8-13, B-25](#)
 - parameters (table) [B-25](#)
- Atomic IPv6 engine
 - described [B-29](#)
 - Neighborhood Discovery protocol [B-29](#)
 - signatures [B-29](#)
 - signatures (table) [B-30](#)
- attack relevance rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 6-22, 9-3, 9-24](#)
- Attack Response Controller
 - described [A-3](#)
 - formerly known as Network Access Controller [A-3](#)
- Attack Response Controller. See ARC.
- attack severity rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 9-3](#)
- authenticated NTP [4-6, 4-13, C-18](#)
- AuthenticationApp
 - authenticating users [A-20](#)
 - described [A-3](#)
 - login attempt limit [A-20](#)
 - method [A-20](#)
 - responsibilities [A-20](#)
 - secure communications [A-21](#)
 - sensor configuration [A-20](#)
- Authorized Keys pane
 - configuring [11-3](#)
 - described [11-2](#)
 - field descriptions [11-2](#)
 - RSA authentication [11-2](#)
 - RSA key generation tool [11-3](#)
- Auto/Cisco.com Update pane
 - configuring [15-21](#)
 - described [15-19](#)
 - field descriptions [15-20](#)
 - UNIX-style directory listings [15-19](#)
 - user roles [15-18](#)

automatic setup [17-1](#)

automatic updates

- Cisco.com [15-19](#)
- servers
 - FTP [15-19](#)
 - SCP [15-19](#)
- troubleshooting [C-55](#)

automatic upgrade

- information required [20-7](#)

autonegotiation for hardware bypass [5-11](#)

auto-upgrade-option command [20-7](#)

B

backing up

- configuration [C-3](#)
- current configuration [C-4, C-5](#)

BackOrifice. See BO.

BackOrifice 2000. See BO2K.

BackOrifice see BO

basic setup [17-3](#)

blocking

- described [12-1](#)
- disabling [12-8](#)
- master blocking sensor [12-24](#)
- necessary information [12-3](#)
- not occurring for signature [C-44](#)
- prerequisites [12-5](#)
- supported devices [12-5](#)
- types [12-2](#)

Blocking Devices pane

- configuring [12-15](#)
- described [12-14](#)
- field descriptions [12-14](#)
- ssh host-key command [12-15](#)

Blocking Properties pane

- adding a host never to be blocked [12-11](#)
- configuring [12-9](#)
- described [12-7](#)

- field descriptions [12-8](#)

BO

- described [B-69](#)
- Trojans [B-69](#)

BO2K

- described [B-69](#)
- Trojans [B-69](#)

Bug Toolkit

- described [C-1](#)
- URL [C-1](#)

bypass mode

- AIP SSC-5 [5-27](#)
- AIP SSM [5-27](#)
- described [5-26](#)

Bypass pane

- field descriptions [5-26](#)
- user roles [5-26](#)

C

calculating risk rating

- attack relevance rating [6-5, 9-3](#)
- attack severity rating [6-5, 9-3](#)
- promiscuous delta [6-5, 9-3](#)
- signature fidelity rating [6-5, 9-3](#)
- target value rating [6-5, 9-3](#)
- watch list rating [6-6, 9-4](#)

cannot access sensor [C-27](#)

Cat 6K Blocking Device Interfaces pane

- configuring [12-23](#)
- described [12-21](#)
- field descriptions [12-22](#)

CDP described [5-29](#)

CDP Mode pane

- configuring [5-29](#)
- field descriptions [5-29](#)
- user roles [5-29](#)

certificates

- displaying [11-11](#)

- Firefox [1-7](#)
- generating [11-11](#)
- IDM [1-6, 11-7](#)
- Internet Explorer [1-7](#)
- changing Microsoft IIS to UNIX-style directory listings [15-19](#)
- cidDump and obtaining information [C-96](#)
- CIDEE
 - defined [A-32](#)
 - example [A-32](#)
 - IPS extensions [A-32](#)
 - protocol [A-32](#)
 - supported IPS events [A-32](#)
- cisco
 - default password [18-2](#)
 - default username [18-2](#)
- Cisco.com
 - accessing software [19-2](#)
 - downloading software [19-1](#)
 - IPS software [19-1](#)
 - software downloads [19-1](#)
- Cisco IOS rate limiting [12-4](#)
- Cisco IPS software
 - files [20-3](#)
 - new features [A-3](#)
- Cisco Security Intelligence Operations
 - described [19-10](#)
 - URL [19-10](#)
- Cisco Services for IPS
 - service contract [1-9, 15-14](#)
 - supported products [1-9, 15-14](#)
- clear events command [4-11, 4-15, 16-4, C-20, C-96](#)
- Clear Flow States pane described [16-27](#)
- clearing
 - events [4-15, 16-4, C-96](#)
 - flow states [16-27](#)
 - statistics [C-82](#)
- clear password command [15-6, 15-10, C-10, C-15](#)
- CLI described [A-3, A-27](#)
- clock set command [4-15](#)
- Clone Event Action Rules dialog box field descriptions [9-11](#)
- Clone Policy dialog box field descriptions [7-2, 10-9](#)
- Clone Signature dialog box field descriptions [7-7](#)
- cloning
 - anomaly detection policies [10-9](#)
 - event action rules policies [9-12](#)
 - signature definition policies [7-2](#)
 - signatures [7-15](#)
- command and control interface
 - described [5-2](#)
 - list [5-2](#)
- commands
 - auto-upgrade-option [20-7](#)
 - clear events [4-11, 4-15, 16-4, C-20, C-96](#)
 - clear password [15-6, 15-10, C-10, C-15](#)
 - clock set [4-15](#)
 - copy backup-config [C-3](#)
 - copy current-config [C-3](#)
 - debug module-boot [C-69](#)
 - downgrade [20-10](#)
 - hw-module module 1 reset [C-68](#)
 - hw-module module slot_number password-reset [15-6, 15-8, C-11, C-12](#)
 - session [18-5, 18-9](#)
 - setup [4-1, 17-1, 17-3, 17-7, 17-12, 17-15, 17-20, 17-24](#)
 - show events [C-93](#)
 - show health [C-74](#)
 - show module 1 details [C-68](#)
 - show settings [15-13, C-17](#)
 - show statistics [C-82](#)
 - show statistics virtual-sensor [C-26, C-82](#)
 - show tech-support [C-75](#)
 - show version [C-79](#)
 - upgrade [20-3, 20-5](#)
- Compare Knowledge Bases dialog box field descriptions [16-19](#)
- comparing KBs [16-19, 16-20](#)

- configuration files
 - backing up [C-3](#)
 - merging [C-3](#)
- configuration restrictions
 - alternate TCP reset interface [5-8](#)
 - inline interface pairs [5-8](#)
 - inline VLAN pairs [5-8](#)
 - interfaces [5-8](#)
 - physical interfaces [5-8](#)
 - VLAN groups [5-9](#)
- Configure Summertime dialog box field descriptions [3-4, 4-9](#)
- configuring
 - AIC policy parameters [7-38](#)
 - allowed hosts [4-5](#)
 - allowed networks [4-5](#)
 - anomaly detection operation settings [10-11](#)
 - application policy [7-38](#)
 - authorized keys [11-3](#)
 - automatic upgrades [20-8](#)
 - blocking devices [12-15](#)
 - blocking properties [12-9](#)
 - Cat 6K blocking device interfaces [12-23](#)
 - CDP mode [5-29](#)
 - CPU, Memory, & Load gadget [2-9](#)
 - CSA MC IPS interfaces [14-4](#)
 - device login profiles [12-13](#)
 - event action filters [6-15, 9-17](#)
 - events [16-3](#)
 - event variables [6-28, 9-29](#)
 - external zone [10-31](#)
 - general settings [6-33, 9-34](#)
 - host blocks [16-7](#)
 - illegal zone [10-25](#)
 - inline VLAN pairs [3-10](#)
 - interface pairs [5-20](#)
 - interfaces [5-18](#)
 - Interface Status gadget [2-6](#)
 - internal zone [10-18](#)
 - IP fragment reassembly signatures [7-42](#)
 - IP logging [16-14](#)
 - IPv4 target value rating [6-18, 9-20](#)
 - IPv6 target value rating [6-20, 9-22](#)
 - known host keys [11-5](#)
 - learning accept mode [10-14](#)
 - Licensing gadget [2-5](#)
 - maintenance partition
 - IDS-M-2 (Catalyst software) [20-30](#)
 - IDS-M-2 (Cisco IOS software) [20-34](#)
 - master blocking sensor [12-26](#)
 - network blocks [16-9](#)
 - Network Security gadget [2-7](#)
 - network settings [4-3](#)
 - NTP servers [4-12](#)
 - OS maps [6-25, 9-27](#)
 - rate limiting [16-11](#)
 - rate limiting devices [12-15](#)
 - risk categories [6-30, 9-32](#)
 - router blocking device interfaces [12-20](#)
 - Sensor Health gadget [2-4](#)
 - Sensor Information gadget [2-3](#)
 - Sensor Setup window [3-4](#)
 - sensor to use NTP [4-13](#)
 - SNMP [13-2](#)
 - SNMP traps [13-4](#)
 - TCP fragment reassembly parameters [7-49](#)
 - time [4-10](#)
 - Top Applications gadget [2-7](#)
 - traffic flow notifications [5-28](#)
 - trusted hosts [11-10](#)
 - upgrades [20-4](#)
 - users [4-17](#)
 - VLAN groups [5-24](#)
 - VLAN pairs [5-22](#)
- control transactions
 - characteristics [A-8](#)
 - request types [A-8](#)
- cookies and IDM [1-5](#)

copy backup-config command [C-3](#)
 copy current-config command [C-3](#)
 correcting time on the sensor [4-11, C-20](#)

CPU, Memory, & Load gadget

configuring [2-9](#)
 described [2-8](#)

creating

Atomic IP Advanced signature [7-24](#)
 custom signatures
 not using signature engines [8-4](#)
 using signature engines [8-2](#)

IPv6 signatures [7-24](#)

Meta signatures [7-22](#)

Post-Block VACLs [12-21](#)

Pre-Block VACLs [12-21](#)

service account [C-6](#)

cryptographic account

Encryption Software Export Distribution
 Authorization from [19-2](#)
 obtaining [19-2](#)

cryptographic features (IDM) [1-1](#)

CSA MC

adding interfaces [14-7](#)
 configuring IPS interfaces [14-4](#)
 host posture events [14-1, 14-4](#)
 quarantined IP address events [14-1](#)
 supported IPS interfaces [14-4](#)

CtlTransSource

described [A-2, A-11](#)
 illustration [A-11](#)

current

configuration backup [C-3](#)
 KB setting [16-21](#)

customizing

dashboards [2-1](#)
 gadgets [2-1](#)

custom signatures

described [7-5](#)
 IPv6 signature [7-24](#)

Custom Signature Wizard

no signature engine sequence [8-4](#)
 signature engine sequence [8-2](#)

D

Dashboard pane gadgets [2-2](#)

dashboards

adding [2-1](#)
 customizing [2-1](#)

data structures (examples) [A-7](#)

DDoS

protocols [B-68](#)
 Stacheldraht [B-68](#)
 TFN [B-68](#)

debug logging enabling [C-47](#)

debug-module-boot command [C-69](#)

default policies

ad0 [10-8](#)
 rules0 [9-11](#)
 sig0 [7-2](#)

defaults

KB filename [10-12](#)
 password [18-2](#)
 restoring [15-25](#)
 username [18-2](#)
 virtual sensor vs0 [6-3](#)

deleting

anomaly detection policies [10-9](#)
 event action filters [6-15, 9-17](#)
 event action overrides [9-14](#)
 event action rules policies [9-12](#)
 event variables [6-28, 9-29](#)
 imported OS values [16-26](#)
 IPv4 target value rating [6-18, 9-20](#)
 IPv6 target value rating [6-20, 9-22](#)
 KBs [16-22](#)
 learned OS values [16-25](#)
 OS maps [6-25, 9-27](#)

- risk categories [6-30, 9-32](#)
 - signature definition policies [7-2](#)
 - signature variables [7-27](#)
 - virtual sensors [6-11](#)
- Denial of Service. See DoS.
- denied attackers
 - adding [16-5](#)
 - clearing list [16-5](#)
 - hit count [16-4](#)
 - resetting hit counts [16-5](#)
- Denied Attackers pane
 - described [16-4](#)
 - field descriptions [16-5](#)
 - user roles [16-4](#)
 - using [16-5](#)
- deny actions (list) [9-8](#)
- Deny Packet Inline described [9-10, B-8](#)
- detect mode (anomaly detection) [10-4](#)
- device access issues [C-42](#)
- Device Login Profiles pane
 - configuring [12-13](#)
 - described [12-12](#)
 - field descriptions [12-12](#)
- devices [12-15](#)
- Diagnostics Report pane
 - button functions [16-29](#)
 - described [16-29](#)
 - user roles [16-29](#)
 - using [16-29](#)
- diagnostics reports [16-29](#)
- Differences between knowledge bases KB_Name and KB_Name window field descriptions [16-19](#)
- disabling
 - anomaly detection [C-22](#)
 - blocking [12-8](#)
 - interfaces [5-18](#)
 - password recovery [15-12, C-16](#)
- disaster recovery [C-6](#)

- displaying
 - events [C-94](#)
 - health status [C-75](#)
 - password recovery setting [15-13, C-17](#)
 - statistics [C-82](#)
 - tech support information [C-76](#)
 - version [C-79](#)

Distributed Denial of Service. See DDoS.

DoS tools [B-6](#)

downgrade command [20-10](#)

downgrading sensors [20-10](#)

downloading

- KBs [16-23](#)

- software [19-1](#)

Download Knowledge Base From Sensor dialog box

- described [16-23](#)

- field descriptions [16-23](#)

duplicate IP addresses [C-30](#)

E

Edit Actions dialog box field descriptions [7-9](#)

Edit Allowed Host dialog box

- field descriptions [4-5](#)

- user roles [4-4](#)

Edit Authorized Key dialog box

- field descriptions [11-3](#)

- user roles [11-2](#)

Edit Blocking Device dialog box

- field descriptions [12-15](#)

- user roles [12-14](#)

Edit Cat 6K Blocking Device Interface dialog box

- field descriptions [12-23](#)

- user roles [12-21](#)

Edit Configured OS Map dialog box

- field descriptions [6-24, 9-26](#)

- user roles [6-23, 9-23](#)

Edit Destination Port dialog box field descriptions [10-16](#)

- Edit Device Login Profile dialog box
 - field descriptions [12-12](#)
 - user roles [12-12](#)
- Edit Event Action Filter dialog box
 - field descriptions [6-14, 9-16](#)
 - user roles [6-13, 9-15](#)
- Edit Event Action Override dialog box
 - field descriptions [6-11, 9-13](#)
 - user roles [6-11, 9-13](#)
- Edit Event Variable dialog box
 - field descriptions [6-27, 9-29](#)
 - user roles [6-26, 9-28](#)
- Edit External Product Interface dialog box
 - field descriptions [14-6](#)
 - user roles [14-5](#)
- Edit Histogram dialog box field descriptions [10-17](#)
- editing
 - event action filters [6-15, 9-17](#)
 - event action overrides [9-14](#)
 - event variables [6-28, 9-29](#)
 - interfaces [5-18](#)
 - IPv4 target value rating [6-18, 9-20](#)
 - IPv6 target value rating [6-20, 9-22](#)
 - OS maps [6-25, 9-27](#)
 - risk categories [6-30, 9-32](#)
 - signatures [7-16](#)
 - signature variables [7-27](#)
 - virtual sensors [6-11](#)
- Edit Inline VLAN Pair dialog box field descriptions [3-9, 5-22](#)
- Edit Interface dialog box field descriptions [5-17](#)
- Edit Interface Pair dialog box field descriptions [5-20](#)
- Edit IP Logging dialog box field descriptions [16-13](#)
- Edit Known Host Key dialog box
 - field descriptions [11-5](#)
 - user roles [11-4](#)
- Edit Master Blocking Sensor dialog box
 - field descriptions [12-25](#)
 - user roles [12-24](#)
- Edit Never Block Address dialog box
 - field descriptions [12-10](#)
 - user roles [12-7](#)
- Edit Posture ACL dialog box field descriptions [14-7](#)
- Edit Protocol Number dialog box field descriptions [10-18, 10-25](#)
- Edit Risk Level dialog box field descriptions [6-30, 9-32](#)
- Edit Router Blocking Device Interface dialog box
 - field descriptions [12-19](#)
 - user roles [12-17](#)
- Edit Signature dialog box field descriptions [7-7](#)
- Edit Signature Variable dialog box
 - field descriptions [7-27](#)
 - user roles [7-26](#)
- Edit SNMP Trap Destination dialog box field descriptions [13-4](#)
- Edit User dialog box
 - field descriptions [4-16](#)
 - user roles [4-16](#)
- Edit Virtual Sensor dialog box
 - field descriptions [6-9](#)
 - user roles [6-9](#)
- Edit VLAN Group dialog box field descriptions [5-24](#)
- enabling
 - debug logging [C-47](#)
 - event action filters [6-15, 9-17](#)
 - event action overrides [9-14](#)
 - interfaces [5-18](#)
- Encryption Software Export Distribution Authorization form
 - cryptographic account [19-2](#)
 - described [19-2](#)
- engines
 - AIC [B-10](#)
 - Atomic [B-13](#)
 - Fixed [B-31](#)
 - Flood [B-33](#)
 - Master [B-4](#)
 - Meta [7-21, B-34](#)
 - Multi String [B-36](#)

- Normalizer [B-37](#)
- Service DNS [B-41](#)
- Service FTP [B-42](#)
- Service Generic [B-43](#)
- Service H225 [B-44](#)
- Service HTTP [8-14, B-46](#)
- Service IDENT [B-48](#)
- Service MSRPC [8-11, B-49](#)
- Service MSSQL [B-51](#)
- Service NTP [B-51](#)
- Service P2P [B-52](#)
- Service RPC [8-17, B-52](#)
- Service SMB Advanced [B-54](#)
- Service SNMP [B-56](#)
- Service SSH [B-56](#)
- Service TNS [B-57](#)
- State [8-18, B-59](#)
- String [8-19, 8-22, B-60](#)
- Sweep [8-22, B-63](#)
- Sweep Other TCP [B-65](#)
- Traffic ICMP [B-68](#)
- Trojan [B-69](#)
- evAlert [A-8](#)
- event action filters
 - adding [6-15, 9-17](#)
 - configuring [6-15, 9-17](#)
 - deleting [6-15, 9-17](#)
 - described [6-13, 9-5](#)
 - editing [6-15, 9-17](#)
 - enabling [6-15, 9-17](#)
- Event Action Filters tab
 - configuring [6-15, 9-17](#)
 - described [6-13, 9-15](#)
 - field descriptions [6-13, 9-15](#)
- event action overrides
 - adding [9-14](#)
 - deleting [9-14](#)
 - described [6-4, 9-4](#)
 - editing [9-14](#)
 - enabling [9-14](#)
- Event Action Overrides tab
 - described [9-13](#)
 - field descriptions [9-13](#)
- event action rules
 - described [9-2](#)
 - functions [9-2](#)
- Event Action Rules (rules0) pane described [9-12](#)
- Event Action Rules pane
 - described [9-11](#)
 - field descriptions [9-11](#)
 - user roles [9-11](#)
- event action rules policies
 - adding [9-12](#)
 - cloning [9-12](#)
 - deleting [9-12](#)
- events
 - displaying [C-94](#)
 - host posture [14-2](#)
 - quarantined IP address [14-2](#)
- Events pane
 - configuring [16-3](#)
 - described [16-2](#)
 - field descriptions [16-2](#)
- Event Store
 - clearing events [4-11, C-20](#)
 - data structures [A-7](#)
 - described [A-2](#)
 - examples [A-7](#)
 - responsibilities [A-7](#)
 - timestamp [A-7](#)
- event types [C-92](#)
- event variables
 - adding [6-28, 9-29](#)
 - configuring [6-28, 9-29](#)
 - deleting [6-28, 9-29](#)
 - editing [6-28, 9-29](#)
 - example [6-27, 9-28](#)

Event Variables tab

- configuring [6-28, 9-29](#)
- described [6-26, 9-28](#)
- field descriptions [6-27, 9-29](#)

Event Viewer window field descriptions [16-3](#)evError [A-8](#)evLogTransaction [A-8](#)evShunRqst [A-8](#)evStatus [A-8](#)

example custom signatures

- Atomic IP Advanced [7-24](#)
- Meta engine [7-22](#)
- Service HTTP [8-15](#)
- String TCP [8-20](#)

examples

- ASA failover configuration [C-71](#)

external product interfaces

- adding [14-7](#)
- described [14-1](#)
- issues [14-3, C-24](#)
- troubleshooting [14-10, C-24](#)
- trusted hosts [14-5](#)

External Product Interfaces pane

- described [14-5](#)
- field descriptions [14-5](#)

external zone

- configuring [10-31](#)
- protocols [10-29](#)
- user roles [10-28](#)

External Zone tab

- described [10-29](#)
- tabs [10-29](#)
- user roles [10-28](#)

F
fail-over testing [5-10](#)false positives described [7-4](#)

files

- Cisco IPS [20-3](#)
- IDSM2 password recovery [15-11, C-15](#)

Firefox

- certificates [1-7](#)
- validating CAs [1-7](#)

Fixed engine described [B-31](#)Fixed ICMP engine parameters (table) [B-31](#)Fixed TCP engine parameters (table) [B-32](#)Fixed UDP engine parameters (table) [B-33](#)Flood engine described [B-33](#)Flood Host engine parameters (table) [B-34](#)Flood Net engine parameters (table) [B-34](#)flow states clearing [16-27](#)FTP servers supported [15-19, 20-2](#)

G

gadgets

- adding [2-1](#)
- CPU, Memory, & Load [2-8](#)
- customizing [2-1](#)
- Dashboard pane [2-2](#)
- IDM [2-2](#)
- IDM home pane [1-2](#)
- Interface Status [2-5](#)
- Licensing [2-5](#)
- Network Security [2-6](#)
- Sensor Health [2-3](#)
- Sensor Information [2-3](#)
- Top Applications [2-7](#)

general settings

- configuring [6-33, 9-34](#)
- described [6-31, 9-33](#)

General tab

- configuring [6-33, 9-34](#)
- described [6-31, 9-33, 10-15, 10-22](#)
- enabling zones [10-15, 10-22](#)
- field descriptions [6-32, 9-34](#)

user roles [6-31, 9-33](#)

generating diagnostics reports [16-29](#)

Global Variables pane field description [15-18](#)

GRUB menu password recovery [15-4, C-8](#)

H

H.225.0 protocol [B-44](#)

H.323 protocol [B-44](#)

hardware bypass

autonegotiation [5-11](#)

configuration restrictions [5-10](#)

fail-over [5-10](#)

IPS 4270-20 [5-10](#)

supported configurations [5-10](#)

with software bypass [5-10](#)

Home pane

device information [1-2](#)

gadgets [1-2](#)

health information [1-2](#)

interface status [1-2](#)

licensing information [1-2](#)

system resources usage [1-2](#)

updating [1-2](#)

Host Blocks pane

configuring [16-7](#)

described [16-6](#)

host posture events

CSA MC [14-4](#)

described [14-2](#)

HTTP/HTTPS servers [15-19, 20-2](#)

HTTP deobfuscation

ASCII normalization [8-14, B-46](#)

described [8-14, B-46](#)

hw-module module 1 reset command [C-68](#)

hw-module module slot_number password-reset
command [15-6, 15-8, C-11, C-12](#)

IDAPI

communications [A-3, A-30](#)

described [A-3](#)

functions [A-30](#)

illustration [A-30](#)

responsibilities [A-30](#)

IDCONF

described [A-31](#)

example [A-31](#)

XML [A-31](#)

IDIOM

defined [A-30](#)

messages [A-30](#)

IDM

Analysis Engine is busy [C-58](#)

certificates [1-6, 11-7](#)

cookies [1-5](#)

cryptographic features [1-1](#)

described [1-2, 1-4](#)

gadgets [2-2](#)

GUI [1-2](#)

logging in [1-4](#)

Signature Wizard supported signature engines [8-2](#)

supported platforms [1-3](#)

system requirements [1-3](#)

TLS [1-6, 11-8](#)

user interface [1-2](#)

web browsers [1-2, 1-4](#)

will not load [C-57](#)

IDS-2

command and control port [C-66](#)

configuring

 maintenance partition (Catalyst software) [20-30](#)

 maintenance partition (Cisco IOS
 software) [20-34](#)

initializing [17-20](#)

- installing
 - system image (Catalyst software) [20-28](#)
 - system image (Cisco IOS software) [20-30](#)
- logging in [18-7](#)
- reimaging [20-27](#)
- sessioning [18-7](#)
- setup command [17-20](#)
- supported configurations [C-62](#)
- TCP reset port [C-67](#)
- time sources [4-7, C-18](#)
- upgrading
 - maintenance partition (Catalyst software) [20-38](#)
 - maintenance partition (Cisco IOS software) [20-38](#)
- IDS M2
 - installing
 - system image (Cisco IOS software) [20-29](#)
 - password recovery [15-11, C-14](#)
 - password recovery image file [15-11, C-15](#)
 - TCP reset port [C-67](#)
- illegal zone
 - configuring [10-25](#)
 - user roles [10-22](#)
- Illegal Zone tab
 - described [10-22](#)
 - user roles [10-22](#)
- IME time synchronization problems [C-60](#)
- Imported OS pane
 - clearing [16-26](#)
 - described [16-26](#)
 - field descriptions [16-26](#)
- imported OS values
 - clearing [16-26](#)
 - deleting [16-26](#)
- inactive mode (anomaly detection) [10-4](#)
- initializing
 - AIM-IPS [17-12](#)
 - AIP-SSC-5 [17-6](#)
 - AIP-SSM [17-15](#)
 - appliances [17-7](#)
 - IDS M-2 [17-20](#)
 - NME-IPS [17-24](#)
 - sensors [4-1, 17-1, 17-3](#)
 - user roles [17-1](#)
 - verifying [17-27](#)
- inline interface pair mode
 - configuration restrictions [5-8](#)
 - described [5-13](#)
- Inline Interface Pair window
 - described [3-8](#)
 - Startup Wizard [3-8](#)
- inline VLAN pair mode
 - described [5-14](#)
 - supported sensors [5-14](#)
- inline VLAN pairs
 - configuration restrictions [5-8](#)
 - configuring [3-10](#)
- Inline VLAN Pairs pane user roles [5-21](#)
- Inline VLAN Pairs window
 - described [3-9](#)
 - field descriptions [3-9](#)
 - Startup Wizard [3-9](#)
- installer major version [19-5](#)
- installer minor version [19-5](#)
- installing
 - sensor license [1-10, 15-16](#)
 - system image
 - AIM-IPS [20-22](#)
 - AIP-SSM [20-25](#)
 - IDS M-2 (Catalyst software) [20-28](#)
 - IDS M-2 (Cisco IOS software) [20-30](#)
 - IDS M2 (Cisco IOS software) [20-29](#)
 - IPS-4240 [20-14](#)
 - IPS-4255 [20-14](#)
 - IPS-4260 [20-18](#)
 - IPS 4270-20 [20-20](#)
 - NME-IPS [20-39](#)

- InterfaceApp
 - described [A-19](#)
 - interactions [A-19](#)
 - NIC drivers [A-19](#)
- InterfaceApp described [A-3](#)
- interface pairs
 - configuring [5-20](#)
 - described [5-19](#)
- Interface Pairs pane
 - configuring [5-20](#)
 - described [5-19](#)
 - field descriptions [5-20](#)
 - user roles [5-19](#)
- interfaces
 - alternate TCP reset [5-2](#)
 - command and control [5-2](#)
 - configuration restrictions [5-8](#)
 - configuring [5-18](#)
 - described [3-6, 5-1](#)
 - disabling [5-18](#)
 - editing [5-18](#)
 - enabling [5-18](#)
 - logical [3-6](#)
 - physical [3-6](#)
 - port numbers [5-1](#)
 - sensing [5-2, 5-3](#)
 - slot numbers [5-1](#)
 - support (table) [5-4](#)
 - TCP reset [5-6](#)
 - VLAN groups [5-2](#)
- Interface Selection window
 - described [3-8](#)
 - Startup Wizard [3-8](#)
- Interfaces pane
 - configuring [5-18](#)
 - described [5-16](#)
 - field descriptions [5-17](#)
 - user roles [5-16](#)
- Interface Status gadget
 - configuring [2-6](#)
 - described [2-5](#)
- Interface Summary window described [3-6](#)
- internal zone
 - configuring [10-18](#)
 - user roles [10-15](#)
- Internal Zone tab
 - described [10-15](#)
 - user roles [10-15](#)
- Internet Explorer validating certificates [1-7](#)
- IP fragmentation described [B-38](#)
- IP fragment reassembly
 - configuring [7-41](#)
 - described [7-39](#)
 - example signature [7-42](#)
 - mode [7-41](#)
 - parameters (table) [7-40](#)
 - signatures [7-42](#)
 - signatures (table) [7-40](#)
- IP logging
 - described [7-50, 16-12](#)
 - event actions [16-13](#)
 - system performance [16-13](#)
- IP Logging pane
 - configuring [16-14](#)
 - described [16-13](#)
 - field descriptions [16-13](#)
 - user roles [16-13](#)
- IP Logging Variables pane described [15-18](#)
- IP logs
 - circular buffer [16-12](#)
 - states [16-12](#)
 - TCPDUMP [16-12](#)
 - viewing [16-14](#)
 - WireShark [16-12](#)
- IPS-4240
 - installing system image [20-14](#)
 - password recovery [15-5, C-9](#)

- reimaging [20-14](#)
- IPS-4255
 - installing system image [20-14](#)
 - password recovery [15-5, C-9](#)
 - reimaging [20-14](#)
- IPS-4260
 - installing system image [20-18](#)
 - password recovery [15-4, C-9](#)
 - reimaging [20-18](#)
- IPS 4270-20
 - hardware bypass [5-10](#)
 - installing system image [20-20](#)
 - password recovery [15-4, C-9](#)
 - reimaging [20-20](#)
- IPS appliances
 - Deny Connection Inline [9-10, C-73](#)
 - Deny Packet Inline [9-10, C-73](#)
 - Reset TCP Connection [9-10, C-73](#)
 - TCP reset packets [9-10, C-73](#)
- IPS applications
 - summary [A-33](#)
 - table [A-33](#)
 - XML format [A-2](#)
- IPS data
 - types [A-8](#)
 - XML document [A-8](#)
- IPS events
 - evAlert [A-8](#)
 - evError [A-8](#)
 - evLogTransaction [A-8](#)
 - evShunRqst [A-8](#)
 - evStatus [A-8](#)
 - list [A-8](#)
 - types [A-8](#)
- IPS internal communications [A-30](#)
- IPS modules
 - time synchronization [4-8, C-19](#)
 - unsupported features [3-7](#)
- IPS Policies pane
 - described [6-8](#)
 - field descriptions [6-9](#)
- IPS software
 - application list [A-2](#)
 - available files [19-1](#)
 - configuring device parameters [A-4](#)
 - directory structure [A-32](#)
 - Linux OS [A-2](#)
 - obtaining [19-1](#)
 - platform-dependent release examples [19-7](#)
 - retrieving data [A-4](#)
 - security features [A-5](#)
 - tuning signatures [A-4](#)
 - updating [A-4](#)
 - user interaction [A-4](#)
 - versioning scheme [19-3](#)
- IPS software file names
 - major updates (illustration) [19-4](#)
 - minor updates (illustration) [19-4](#)
 - patch releases (illustration) [19-4](#)
 - service packs (illustration) [19-4](#)
- IPv4 Add Target Value Rating dialog box
 - field descriptions [6-18, 9-20](#)
 - user roles [6-18, 9-20](#)
- IPv4 Edit Target Value Rating dialog box
 - field descriptions [6-18, 9-20](#)
 - user roles [6-18, 9-20](#)
- IPv4 target value rating
 - adding [6-18, 9-20](#)
 - configuring [6-18, 9-20](#)
 - deleting [6-18, 9-20](#)
 - editing [6-18, 9-20](#)
- IPv4 Target Value Rating tab
 - configuring [6-18, 9-20](#)
 - field descriptions [6-18, 9-20](#)
- IPv6
 - described [B-29](#)
 - SPAN ports [5-12, A-4](#)

switches [5-12, A-4](#)

IPv6 Add Target Value Rating dialog box

field descriptions [6-20, 9-22](#)

user roles [6-19, 9-21](#)

IPv6 Edit Target Value Rating dialog box

field descriptions [6-20, 9-22](#)

user roles [6-19, 9-21](#)

IPv6 target value rating

adding [6-20, 9-22](#)

configuring [6-20, 9-22](#)

deleting [6-20, 9-22](#)

editing [6-20, 9-22](#)

IPv6 Target Value Rating tab

configuring [6-20, 9-22](#)

field descriptions [6-20, 9-22](#)

K

KBs

comparing [16-20](#)

default filename [10-12](#)

deleting [16-22](#)

described [10-3](#)

downloading [16-23](#)

histogram [10-12, 16-16](#)

initial baseline [10-3](#)

learning accept mode [10-12](#)

loading [16-21](#)

monitoring [16-18](#)

renaming [16-22](#)

saving [16-22](#)

scanner threshold [10-12, 16-16](#)

tree structure [10-12, 16-16](#)

uploading [16-24](#)

Knowledge Base. See KB.

Known Host Keys pane

configuring [11-5](#)

describing [11-4](#)

field descriptions [11-5](#)

L

Learned OS pane

clearing [16-25](#)

described [16-25](#)

field descriptions [16-25](#)

learned OS values

clearing [16-25](#)

deleting [16-25](#)

learning accept mode

anomaly detection [10-3](#)

configuring [10-14](#)

Learning Accept Mode tab

described [10-12](#)

field descriptions [10-13, 10-14](#)

user roles [10-12](#)

license files

BSD license [D-3](#)

expat license [D-12](#)

GNU Lesser license [D-22](#)

GNU license [D-17](#)

license key trial [1-8, 15-14](#)

licensing

described [1-8, 15-14](#)

IPS device serial number [1-8, 15-14](#)

Licensing gadget

configuring [2-5](#)

described [2-5](#)

Licensing pane

configuring [1-10, 15-16](#)

described [1-8, 15-14](#)

field descriptions [1-10, 15-15](#)

user roles [1-10, 15-13](#)

limitations for concurrent CLI sessions [18-1](#)

listings UNIX-style [15-19](#)

loading KBs [16-21](#)

Logger

described [A-3, A-19](#)

functions [A-19](#)

- syslog messages [A-19](#)
- logging in
 - AIM-IPS [18-5](#)
 - AIP-SSC-5 [18-6](#)
 - AIP-SSM [18-6](#)
 - appliances [18-2](#)
 - IDM [1-4](#)
 - IDS-2 [18-7](#)
 - NME-IPS [18-10](#)
 - sensors
 - SSH [18-11](#)
 - Telnet [18-11](#)
 - service role [18-2](#)
 - terminal servers [18-3, 20-13](#)
 - user role [18-1](#)
- LOKI
 - described [B-68](#)
 - protocol [B-68](#)
- loose connections and sensors [C-25](#)

M

- MainApp
 - components [A-5](#)
 - described [A-2, A-5](#)
 - host statistics [A-6](#)
 - responsibilities [A-6](#)
 - show version command [A-6](#)
- maintenance partition
 - configuring
 - IDS-2 (Catalyst software) [20-30](#)
 - IDS-2 (Cisco IOS software) [20-34](#)
 - described [A-3](#)
- major updates described [19-3](#)
- managing rate limiting [16-11](#)
- manual block to bogus host [C-44](#)
- master blocking sensor
 - described [12-24](#)
 - not set up properly [C-45](#)
- Master Blocking Sensor pane
 - configuring [12-26](#)
 - described [12-24](#)
 - field descriptions [12-25](#)
- Master engine
 - alert frequency [B-6](#)
 - alert frequency parameters (table) [B-6](#)
 - described [B-3](#)
 - event actions [B-7](#)
 - general parameters (table) [B-4](#)
 - universal parameters [B-4](#)
- master engine parameters
 - obsoletes [B-6](#)
 - promiscuous delta [B-5](#)
 - vulnerable OSes [B-6](#)
- merging configuration files [C-3](#)
- Meta engine
 - described [7-21, B-34](#)
 - parameters (table) [B-35](#)
 - Signature Event Action Processor [7-21, B-34](#)
- Meta Event Generator described [6-31, 9-33](#)
- MIBs supported [13-6, C-21](#)
- minor updates described [19-3](#)
- Miscellaneous tab
 - button functions [7-29](#)
 - configuring
 - application policy [7-38](#)
 - IP fragment reassembly mode [7-41](#)
 - IP logging [7-50](#)
 - TCP stream reassembly mode [7-48](#)
 - described [7-28](#)
 - field descriptions [7-29](#)
 - user roles [7-28](#)
- modes
 - anomaly detection detect [10-4](#)
 - anomaly detection inactive [10-4](#)
 - anomaly detection learning accept [10-3](#)
 - bypass [5-26](#)
 - inline interface pair [5-13](#)

- inline VLAN pair [5-14](#)
- promiscuous [5-11](#)
- VLAN Groups [5-14](#)
- modify packets inline modes [6-4](#)
- monitoring
 - events [16-3](#)
 - KBs [16-18](#)
- moving OS maps [6-25, 9-27](#)
- Multi String engine
 - described [B-36](#)
 - parameters (table) [B-36](#)
 - Regex [B-36](#)
- MySDN described [7-5](#)

N

- Neighborhood Discovery
 - options [B-29](#)
 - types [B-29](#)
- Network Blocks pane
 - configuring [16-9](#)
 - described [16-8](#)
 - field descriptions [16-9](#)
 - user roles [16-8](#)
- Network pane
 - configuring [4-3](#)
 - field descriptions [4-2](#)
 - TLS/SSL [4-3](#)
 - user roles [4-2](#)
- Network Security gadget
 - configuring [2-7](#)
 - described [2-6](#)
- network security health data reset [16-28](#)
- Network Timing Protocol. See NTP.
- Network Timing Protocol see NTP
- never block
 - hosts [12-7](#)
 - networks [12-7](#)

- NME-IPS
 - initializing [17-24](#)
 - installing system image [20-39](#)
 - logging in [18-10](#)
 - reimaging [20-39](#)
 - session command [18-9](#)
 - sessioning [18-8, 18-10](#)
 - setup command [17-24](#)
 - time sources [4-7, C-18](#)
- Normalizer engine
 - described [B-37](#)
 - IP fragment reassembly [B-38](#)
 - parameters (table) [B-39](#)
 - TCP stream reassembly [B-38](#)
- Normalizer mode described [6-4](#)
- NotificationApp
 - alert information [A-9](#)
 - described [A-3](#)
 - functions [A-9](#)
 - SNMP gets [A-9](#)
 - SNMP traps [A-9](#)
 - statistics [A-10](#)
 - system health information [A-10](#)
- NTP
 - authenticated [4-6, 4-13, C-18](#)
 - configuring servers [4-12](#)
 - described [4-6, C-18](#)
 - incorrect configuration [4-8, C-19](#)
 - sensor time source [4-12, 4-13](#)
 - time synchronization [4-6, C-18](#)
 - unauthenticated [4-6, 4-13, C-18](#)
- NTP configuration verifying [4-8](#)

O

- obsoletes field described [B-6](#)
- obtaining
 - cryptographic account [19-2](#)
 - IPS software [19-1](#)

one-way TCP reset described [6-32, 9-33](#)

Operation Settings tab

described [10-10](#)

field descriptions [10-11](#)

user roles [10-10](#)

OS Identifications tab

described [6-23, 9-24](#)

field descriptions [6-24, 9-26](#)

OS maps

adding [6-25, 9-27](#)

configuring [6-25, 9-27](#)

deleting [6-25, 9-27](#)

editing [6-25, 9-27](#)

moving [6-25, 9-27](#)

other actions (list) [9-9](#)

Other Protocols tab

described [10-24, 10-30](#)

describing [10-17](#)

enabling other protocols [10-17](#)

external zone [10-30](#)

field descriptions [10-18, 10-30](#)

illegal zone [10-24](#)

P

P2P networks described [B-52](#)

partitions

application [A-3](#)

maintenance [A-3](#)

recovery [A-3](#)

passive OS fingerprinting

components [6-22, 9-24](#)

configuring [6-23, 9-25](#)

described [6-21, 9-24](#)

password policy caution [15-2, 15-3](#)

password recovery

AIP SSC-5 [15-6, C-10](#)

AIP SSM [15-8, C-12](#)

appliances [15-4, C-8](#)

CLI [15-12, C-16](#)

described [15-4, C-8](#)

disabling [15-12, C-8](#)

GRUB menu [15-4, C-8](#)

IDSM2 [15-11, C-14](#)

IPS-4240 [15-5, C-9](#)

IPS-4255 [15-5, C-9](#)

platforms [15-4, C-8](#)

ROMMON [15-5, C-9](#)

troubleshooting [15-12, C-17](#)

verifying [15-13, C-17](#)

password requirements configuration [15-2](#)

Passwords pane

described [15-2](#)

field descriptions [15-2](#)

patch releases described [19-4](#)

peacetime learning (anomaly detection) [10-3](#)

Peer-to-Peer. See P2P.

physical connectivity issues [C-33](#)

physical interfaces configuration restrictions [5-8](#)

platforms concurrent CLI sessions [18-1](#)

Post-Block ACLs [12-17, 12-18](#)

Pre-Block ACLs [12-17, 12-18](#)

prerequisites for blocking [12-5](#)

promiscuous delta

calculating risk rating [6-5, 9-3](#)

described [6-5, 9-3](#)

promiscuous delta described [B-5](#)

promiscuous mode

described [5-11](#)

packet flow [5-11](#)

SPAN ports [5-12, A-4](#)

VACL capture [5-12, A-4](#)

protocols

ARP [B-13](#)

CIDEE [A-32](#)

DCE [8-11, B-49](#)

DDoS [B-68](#)

H.323 [B-44](#)

H225.0 [B-44](#)
 ICMPv6 [B-15](#)
 IDAPI [A-30](#)
 IDCONF [A-31](#)
 IDIOM [A-30](#)
 IPv6 [B-29](#)
 LOKI [B-68](#)
 MSSQL [B-51](#)
 Neighborhood Discovery [B-29](#)
 Q.931 [B-44](#)
 RPC [8-11](#), [B-49](#)
 SDEE [A-31](#)
 Signature Wizard [8-10](#)

Q

Q.931 protocol
 described [B-44](#)
 SETUP messages [B-44](#)
 quarantined IP address events described [14-2](#)

R

rate limiting
 ACLs [12-5](#)
 configuring [16-11](#)
 described [12-4](#)
 managing [16-11](#)
 percentages [16-10](#)
 routers [12-4](#)
 service policies [12-5](#)
 supported signatures [12-4](#)
 Rate Limits pane
 described [16-10](#)
 field descriptions [16-10](#)
 RDEP event server deprecated [A-22](#)
 rebooting the sensor [15-26](#)

Reboot Sensor pane
 configuring [15-26](#)
 described [15-26](#)
 user roles [15-26](#)
 recover command [20-11](#)
 recovering
 AIP-SSM [C-69](#)
 application partition image [20-11](#)
 recovery partition
 described [A-3](#)
 upgrading [20-6](#)
 Regular Expression. See [Regex](#).
 regular expression syntax
 signatures [B-9](#)
 reimaging
 AIM-IPS [20-22](#)
 AIP-SSC-5 [20-25](#)
 AIP-SSM [20-25](#)
 appliances [20-11](#)
 described [20-1](#)
 IDSM-2 [20-27](#)
 IPS-4240 [20-14](#)
 IPS-4255 [20-14](#)
 IPS-4260 [20-18](#)
 IPS 4270-20 [20-20](#)
 NME-IPS [20-39](#)
 sensors [20-1](#)
 removing
 last applied
 service pack [20-10](#)
 signature update [20-10](#)
 renaming KBs [16-22](#)
 Reset Network Security Health pane
 described [16-28](#)
 field descriptions [16-28](#)
 user roles [16-28](#)
 reset not occurring for a signature [C-53](#)
 resetting
 AIP-SSM [C-68](#)

- network security health data [16-28](#)
- passwords
 - ASDM [15-8, 15-10, C-12, C-14](#)
 - hw-module command [15-6, 15-8, C-11, C-12](#)
- resetting the password
 - AIP SSC-5 [15-7, C-11](#)
 - AIP SSM [15-8, C-13](#)
- Restore Default Interface dialog box field descriptions [3-7](#)
- Restore Defaults pane
 - configuring [15-25](#)
 - described [15-25](#)
 - user roles [15-25](#)
- restoring
 - defaults [15-25](#)
- restoring the current configuration [C-4, C-5](#)
- risk categories
 - adding [6-30, 9-32](#)
 - configuring [6-30, 9-32](#)
 - deleting [6-30, 9-32](#)
 - editing [6-30, 9-32](#)
- Risk Category tab
 - configuring [6-30, 9-32](#)
 - described [6-29, 9-31](#)
 - field descriptions [6-30, 9-31](#)
- risk rating
 - calculating [6-4, 9-2](#)
 - described [6-22](#)
- ROMMON
 - described [20-13](#)
 - IPS-4240 [20-14](#)
 - IPS-4255 [20-14](#)
 - IPS-4260 [20-18](#)
 - IPS 4270-20 [20-18, 20-20](#)
 - password recovery [15-5, C-9](#)
 - remote sensors [20-13](#)
 - serial console port [20-13](#)
 - TFTP [20-13](#)
- round-trip time. See RTT.

- Router Blocking Device Interfaces pane
 - configuring [12-20](#)
 - described [12-17](#)
 - field descriptions [12-19](#)
- RPC portmapper [8-17, B-52](#)
- RTT
 - described [20-13](#)
 - TFTP limitation [20-13](#)

S

- Save Knowledge Base dialog box
 - described [16-21](#)
 - field descriptions [16-21](#)
- saving KBs [16-22](#)
- scheduling automatic upgrades [20-8](#)
- SDEE
 - described [A-31](#)
 - HTTP [A-31](#)
 - protocol [A-31](#)
 - server requests [A-31](#)
- security
 - information on Cisco Security Intelligence Operations [19-10](#)
- security and SSH [11-1](#)
- security information
 - MySDN [7-5](#)
- security policies described [6-1, 7-1, 9-1, 10-1](#)
- sensing interfaces
 - described [5-3](#)
 - modes [5-3](#)
 - PCI cards [5-3](#)
- SensorApp
 - Alarm Channel [A-24](#)
 - Analysis Engine [A-24](#)
 - described [A-3](#)
 - event action filtering [A-25](#)
 - inline packet processing [A-24](#)
 - IP normalization [A-24](#)

- packet flow [A-25](#)
- processors [A-22](#)
- responsibilities [A-22](#)
- risk rating [A-25](#)
- Signature Event Action Processor [A-23, A-25](#)
- TCP normalization [A-24](#)
- Sensor Health gadget
 - configuring [2-4](#)
 - described [2-3](#)
 - metrics [2-4](#)
 - status [2-4](#)
- Sensor Health pane
 - described [15-17](#)
 - field descriptions [15-17](#)
- Sensor Information gadget
 - configuring [2-3](#)
 - described [2-3](#)
- Sensor Key pane
 - button functions [11-7](#)
 - described [11-7](#)
 - field descriptions [11-7](#)
 - sensor SSH key
 - displaying [11-7](#)
 - generating [11-7](#)
 - user roles [11-7](#)
- sensors
 - access problems [C-27](#)
 - asymmetric traffic disabling anomaly detection [C-22](#)
 - blocking itself [12-8](#)
 - configuring to use NTP [4-13](#)
 - corrupted SensorApp configuration [C-38](#)
 - diagnostics reports [16-29](#)
 - disaster recovery [C-6](#)
 - downgrading [20-10](#)
 - incorrect NTP configuration [4-8, C-19](#)
 - initializing [4-1, 17-1, 17-3](#)
 - interface support [5-4](#)
 - IP address conflicts [C-30](#)
 - license [1-10, 15-16](#)
 - logging in
 - SSH [18-11](#)
 - Telnet [18-11](#)
 - loose connections [C-25](#)
 - misconfigured access lists [C-29](#)
 - no alerts [C-34, C-59](#)
 - not seeing packets [C-36](#)
 - NTP time source [4-13](#)
 - NTP time synchronization [4-6, C-18](#)
 - partitions [A-3](#)
 - physical connectivity [C-33](#)
 - preventive maintenance [C-2](#)
 - process not running [C-31](#)
 - rebooting [15-26](#)
 - reimaging [20-1](#)
 - restoring defaults [15-25](#)
 - sensing process not running [C-31](#)
 - setting up [4-1](#)
 - setup command [4-1, 17-1, 17-3, 17-7](#)
 - shutting down [15-26](#)
 - statistics [16-30](#)
 - system information [16-31](#)
 - time sources [4-6, C-18](#)
 - troubleshooting software upgrades [C-56](#)
 - updating [15-21, 15-24](#)
 - upgrading [20-4](#)
 - using NTP time source [4-12](#)
- Sensor Setup window
 - described [3-2](#)
 - Startup Wizard [3-2](#)
- Server Certificate pane
 - button functions [11-11](#)
 - certificate
 - displaying [11-11](#)
 - generating [11-11](#)
 - described [11-11](#)
 - field descriptions [11-11](#)
 - user roles [11-11](#)

- service account
 - creating [C-6](#)
 - described [4-17, A-29, C-5](#)
 - TAC [A-29](#)
 - troubleshooting [A-29](#)
- Service DNS engine
 - described [B-41](#)
 - parameters (table) [B-41](#)
- Service engine
 - described [B-40](#)
 - Layer 5 traffic [B-40](#)
- Service FTP engine
 - described [B-42](#)
 - parameters (table) [B-42](#)
 - PASV port spoof [B-42](#)
- Service Generic engine
 - described [B-43](#)
 - parameters (table) [B-43](#)
- Service H225 engine
 - ASN.1PER validation [B-44](#)
 - described [B-44](#)
 - features [B-45](#)
 - parameters (table) [B-45](#)
 - TPKT validation [B-44](#)
- Service HTTP engine
 - described [8-14, B-46](#)
 - parameters (table) [B-47](#)
- Service IDENT engine
 - described [B-48](#)
 - parameters (table) [B-49](#)
- service-module ids-sensor slot/port session command [18-4, 18-9](#)
- Service MSRPC engine
 - DCS/RPC protocol [8-11, B-49](#)
 - described [8-11, B-49](#)
 - parameters (table) [B-50](#)
- Service MSSQL engine
 - described [B-51](#)
 - MSSQL protocol [B-51](#)
 - parameters (table) [B-51](#)
- Service NTP engine
 - described [B-51](#)
 - parameters (table) [B-51](#)
- Service P2P engine described [B-52](#)
- service packs described [19-3](#)
- service role [18-2, A-28](#)
- Service RPC engine
 - described [8-17, B-52](#)
 - parameters (table) [8-17, B-52](#)
 - RPC portmapper [8-17, B-52](#)
- Service SMB Advanced engine
 - described [B-54](#)
 - parameters (table) [B-54](#)
- Service SNMP engine
 - described [B-56](#)
 - parameters (table) [B-56](#)
- Service SSH engine
 - described [B-56](#)
 - parameters (table) [B-57](#)
- Service TNS engine
 - described [B-57](#)
 - parameters (table) [B-58](#)
- session command
 - AIM-IPS [18-5](#)
 - AIP-SSC-5 [18-6](#)
 - AIP-SSM [18-6](#)
 - IDSM-2 [18-7](#)
 - NME-IPS [18-9](#)
- sessioning
 - AIM-IPS [18-5](#)
 - AIP-SSM [18-6](#)
 - IDSM-2 [18-7](#)
 - NME-IPS [18-10](#)
- setting
 - current KB [16-21](#)
 - system clock [4-15](#)
- setting up
 - sensors [4-1](#)

- terminal servers [18-3, 20-13](#)
- setup
 - automatic [17-1](#)
 - simplified mode [17-1](#)
- setup command [4-1, 17-1, 17-3, 17-7, 17-12, 17-15, 17-20, 17-24](#)
- show events command [C-92, C-93](#)
- show health command [C-74](#)
- show interfaces command [C-91](#)
- show module 1 details command [C-68](#)
- show settings command [15-13, C-17](#)
- show statistics command [C-81, C-82](#)
- show statistics virtual-sensor command [C-26, C-82](#)
- show tech-support command [C-75](#)
- show version command [C-79](#)
- Shut Down Sensor pane
 - configuring [15-26](#)
 - described [15-26](#)
 - user roles [15-26](#)
- shutting down the sensor [15-26](#)
- Sig0 pane
 - field descriptions [7-6](#)
- sig0 pane
 - default [7-3](#)
 - described [7-3](#)
 - signatures
 - assigning actions [7-17](#)
 - cloning [7-14](#)
 - tuning [7-16](#)
 - tabs [7-3](#)
- signature/virus update files described [19-4](#)
- signature definition policies
 - adding [7-2](#)
 - cloning [7-2](#)
 - default policy [7-2](#)
 - deleting [7-2](#)
 - sig0 [7-2](#)
- Signature Definitions pane
 - described [7-2](#)
 - field descriptions [7-2](#)
- signature engines
 - AIC [B-10](#)
 - Atomic [B-13](#)
 - Atomic ARP [B-13](#)
 - Atomic IP [8-13, B-25](#)
 - Atomic IP Advanced [B-15](#)
 - Atomic IPv6 [B-29](#)
 - creating custom signatures [8-2](#)
 - described [B-1](#)
 - event actions [B-7](#)
 - Fixed [B-31](#)
 - Flood [B-33](#)
 - Flood Host [B-34](#)
 - Flood Net [B-34](#)
 - list [B-2](#)
 - Master [B-4](#)
 - Meta [7-21, B-34](#)
 - Multi String [B-36](#)
 - Normalizer [B-37](#)
 - Regex
 - patterns [B-10](#)
 - syntax [B-9](#)
 - Service [B-40](#)
 - Service DNS [B-41](#)
 - Service FTP [B-42](#)
 - Service Generic [B-43](#)
 - Service H225 [B-44](#)
 - Service HTTP [8-14, B-46](#)
 - Service IDENT [B-48](#)
 - Service MSRPC [8-11, B-49](#)
 - Service MSSQL [B-51](#)
 - Service NTP engine [B-51](#)
 - Service P2P [B-52](#)
 - Service RPC [8-17, B-52](#)
 - Service SMB Advanced [B-54](#)
 - Service SNMP [B-56](#)
 - Service SSH engine [B-56](#)
 - Service TNS [B-57](#)
 - State [8-18, B-59](#)

- String [8-19, 8-22, B-60](#)
- supported by IDM [8-2](#)
- Sweep [B-63](#)
- Sweep Other TCP [B-66](#)
- Traffic Anomaly [10-6, B-66](#)
- Traffic ICMP [B-68](#)
- Trojan [B-69](#)
- signature engine update files described [19-5](#)
- Signature Event Action Filter
 - described [9-6, A-26](#)
 - parameters [9-6, A-26](#)
- Signature Event Action Handler described [9-6, A-26](#)
- Signature Event Action Override described [9-6, A-26](#)
- Signature Event Action Processor
 - Alarm Channel [9-6, A-26](#)
 - components [9-6, A-26](#)
 - described [9-6, A-23, A-25, A-26](#)
 - illustration [9-7, A-26](#)
 - logical flow of events [9-7, A-26](#)
- signature fidelity rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 9-3](#)
- signatures
 - adding [7-13](#)
 - alert frequency [7-19](#)
 - assigning actions [7-17](#)
 - cloning [7-15](#)
 - custom [7-5](#)
 - default [7-4](#)
 - described [7-4](#)
 - editing [7-16](#)
 - false positives [7-4](#)
 - no TCP reset [C-53](#)
 - rate limits [12-4](#)
 - subsignatures [7-4](#)
 - tuned [7-4](#)
 - tuning [7-16](#)
- signature updates installation time [15-20](#)
- signature variables
 - adding [7-27](#)
 - deleting [7-27](#)
 - described [7-26](#)
 - editing [7-27](#)
- Signature Variables tab
 - configuring [7-27](#)
 - field descriptions [7-27](#)
- Signature Wizard
 - alert behavior [8-24](#)
 - Alert Response window field descriptions [8-24](#)
 - Atomic IP Engine Parameters window field descriptions [8-13](#)
 - described [8-1](#)
 - ICMP Traffic Type window field descriptions [8-12](#)
 - Inspect Data window field descriptions [8-12](#)
 - MSRPC Engine Parameters window field descriptions [8-11](#)
 - protocols [8-10](#)
 - Protocol Type window field descriptions [8-10](#)
 - Service HTTP Engine Parameters window field descriptions [8-14](#)
 - Service RPC Engine Parameters window field descriptions [8-17](#)
 - Service Type window field descriptions [8-13](#)
 - signature identification [8-11](#)
 - Signature Identification window field descriptions [8-11](#)
 - State Engine Parameters window field descriptions [8-18](#)
 - String ICMP Engine Parameters window field descriptions [8-19](#)
 - String TCP Engine Parameters window field descriptions [8-19](#)
 - String UDP Engine Parameters window field descriptions [8-22](#)
 - supported signature engines [8-2](#)
 - Sweep Engine Parameters window field descriptions [8-23](#)
 - TCP Sweep Type window field descriptions [8-13](#)
 - TCP Traffic Type window field descriptions [8-12](#)
 - UDP Sweep Type window field descriptions [8-12](#)

- UDP Traffic Type window field descriptions [8-12](#)
- using [8-5](#)
- Welcome window field descriptions [8-10](#)
- SNMP
 - configuring [13-2](#)
 - described [13-1](#)
 - Get [13-1](#)
 - GetNext [13-1](#)
 - Set [13-1](#)
 - supported MIBs [13-6, C-21](#)
 - Trap [13-1](#)
- SNMP General Configuration pane
 - configuring [13-2](#)
 - described [13-2](#)
 - field descriptions [13-2](#)
 - user roles [13-2](#)
- SNMP traps
 - configuring [13-4](#)
 - described [13-1](#)
- SNMP Traps Configuration pane
 - described [13-3](#)
 - field descriptions [13-4](#)
 - user roles [13-3](#)
- software architecture
 - ARC (illustration) [A-12](#)
 - IDAPI (illustration) [A-30](#)
- software bypass
 - supported configurations [5-10](#)
 - with hardware bypass [5-10](#)
- software downloads Cisco.com [19-1](#)
- software file names
 - recovery (illustration) [19-6](#)
 - signature/virus updates (illustration) [19-5](#)
 - signature engine updates (illustration) [19-5](#)
 - system image (illustration) [19-6](#)
- software release examples
 - platform-dependent [19-7](#)
 - platform identifiers [19-7](#)
 - platform-independent [19-6](#)
- software updates
 - supported FTP servers [15-19, 20-2](#)
 - supported HTTP/HTTPS servers [15-19, 20-2](#)
- SPAN port issues [C-33](#)
- SSH
 - security [11-1](#)
 - understanding [11-1](#)
- SSH Server
 - private keys [A-21](#)
 - public keys [A-21](#)
- standards
 - IDCONF [A-31](#)
 - IDIOM [A-30](#)
 - SDEE [A-31](#)
- standards CIDEE [A-32](#)
- Startup Wizard
 - access lists [3-3](#)
 - adding virtual sensors [3-12](#)
 - Add Virtual Sensor dialog box [3-11](#)
 - described [3-1](#)
 - Inline Interface Pair window
 - described [3-8](#)
 - field descriptions [3-8](#)
 - Inline VLAN Pairs window configuration [3-10](#)
 - Interface Selection window [3-8](#)
 - Interface Summary window [3-6](#)
 - Sensor Setup window
 - configuring [3-4](#)
 - field descriptions [3-2](#)
 - Traffic Inspection Mode window [3-8](#)
 - Virtual Sensors window
 - described [3-11](#)
 - field descriptions [3-11](#)
- State engine
 - Cisco Login [8-18, B-59](#)
 - described [8-18, B-59](#)
 - LPR Format String [8-18, B-59](#)
 - parameters (table) [B-59](#)
 - SMTP [8-18, B-59](#)

- Statistics pane
 - button functions [16-30](#)
 - categories [16-30](#)
 - described [16-30](#)
 - using [16-30](#)
- statistics viewing [16-30](#)
- String engine described [8-19, 8-22, B-60](#)
- String ICMP engine parameters (table) [B-61](#)
- String TCP engine parameters (table) [B-61](#)
- String UDP engine parameters (table) [B-62](#)
- subinterface 0 described [5-15](#)
- subsignatures described [7-4](#)
- summarization
 - described [6-6, 9-5](#)
 - Fire All [6-7, 9-5](#)
 - Fire Once [6-7, 9-6](#)
 - Global Summarization [6-7, 9-6](#)
 - Meta engine [6-7, 9-5](#)
 - Summary [6-7, 9-5](#)
- Summarizer described [6-31, 9-33](#)
- Summary pane
 - button functions [5-16](#)
 - described [5-15](#)
 - field descriptions [3-7, 5-16](#)
- supported
 - FTP servers [15-19, 20-2](#)
 - HTTP/HTTPS servers [15-19, 20-2](#)
 - IDM platforms [1-3](#)
 - IDSM-2 configurations [C-62](#)
 - IPS interfaces for CSA MC [14-4](#)
- Sweep engine
 - described [8-22, B-63](#)
 - parameters (table) [B-64, B-66](#)
- Sweep Other TCP engine described [B-66](#)
- switch commands for troubleshooting [C-63](#)
- system architecture
 - directory structure [A-32](#)
 - supported platforms [A-1](#)
- system clock setting [4-15](#)
- system components IDAPI [A-30](#)
- System Configuration Dialog
 - described [17-2](#)
 - example [17-2](#)
- system image
 - installing
 - AIM-IPS [20-22](#)
 - AIP-SSC-5 [20-25](#)
 - AIP-SSM [20-25](#)
 - IDSM-2 (Catalyst software) [20-28](#)
 - IDSM2 (Cisco IOS software) [20-29](#)
 - IPS-4240 [20-14](#)
 - IPS-4255 [20-14](#)
 - IPS-4260 [20-18](#)
 - IPS 4270-20 [20-20](#)
 - NME-IPS [20-39](#)
- System Information pane
 - described [16-31](#)
 - using [16-31](#)
- system information viewing [16-31](#)
- system requirements IDM [1-3](#)

T

- TAC
 - service account [4-17, A-29, C-5](#)
 - show tech-support command [C-75](#)
- target value rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 6-18, 6-19, 9-3, 9-20, 9-21](#)
- TCP fragmentation described [B-38](#)
- TCP Protocol tab
 - described [10-16, 10-23, 10-29](#)
 - enabling TCP [10-16](#)
 - external zone [10-29](#)
 - field descriptions [10-16](#)
 - illegal zone [10-23](#)
- TCP reset interfaces
 - conditions [5-7](#)

- described [5-6](#)
- list [5-7](#)
- TCP resets
 - IDSM-2 port [C-67](#)
 - IDSM2 port [C-67](#)
 - not occurring [C-53](#)
- TCP stream reassembly
 - described [7-43](#)
 - mode [7-48](#)
 - parameters (table) [7-43](#)
 - signatures (table) [7-43](#)
- terminal server setup [18-3, 20-13](#)
- testing fail-over [5-10](#)
- TFN2K
 - described [B-68](#)
 - Trojans [B-69](#)
- TFTP servers
 - maximum file size limitation [20-13](#)
 - RTT [20-13](#)
- threat rating described [6-6, 9-4](#)
- Thresholds for KB Name window
 - described [16-17](#)
 - field descriptions [16-18](#)
 - filtering information [16-18](#)
- time and the sensor [4-6, C-18](#)
- time correcting on the sensor [4-11, C-20](#)
- Time pane
 - configuring [4-10](#)
 - described [4-6](#)
 - field descriptions [4-9](#)
 - user roles [4-6](#)
- time sources
 - AIM-IPS [4-7, C-18](#)
 - AIP-SSM [4-7, C-19](#)
 - appliances [4-7, C-18](#)
 - IDSM-2 [4-7, C-18](#)
 - NME-IPS [4-7, C-18](#)
- time synchronization and IPS modules [4-8, C-19](#)
- TLS
 - described [4-3](#)
 - handshaking [1-6, 11-8](#)
 - IDM [1-6, 11-8](#)
- Top Applications gadget
 - configuring [2-7](#)
 - described [2-7](#)
- Traffic Anomaly engine
 - described [10-6, B-66](#)
 - protocols [10-6, B-66](#)
 - signatures [10-6, B-66](#)
- traffic flow notifications
 - configuring [5-28](#)
 - described [5-28](#)
- Traffic Flow Notifications pane
 - configuring [5-28](#)
 - field descriptions [5-28](#)
 - user roles [5-28](#)
- Traffic ICMP engine
 - DDoS [B-68](#)
 - described [B-68](#)
 - LOKI [B-68](#)
 - parameters (table) [B-69](#)
 - TFN2K [B-68](#)
- Traffic Inspection Mode window described [3-8](#)
- Traps Configuration pane configuration [13-4](#)
- trial license key [1-8, 15-14](#)
- Tribe Flood Network. See TFN.
- Tribe Flood Network 2000. See TFN2K.
- Trojan engine
 - BO2K [B-69](#)
 - described [B-69](#)
 - TFN2K [B-69](#)
- Trojans
 - BO [B-69](#)
 - BO2K [B-69](#)
 - LOKI [B-68](#)
 - TFN2K [B-69](#)

troubleshooting

AIP SSM

failover scenarios [C-70](#)

AIP-SSM

commands [C-68](#)debugging [C-69](#)recovering [C-69](#)reset [C-68](#)Analysis Engine busy [C-58](#)applying software updates [C-55](#)

ARC

blocking not occurring for signature [C-44](#)device access issues [C-42](#)enabling SSH [C-44](#)inactive state [C-40](#)misconfigured master blocking sensor [C-45](#)verifying device interfaces [C-43](#)automatic updates [C-55](#)cannot access sensor [C-27](#)cidDump [C-96](#)cidLog messages to syslog [C-52](#)communication [C-27](#)corrupted SensorApp configuration [C-38](#)debug logger zone names (table) [C-51](#)debug logging [C-47](#)disaster recovery [C-6](#)duplicate sensor IP addresses [C-30](#)enabling debug logging [C-47](#)external product interfaces [14-10, C-24](#)gathering information [C-74](#)

IDM

cannot access sensor [C-58](#)will not load [C-57](#)

IDSM-2

command and control port [C-66](#)diagnosing problems [C-61](#)not online [C-65, C-66](#)serial cable [C-67](#)status indicator [C-63](#)switch commands [C-63](#)IME time synchronization [C-60](#)IPS modules time drift [4-8, C-19](#)manual block to bogus host [C-44](#)misconfigured access list [C-29](#)no alerts [C-34, C-59](#)NTP [C-53](#)password recovery [15-12, C-17](#)physical connectivity issues [C-33](#)preventive maintenance [C-2](#)reset not occurring for a signature [C-53](#)sensing process not running [C-31](#)sensor events [C-92](#)sensor loose connections [C-25](#)sensor not seeing packets [C-36](#)sensor software upgrade [C-56](#)service account [4-17, C-5](#)show events command [C-92](#)show interfaces command [C-91](#)show statistics command [C-81](#)show tech-support command [C-75, C-77](#)show version command [C-78, C-79](#)software upgrades [C-54](#)SPAN port issue [C-33](#)upgrading to 6.x [C-54](#)verifying Analysis Engine is running [C-23](#)verifying ARC status [C-39](#)

Trusted Hosts pane

configuring [11-10](#)described [11-9](#)field descriptions [11-9](#)tuned signatures described [7-4](#)

tuning

AIC signatures [7-38](#)IP fragment reassembly signatures [7-42](#)signatures [7-16](#)turning off anomaly detection [10-34](#)

U

UDP Protocol tab

- described [10-17, 10-23, 10-29](#)
- enabling UDP [10-17](#)
- external zone [10-29](#)
- field descriptions [10-29](#)
- illegal zone [10-23](#)

unassigned VLAN groups described [5-15](#)

unauthenticated NTP [4-6, 4-13, C-18](#)

UNIX-style directory listings [15-19](#)

Update Sensor pane

- configuring [15-24](#)
- described [15-23](#)
- field descriptions [15-23](#)
- user roles [15-23](#)

updating

- Cisco.com [15-23](#)
- FTP server [15-23](#)
- Home pane [1-2](#)
- sensors [15-24](#)

upgrade command [20-3, 20-5](#)

upgrading

- 6.x [C-54](#)
- maintenance partition
 - IDSM-2 (Catalyst software) [20-38](#)
 - IDSM-2 (Cisco IOS software) [20-38](#)
- minimum required version [19-8](#)
- recovery partition [20-6, 20-11](#)
- sensors [20-4](#)
- to 6.2 [19-8](#)

uploading KBs

- FTP [16-24](#)
- SCP [16-24](#)

Upload Knowledge Base to Sensor dialog box

- described [16-24](#)
- field descriptions [16-24](#)

URLs for Cisco Security Intelligence Operations [19-10](#)

Users pane

- configuring [4-17](#)
- field descriptions [4-16](#)
- user roles [A-28](#)

using

- debug logging [C-47](#)
- TCP reset interfaces [5-7](#)

V

VACLs

- described [12-2](#)
- Post-Block [12-21](#)
- Pre-Block [12-21](#)

verifying

- NTP configuration [4-8](#)
- password recovery [15-13, C-17](#)
- sensor initialization [17-27](#)
- sensor setup [17-27](#)

viewing

- IP logs [16-14](#)
- statistics [16-30](#)
- system information [16-31](#)

virtual sensors

- adding [3-12, 6-11](#)
- default virtual sensor [6-3, 6-8](#)
- deleting [6-11](#)
- described [6-2, 6-8](#)
- editing [6-11](#)
- stream segregation [6-4](#)

Virtual Sensors window described [3-11](#)

VLAN groups

- 802.1q encapsulation [5-15](#)
- configuration restrictions [5-9](#)
- configuring [5-24](#)
- deploying [5-23](#)
- described [5-14](#)
- switches [5-23](#)

VLAN Groups pane

- configuring [5-24](#)
- described [5-23](#)
- field descriptions [5-24](#)
- user roles [5-23](#)

VLAN IDs [5-23](#)

VLAN Pairs pane

- configuring [5-22](#)
- describing [5-21](#)
- field descriptions [5-21](#)

vulnerable OSes field

- described [B-6](#)

Z

zones

- external [10-4](#)
- illegal [10-4](#)
- internal [10-4](#)

W

watch list rating

- calculating risk rating [6-6, 9-4](#)
- described [6-6, 9-4](#)

Web Server

- described [A-3, A-22](#)
- HTTP 1.0 and 1.1 support [A-22](#)
- private keys [A-21](#)
- public keys [A-21](#)
- SDEE support [A-22](#)

worms

- Blaster [10-2](#)
- Code Red [10-2](#)
- histograms [10-12, 16-16](#)
- Nimble [10-2](#)
- protocols [10-3](#)
- Sasser [10-2](#)
- scanners [10-3](#)
- Slammer [10-2](#)
- SQL Slammer [10-2](#)

