



## INDEX

---

### A

antivirus utilities, requirement to disable [3-5](#),  
[5-6](#)

audience for this document [1-viii](#)

Auto Update Server (AUS)

documentation [1-xi](#)

licensing [1-9](#)

overview [1-4](#)

---

### B

bootstrapping devices [7-4](#)

browsers

requirements

cache [7-2](#)

client [2-9](#)

server [2-6](#)

*See also* Internet Explorer

*See also* Mozilla

---

### C

C/C++ library files, where stored [1-11](#)

casuser

permissions

for running getCerts.pl [4-12](#)

for running loadCerts.pl [4-12](#)

cautions, significance of [1-ix](#)

CD-ONE

unsupported use [3-4](#)

certificate authentication

disabled in previous version of Security  
Manager

and adding certificates [4-11](#)

enabled in previous version of Security  
Manager

and certificate data store [4-11](#)

certificates. *See* digital certificates

certificate thumbprints

adding to Security Manager

after upgrade from 3.0.1 [4-11](#)

from CLI [4-11](#)

using perl scripts [4-11](#)

checklists

client, browser best practices [7-2](#)

server

enhancing performance [3-2](#)

installation readiness [3-5](#)

- post-installation tasks **6-2**
  - security best practices **6-4**
- Cisco Marketplace **1-xiii**
- Cisco Press **1-xiii**
- Cisco Product Quick Reference Guide, obtaining **1-xiii**
- Cisco product security
  - PSIRT **1-xiii**
  - vulnerability policy portal **1-xiii**
- Cisco Security Agent
  - documentation **C-1**
  - installation, conditions for **1-7**
  - IPS Event Viewer and modifying policy **1-5**
  - modifying policy for IPS Event Viewer
    - automatically **1-5**
    - manually **1-5**
  - not installed on Security Manager server
    - automatically modifying policy for IPS Event Viewer **1-5**
  - overview **1-7**
  - policies
    - exported, on DVD **1-7, 3-3**
    - imported, requirement to reconcile **3-3**
    - standalone agent **1-7, C-1**
  - preexisting on Security Manager server
    - manually modifying policy for IPS Event Viewer **1-5**
  - security levels
    - changing **C-3**
    - default **C-3**
    - understanding **C-3**
  - troubleshooting **B-19, C-1**
  - uninstalling, recommendation against **3-3, B-20**
- Cisco Security Manager
  - basic concepts **7-4**
  - getting started **7-4**
  - late-breaking information about **1-viii**
  - learning more about **7-4**
  - logging in **7-3**
  - overview **1-3**
  - using **7-4**
- Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)
  - date and time synchronization **3-5**
  - interoperation with **3-5**
  - overview **1-vii**
- Cisco security strategies
  - Design Zones **1-viii**
- CiscoView Device Manager
  - unsupported use **3-4**
- CiscoWorks
  - Common Services, overview **1-2**
  - Monitoring Center for Performance. *See* Performance Monitor
  - Monitoring Center for Security. *See* Security Monitor
  - TCP ports
    - Daemon Manager **2-4**
    - HTTP **2-3**

- VPN/Security Management Solution (VMS)
    - migrating data to Security Manager [1-x](#)
  - client software
    - installing [5-5](#)
    - InstallShield database corruption [5-5](#)
    - logging in to a server [7-3](#)
    - using [7-3](#)
  - client systems
    - deleting Temp files [5-7](#)
    - file locations on [1-11, 5-9](#)
    - recommendation to delete Temp files [5-10](#)
    - video (graphics) card drivers
      - confirming installed versions [2-8](#)
      - upgrading [2-8](#)
  - CMFLOCK.TXT file, deleting [4-24](#)
  - Common Services
    - documentation [2-2](#)
    - installing [2-1](#)
    - licensing [1-9](#)
    - required version [1-2](#)
    - requirement to use [2-1](#)
  - CSTM TCP port [2-4](#)
- 
- D**
- database TCP port [2-4](#)
  - date and time settings
    - caution against changing [3-5](#)
    - recommendation to synchronize [2-2, 3-5](#)
    - use of NTP servers [2-2](#)
  - Design Zones [1-viii](#)
  - device bootstrapping [7-4](#)
  - device certificates
    - before adding to Security Manager
      - checking validity [4-12](#)
      - validating encryption keys [4-12](#)
      - verifying end-host identity [4-12](#)
      - verifying signature [4-12](#)
  - device credentials
    - exporting from DCR as a .csv file
      - before adding certificates to Security Manager [4-12](#)
      - before running getCerts.pl [4-12](#)
  - device credentials repository (DCR)
    - exporting certificates from
      - using getCerts.pl [4-12](#)
    - server process [3-5](#)
    - TCP port [2-4](#)
    - troubleshooting [3-5](#)
  - digital certificates
    - adding to Security Manager
      - using getCerts.pl [4-11](#)
      - using loadCerts.pl [4-11](#)
    - adding to Security Manager in bulk in one step [4-11](#)
    - confirming validity
      - before using getCerts.pl [4-12](#)
    - refreshing cache

- and using loadCerts.pl [4-13](#)
- requirement to create [6-2](#)
- retrieving
  - after upgrade from 3.0.1 [4-11](#)
  - from devices in bulk [4-11](#)
  - using perl scripts [4-11](#)
- retrieving for unreachable devices [4-14](#)
- troubleshooting [3-5](#)
- directory encryption, restriction against [2-7, 3-6](#)
- documentation
  - audience for this [1-viii](#)
  - on Cisco.com [1-xiii](#)
  - ordering [1-xiii](#)
  - reviewing updated [1-ix](#)
  - typographical conventions in [1-viii](#)
- documentation, obtaining
  - Auto Update Server [1-xi](#)
  - Cisco Security Agent [C-1](#)
  - Cisco Security Manager [1-x](#)
  - Common Services [1-xi](#)
  - Performance Monitor [1-xiii](#)
  - Resource Manager Essentials (RME) [1-xii](#)
- documentation feedback, sending to Cisco [1-viii, 1-xiii](#)
- domain controllers (primary or backup), unsupported use [2-7](#)

---

## E

- encrypted directories, restriction against [2-7, 3-6](#)
- evaluation license
  - device count limitations [4-6](#)
  - duration [4-6](#)
  - upgrading to permanent license [1-8](#)
- Event Services software TCP port requirements
  - HTTP [2-4](#)
  - listening [2-4](#)
  - routing [2-4](#)
  - services [2-4](#)

---

## F

- FAQs, in the troubleshooting guide [1-x](#)
- files, where stored
  - Cisco Security Agent
    - logs [C-2](#)
    - policies [1-7, 3-3](#)
  - on client systems [1-11](#)
  - on servers [1-11](#)
- file system recommendations [2-6](#)

---

## G

- gatekeeper HIPO TCP port [2-4](#)
- getCerts.pl
  - access permissions for running [4-12](#)

adding certificates to Security Manager **4-11**

confirming validity of certificates

- before using -a argument **4-12**

device credentials, exporting to .csv file **4-11**

syntax, description **4-12**

- using in conjunction with loadCerts.pl **4-11**

getting started with Cisco Security Manager **7-4**

---

## H

HTTP TCP port **2-3**

---

## I

installation

- client software **5-5**
- InstallShield database corruption **5-5**
- planning and preparation **1-viii**
- servers
  - dependencies **2-1**
  - general requirements **2-1**
  - GUI reference **A-1**
  - post-installation tasks **6-2**
  - preparatory tasks **3-1**
  - starting an installation **4-5**
  - troubleshooting **4-5**
  - verifying **6-4**

installing server software **4-4**

Internet Explorer

- cache size requirement **5-6, 5-10**
- confirming the installed Java version **2-10**
- security settings **5-6, 5-10**
- versions supported **2-6, 2-9**
- See also* browsers
- See also* Mozilla

Internet Information Server (IIS)

- conflict with Security Manager **3-4, 3-6**
- requirement to uninstall **3-4, 3-6**

Internet Inter-ORB Protocol (IIOP) TCP port **2-3**

IP addresses

- disabling dynamic addresses **3-5**
- static address requirement **2-7**
- using a static address **3-5**

IPS Event Viewer client

- communicating with server **1-5**

IPS Event Viewer server

- communicating with client
  - modifying firewall software policy **1-5**
- installing on a server with CSA **1-5**

IPS Manager

- importing IPS MC 2.2 data **4-18**
- migrating from IPS MC **4-3, 4-18**
- prerequisites to import IPS MC data **4-18**
- time required to import IPS MC data **4-19**
- See also* IPS MC

IPS MC

backing up server data [4-3](#)  
 exporting data [4-3](#)  
 migrating to IPS Manager [4-3, 4-18](#)  
 securing the backed-up data [4-3](#)  
*See also* IPS Manager

---

## J

### Java

confirming the installed version [2-10](#)  
 embedded version on client systems [2-10](#)  
 enabling [7-2](#)

JavaScript, enabling [7-2](#)

---

## L

language versions supported (Windows)

server [2-6, 2-9](#)

LAN Management Solution (LMS),  
 unsupported use [3-2, 3-4](#)

licenses

file locations for

Performance Monitor [1-7](#)

RME [1-6](#)

installing [1-10](#)

Product Authorization Key (PAK) [1-9](#)

Security Manager kit part numbers [1-8](#)

settings [1-8](#)

Software License Claim Certificate [1-9](#)

understanding [1-8](#)

upgrading [1-8](#)

uploading new [1-8](#)

working with [1-8](#)

license server TCP port [2-4](#)

loadCerts.pl

access permissions for running [4-12](#)

adding certificates to Security Manager  
 using the .csv file with exported  
 details [4-12](#)

enabling certificate authentication  
 after running the script [4-12](#)

retrieving certificates

for unreachable devices [4-14](#)

running in verbose mode [4-14](#)

running when Security Manager is  
 launched

refreshing certificate cache [4-13](#)

syntax, description [4-14](#)

---

## M

McAfee Antivirus

incompatibility [5-6](#)

reenabling [5-9](#)

requirement to disable [5-6](#)

memory (RAM)

client requirements [2-9](#)

server requirements [2-6](#)

modifying firewall software policy [1-5](#)

Monitoring Center for Performance. *See*  
Performance Monitor

## Mozilla

- confirming the installed Java version [2-10](#)
- security settings [5-6, 5-10](#)
- versions supported [2-6, 2-9](#)

---

## N

NETBIOS, recommendation to disable [3-4](#)

Networking Professionals Connection [1-xiii](#)

network protocols, recommendation to  
disable [3-4](#)

network shares, recommendation to avoid [3-4](#)

Network Time Protocol (NTP) server,  
recommendation to use [2-2, 3-5](#)

Norton Internet Security 2005

- incompatibility [5-6, 5-9](#)
- requirement to disable [5-6](#)
- requirement to uninstall [5-9](#)

NTFS file system, requirement to use [2-6](#)

---

## O

ODBC driver manager

- confirming the installed version [2-6](#)
- requirements [2-6](#)
- working with Sybase files [2-6](#)

OGS TCP port [2-4](#)

online help, tips for viewing [5-1](#)

operating systems

on client systems

- Windows 2000 [2-9](#)
- Windows 2003 [2-9](#)
- Windows XP Professional [2-9](#)

on servers

- Windows 2000 [2-6](#)
- Windows 2003 Server [2-6](#)

Osagent UDP port [2-4](#)

overview [1-1](#)

---

## P

passwords

- admin account [4-6](#)
- requirement to use identical passwords [4-6](#)
- security basics [D-4](#)
- strong passwords
  - characteristics [D-3](#)
  - definition [3-3](#)
  - how to require [3-3](#)
  - recommendations [D-3](#)
- System Identity Account [4-6](#)

peer support, Networking Professionals  
Connection [1-xiii](#)

Performance Monitor

- availability [1-xiii](#)
- documentation [1-xiii](#)
- entitlement to install [1-7](#)
- license file location [1-7](#)

- licensing [1-9](#)
- overview [1-7](#)
- perl scripts
  - exporting certificates into a .csv file [4-11](#)
  - loading certificates into Security Manager in bulk [4-11](#)
  - retrieving certificates
    - after upgrading from 3.0.1 [4-11](#)
  - See also* `getCerts.pl`
  - See also* `loadCerts.pl`
- permanent license, upgrading from evaluation license [1-8](#)
- point patches
  - applying to a client [5-10](#)
  - applying to a server [4-21](#)
  - caution against accepting from a third-party [4-20](#)
  - default location on client systems [5-12](#)
  - deleting Temp files on client systems [5-7](#)
  - obtaining [4-20](#)
  - recommendation to delete Temp files on client systems [5-10](#)
  - version mismatch [5-10](#)
- popup blockers
  - configuring [5-1, 7-2](#)
  - conflicting with other installed software [3-3](#)
  - disabling [5-1, 7-2](#)
  - requirements [7-2](#)
  - troubleshooting [5-1, 7-2](#)
- ports

- required for TCP [2-2](#)

- required for UDP [2-2](#)

- product registration. *See* licenses

- PSIRT [1-xiii](#)

- publications, obtaining additional [1-xiii](#)

---

## R

- related documentation, obtaining [1-xi](#)

- Remote Copy Protocol TCP port [2-3](#)

- removable media drives, security implications if compromised [6-4](#)

- requirements

- client system [2-8](#)

- servers

- installation, general [2-1](#)

- system [2-5](#)

- Resource Manager Essentials (RME)

- documentation [1-xii](#)

- entitlement to install [1-6](#)

- installing [1-6](#)

- license file location [1-6](#)

- licensing [1-9](#)

- overview [1-6](#)

---

## S

- Secure Shell (SSH) TCP port [2-3](#)

- security

- advisories [1-xiii](#)
- incidents, obtaining assistance [1-xiii](#)
- news from Cisco
  - registering to receive [1-xiii](#)
  - RSS feed URL [1-xiii](#)
- notices [1-xiii](#)
- PSIRT [1-xiii](#)
- vulnerabilities, reporting [1-xiii](#)
- Security Manager database TCP port [2-4](#)
- Security Monitor [4-3](#)
- server
  - configuration
    - boot settings [3-4](#)
    - date and time settings [3-5](#)
  - file locations
    - database files [1-11](#)
    - log files [1-11](#)
    - miscellaneous files [1-11](#)
  - installations
    - best practices [3-1](#)
    - dependencies [2-1](#)
    - procedures [4-1](#)
  - performance
    - best practices for enhancing [3-1](#)
    - operating environment [2-5, 4-4](#)
  - preparation checklists [3-1](#)
  - processes, verifying status [6-5](#)
  - traffic
    - required inbound ports [2-2](#)
    - required outbound ports [2-2](#)
  - service agreement contracts [1-8](#)
  - service packs
    - applying to a client [5-10](#)
    - applying to a server [4-21](#)
    - caution against accepting from a third-party [4-20](#)
    - default location on client systems [5-12](#)
    - deleting Temp files on client systems [5-7](#)
    - obtaining [4-20](#)
    - recommendation to delete Temp files on client systems [5-10](#)
    - version mismatch [5-10](#)
  - service requests
    - submitting [1-xiii](#)
  - services
    - minimum required for Windows [3-4](#)
    - required for TCP [2-2](#)
    - required for UDP [2-2](#)
  - SNMP polling UDP port [2-3](#)
  - SNMP trap UDP port [2-3](#)
  - software updates. *See* point patches
  - SSL certificate invalidation [3-5](#)
  - SSL mode (for HTTP server) TCP port [2-3](#)
  - support
    - Networking Professionals Connection [1-xiii](#)
    - obtaining from Cisco [1-xiii](#)
    - service agreement contracts [1-8](#)
    - Software Application Support contracts [1-8](#)

Sybase, requirement to disable [3-6, 4-5](#)

Sybase database files, requirement to use correct ODBC version [2-6](#)

Syslog UDP port [2-3](#)

## T

TACACS+ TCP port [2-3](#)

TCP

- list of required ports [2-2](#)

- list of required services [2-2](#)

technical support (TAC)

- obtaining [1-xiii](#)

- URL for service requests [1-xiii](#)

Telnet TCP port [2-3](#)

Terminal Services

- requirements [2-7, 3-6](#)

- unsupported configuration [2-7](#)

Tomcat

- Ajp13 connector TCP port [2-4](#)

- global library files, where stored [1-11](#)

- shutdown TCP port [2-4](#)

training, obtaining [1-xiii](#)

Trivial File Transfer Protocol (TFTP) UDP port [2-3](#)

troubleshooting

- antivirus scanners [3-3](#)

- Cisco Security Agent

- blocking a valid operation [B-21](#)

- blocking network access [B-19](#)

- diagnostic utility [B-21](#)

- icon appearance changed in system tray [B-20](#)

- obtaining a revised agent from TAC [B-20](#)

- recognizing when the agent is disabled [B-20](#)

- security level is High [B-19](#)

- setting the security level to Medium [B-19](#)

- untrusted rootkit detected [B-19](#)

- using the log file [B-19](#)

- collecting server troubleshooting information [B-22](#)

- DCRServer process does not start [3-5](#)

- error messages

- client installation [B-11](#)

- server installation [B-2](#)

- server uninstallation [B-7](#)

- file contents cannot be unpacked [4-5](#)

- file corruption

- executable file [4-5](#)

- host-based intrusion software [3-3](#)

- incorrect GUI [2-8, 6-5, B-5](#)

- installation

- does not run [B-18](#)

- hangs [B-4, B-14](#)

- reviewing log files [B-24](#)

- interoperation with CS-MARS [3-5](#)

- invalid SSL certificate [3-5](#)

- java.security.cert errors [3-5](#)

- mapped drives [B-6](#)
- missing
  - GUI [B-5](#)
  - product features [B-5](#)
- popup blockers [3-3, 5-1, 7-2](#)
- security software conflicts [3-3](#)
- server processes
  - changing [B-23](#)
  - restarting [B-23](#)
  - viewing [B-23](#)
- server self-test [B-21](#)
- uninstallation
  - does not run [B-18](#)
  - hangs [B-9](#)
  - using MDCSupport.exe [B-22](#)
- troubleshooting guide, obtaining [1-x](#)
- typographical conventions in this document [1-viii](#)
- recommendation to restart servers [4-24](#)
- servers
  - deleting CMFLOCK.TXT [4-24](#)
  - failure to delete CSCOpX/bin folder [4-24](#)
  - server software [4-24](#)
- updates. *See* point patches
- upgrading from
  - an earlier release [4-8](#)
  - VMS [4-8](#)
- user accounts
  - admin [D-1](#)
  - casuser [D-1](#)
  - System Identity [D-2](#)
  - understanding [D-1](#)
- user permissions, understanding [D-2](#)
- using Security Manager [7-4](#)

---

## U

- UDP
  - list of required ports [2-2](#)
  - list of required services [2-2](#)
- uninstallation
  - cautions against
    - uninstalling from infected servers [4-23](#)
  - InstallShield database corruption [5-12](#)
  - recommendation to restart client systems [5-13](#)

---

## V

- verifying an installation [6-4](#)

---

## W

- web context files, where stored [1-11](#)
- Windows services, required [3-4](#)

