



## INDEX

---

### A

- antivirus utilities, requirement to disable [3-4](#)
- assigning
  - AUS to devices
    - after migration [5-8](#)
  - Configuration Engines to devices
    - after migration [5-8](#)
- audience for this document [1-xii](#)
- AUS-managed devices
  - association with AUS
    - after migration [5-8](#)
  - migrating
    - servers for [5-8](#)
- Auto Update Server (AUS)
  - assigning to devices
    - after migration [5-8](#)
  - documentation [1-xiv](#)
  - downgrading [5-12](#)
  - importing from DCR
    - after migration [5-8](#)
  - licensing [1-6](#)
  - migrating
    - for AUS-managed devices [5-8](#)
  - overview [1-3](#)
  - upgrading [5-4](#)

---

### B

- backing up
  - across mapped drives [5-5](#)
  - before upgrade [5-5](#)
  - database for downgrade [5-12](#)

- interference with network management applications [5-5](#)

- Security Manager database [5-5](#)

- backup and restore

- upgrade using, definition [5-1](#)

- upgrade using, procedure [5-4](#)

- bootstrapping devices [8-5](#)

- browsers

- requirements

- cache [6-1](#)

- client [2-6](#)

- server [2-4](#)

- See also* Firefox

- See also* Internet Explorer

---

### C

- C/C++ library files, where stored [1-7](#)

- Catalyst 6500 Series switches

- client system

- retrieval of inventory details [5-10](#)

- migrating to 3.2 [5-9](#)

- migration report

- after upgrading to 3.2 [5-10](#)

- viewing on client systems after upgrade [5-10](#)

- cautions

- regarding

- system time, changing after installing RME [7-2](#)

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

- CD-ONE

- unsupported use [3-3](#)

- certificate authentication

- disabled in previous version of Security Manager

- and adding certificates [5-6](#)
  - enabled in previous version of Security Manager
    - and certificate data store [5-6](#)
- certificates. *See* digital certificates
- certificate thumbprints
  - adding to Security Manager
    - after upgrade from 3.0.2 [5-6](#)
    - from CLI [5-6](#)
    - using perl scripts [5-6](#)
- checklists
  - client, browser best practices [6-1](#)
  - server
    - enhancing performance [3-1](#)
    - installation readiness [3-4](#)
    - post-installation tasks [8-1](#)
    - security best practices [8-4](#)
- Cisco 7600 Series routers
  - client system
    - retrieval of inventory details [5-10](#)
  - migrating to 3.2 [5-9](#)
  - migration report
    - after upgrading to 3.2 [5-10](#)
  - viewing on client systems after upgrade [5-10](#)
- Cisco Marketplace [1-xv](#)
- Cisco Press [1-xv](#)
- Cisco Product Quick Reference Guide, obtaining [1-xv](#)
- Cisco product security
  - PSIRT [1-xv](#)
  - SAFE blueprint [1-xii](#)
  - vulnerability policy portal [1-xv](#)
- Cisco Security Agent
  - customized, standalone version
    - overwritten during installation [5-5](#)
  - fully configurable version
    - not overwritten during installation [5-5](#)
  - installing with Security Manager server [5-5](#)
  - not uninstalled with server uninstallation [5-5](#)
- Cisco Security Agent
  - documentation [B-1](#)
- installation, conditions for [1-5](#)
- IPS Event Viewer and modifying policy [1-4](#)
- modifying policy for IPS Event Viewer
  - automatically [1-4](#)
  - manually [1-4](#)
- not installed on Security Manager server
  - automatically modifying policy for IPS Event Viewer [1-4](#)
- overview [1-5](#)
- policies
  - exported, on DVD [1-5, 3-2](#)
  - imported, requirement to reconcile [3-2](#)
  - standalone agent [1-5, B-1](#)
- preexisting on Security Manager server
  - manually modifying policy for IPS Event Viewer [1-4](#)
- security levels
  - changing [B-2](#)
  - default [B-2](#)
  - understanding [B-2](#)
- troubleshooting [A-12, B-1](#)
- uninstalling, recommendation against [3-2, A-12](#)
- Cisco Security Manager
  - and Performance Monitor 3.1
    - recommendation [1-5](#)
  - basic concepts [8-5](#)
  - getting started [8-5](#)
  - interoperability with
    - Performance Monitor 3.1 [1-5](#)
  - late-breaking information about [1-xi](#)
  - logging in [6-13](#)
  - overview [1-2](#)
- Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)
  - date and time synchronization [3-4](#)
  - interoperation with [3-4](#)
  - overview [1-xi](#)
- CiscoView Device Manager
  - unsupported use [3-3](#)
- CiscoWorks

- Common Services, overview [1-2](#)
- Monitoring Center for Security. *See* Security Monitor
- TCP ports
  - Daemon Manager [2-3](#)
  - HTTP [2-2](#)
- VPN/Security Management Solution (VMS)
  - migrating data to Security Manager [1-xiii](#)
- client software
  - logging in to a server [6-13](#)
  - migration of Catalyst 6500/7600 switches [5-10](#)
  - using [6-13](#)
- client systems
  - deleting Temp files [6-2](#)
- Device View
  - representation of Catalyst 6500/7600 switches [5-10](#)
  - representing devices managed by AUS and CNS after upgrade [5-9](#)
- file locations on [1-7, 6-11](#)
- recommendation to delete Temp files [6-2](#)
- video (graphics) card drivers
  - confirming installed versions [2-5](#)
  - upgrading [2-5](#)
- CMFLOCK.TXT file, deleting [4-7](#)
- CNS-managed devices
  - association with Configuration Engines
    - after migration [5-8](#)
  - migrating
    - Configuration Engines for [5-8](#)
- Common Services
  - documentation [2-1](#)
  - installing [2-1](#)
  - licensing [1-6](#)
  - required version [1-2](#)
  - requirement to use [2-1](#)
  - upgrading [5-1](#)
- Configuration Engines
  - assigning to devices
    - after migration [5-8](#)

- importing from DCR
  - after migration [5-8](#)
- migrating
  - for devices managed by [5-8](#)
- CSTM TCP port [2-3](#)

---

## D

- database TCP port [2-3](#)
- date and time settings
  - caution against changing [3-4](#)
  - recommendation to synchronize [2-1, 3-4](#)
  - use of NTP servers [2-1](#)
- device bootstrapping [8-5](#)
- device certificates
  - before adding to Security Manager
    - checking validity [5-7](#)
    - validating encryption keys [5-7](#)
    - verifying end-host identity [5-7](#)
    - verifying signature [5-7](#)
- device credentials
  - exporting from DCR as a .csv file
    - before adding certificates to Security Manager [5-7](#)
    - before running getCerts.pl [5-7](#)
- device credentials repository (DCR)
  - exporting certificates from
    - using getCerts.pl [5-7](#)
  - inventory file exported from
    - for adding AUS and Configuration Engines [5-8](#)
  - server process [3-4](#)
  - TCP port [2-3](#)
  - troubleshooting [3-4](#)
- Device View
  - migrated Catalyst 6500/7600 switches
    - retrieving inventory details [5-10](#)
  - red X icon
    - representing Cisco 7600 Series routers [5-10](#)

- representing devices managed by AUS and CNS [5-8](#)
- digital certificates
  - adding to Security Manager
    - using getCerts.pl [5-6](#)
    - using loadCerts.pl [5-6](#)
  - adding to Security Manager in bulk in one step [5-6](#)
  - confirming validity
    - before using getCerts.pl [5-6](#)
  - refreshing cache
    - and using loadCerts.pl [5-8](#)
  - requirement to create [8-1](#)
  - retrieving
    - after upgrade from 3.0.2 [5-6](#)
    - from devices in bulk [5-6](#)
    - using perl scripts [5-6](#)
  - retrieving for unreachable devices [5-8](#)
  - troubleshooting [3-4](#)
- directory encryption, restriction against [2-5, 3-4](#)
- documentation
  - audience for this [1-xii](#)
  - on Cisco.com [1-xv](#)
  - ordering [1-xv](#)
  - reviewing updated [1-xiii](#)
  - typographical conventions in [1-xii](#)
- documentation, obtaining
  - Auto Update Server [1-xiv](#)
  - Cisco Security Agent [B-1](#)
  - Cisco Security Manager [1-xiii](#)
  - Common Services [1-xiv](#)
  - Resource Manager Essentials (RME) [1-xiv](#)
- documentation feedback, sending to Cisco [1-xi, 1-xv](#)
- domain controllers (primary or backup), unsupported use [2-5](#)
- downgrading
  - related applications [5-12](#)
  - requirements to be met [5-12](#)
  - restoring backed up data [5-12](#)
  - to earlier supported versions

- from 3.2 [5-12](#)

---

## E

- encrypted directories, restriction against [2-5, 3-4](#)
- evaluation license
  - upgrading to permanent license [1-6](#)
- Event Services software TCP port requirements
  - HTTP [2-3](#)
  - listening [2-3](#)
  - routing [2-3](#)
  - services [2-3](#)

---

## F

- FAQs, in the troubleshooting guide [1-xiii](#)
- files, where stored
  - Cisco Security Agent
    - logs [B-2](#)
    - policies [1-5, 3-2](#)
    - on client systems [1-7](#)
    - on servers [1-7](#)
- file system recommendations [2-4](#)
- Firefox
  - cache size requirement [6-3](#)
  - confirming the installed Java version [2-7](#)
  - versions supported [2-4, 2-6](#)

---

## G

- gatekeeper HIPO TCP port [2-2](#)
- getCerts.pl
  - access permissions for running [5-7](#)
  - adding certificates to Security Manager [5-6](#)
  - confirming validity of certificates
    - before using -a argument [5-6](#)
  - device credentials, exporting to .csv file [5-6](#)
  - syntax, description [5-7](#)

using in conjunction with loadCerts.pl [5-6](#)  
 getting started with Cisco Security Manager [8-5](#)

---

## H

HTTP TCP port [2-2](#)

---

## I

inline upgrade

*See also* in place upgrade

in place upgrade

definition [5-1](#)

error during [5-2](#)

from an earlier version with pending data [5-2](#)

procedure [5-2](#)

running the installer [5-2](#)

installation

migrating Catalyst 6500/7600 switches [5-9](#)

planning and preparation [1-xi](#)

servers

dependencies [2-1](#)

general requirements [2-1](#)

post-installation tasks [8-1](#)

preparatory tasks [3-1](#)

starting an installation [4-2](#)

troubleshooting [4-2](#)

verifying [8-4](#)

installing RME

installation notes [7-1](#)

procedures

custom installations [7-4](#)

typical installations [7-2](#)

installing server software [4-1](#)

Internet Explorer

cache size requirement [6-2](#)

confirming the installed Java version [2-7](#)

security settings [6-2](#)

versions supported [2-4, 2-6](#)

*See also* browsers

Internet Information Server (IIS)

conflict with Security Manager [3-3, 3-4](#)

requirement to uninstall [3-3, 3-4](#)

Internet Inter-ORB Protocol (IIOP) TCP port [2-2](#)

IOS IPS devices

migrating from Security Manager 3.0.x

IP addresses

multiple network interface cards and [2-4](#)

static address requirement [2-4](#)

using dynamic addresses [2-4](#)

using multiple interface cards [2-4](#)

IPS Event Viewer client

communicating with server [1-4](#)

IPS Event Viewer server

communicating with client

modifying firewall software policy [1-4](#)

installing on a server with CSA [1-4](#)

IPS Manager

downgrading [5-12](#)

IPS Manager

importing IPS MC 2.2 data [C-4](#)

migrating from IPS MC [C-4](#)

prerequisites to import IPS MC data [C-4](#)

time required to import IPS MC data [C-5](#)

*See also* IPS MC

IPS MC

backing up server data [C-4](#)

exporting data [C-4](#)

migrating to IPS Manager [C-4](#)

securing the backed-up data [C-4](#)

*See also* IPS Manager

IPS sensors

migrating from Security Manager 3.0.x [5-10](#)

---

## J

Java

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

---

## L

language versions supported (Windows)  
 server [2-4, 2-6](#)

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

licenses  
 installing [1-7](#)  
 Product Authorization Key (PAK) [1-6](#)  
 Security Manager kit part numbers [1-6](#)  
 settings [1-6](#)  
 Software License Claim Certificate [1-6](#)  
 understanding [1-6](#)  
 upgrading [1-6](#)  
 uploading new [1-6](#)  
 working with [1-6](#)

license server TCP port [2-3](#)

loadCerts.pl  
 access permissions for running [5-7](#)  
 adding certificates to Security Manager  
   using the .csv file with exported details [5-7](#)  
 enabling certificate authentication  
   after running the script [5-7](#)  
 retrieving certificates  
   for unreachable devices [5-8](#)  
 running in verbose mode [5-8](#)  
 running when Security Manager is launched  
   refreshing certificate cache [5-8](#)  
 syntax, description [5-8](#)

---

## M

McAfee Antivirus  
 reenabling [6-10](#)

memory (RAM)  
 client requirements [2-6](#)

server requirements [2-4](#)

migrating  
 Catalyst 6500/7600 switches  
   after upgrade [5-9](#)  
   retrieving device details after upgrade [5-10](#)

IOS IPS devices

IPS sensors

modifying firewall software policy [1-4](#)

---

## N

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

Networking Professionals Connection [1-xv](#)

network management applications  
 backup failure [5-5](#)

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

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

Network Time Protocol (NTP) server, recommendation to use [2-1, 3-4](#)

Norton Internet Security 2005  
 incompatibility [6-10](#)  
 requirement to uninstall [6-10](#)

NTFS file system, requirement to use [2-4](#)

---

## O

ODBC driver manager  
 confirming the installed version [2-4](#)  
 requirements [2-4](#)  
 working with Sybase files [2-4](#)

OGS TCP port [2-3](#)

online help, tips for viewing [6-2](#)

operating systems  
 on client systems  
   Windows 2003 [2-6](#)  
   Windows Vista [2-6](#)  
   Windows XP Professional [2-6](#)

on servers  
 Windows 2003 Server [2-4](#)

Osagent UDP port [2-3](#)

overview [1-1](#)

## P

passwords

security basics [C-3](#)

strong passwords

characteristics [C-2](#)

definition [3-2](#)

how to require [3-2](#)

recommendations [C-2](#)

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

pending data

and upgrading [5-2, 5-4](#)

submitting

in non-Workflow mode [5-2, 5-4](#)

in Workflow mode [5-2, 5-4](#)

taking over a user's session

before upgrading [5-2, 5-4](#)

Performance Monitor

overview [1-5](#)

version 3.1, interoperability with

Security Manager 3.2 [1-5](#)

version 3.1, recommendation [1-5](#)

perl scripts

exporting certificates into a .csv file [5-6](#)

loading certificates into Security Manager in bulk [5-6](#)

retrieving certificates

after upgrading from 3.0.2 [5-6](#)

*See also* getCerts.pl

*See also* loadCerts.pl

permanent license, upgrading from evaluation license [1-6](#)

point patches

applying to a client [6-11](#)

caution against accepting from a third-party [5-12](#)

default location on client systems [6-12](#)

deleting Temp files on client systems [6-2](#)

obtaining [5-12](#)

version mismatch [6-11](#)

popup blockers

configuring [6-1, 6-2](#)

conflicting with other installed software [3-2](#)

disabling [6-1, 6-2](#)

requirements [6-1](#)

troubleshooting [6-1, 6-2](#)

ports

required for TCP [2-2](#)

required for UDP [2-2](#)

product registration. *See* licenses

PSIRT [1-xv](#)

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

## R

red X icon

in Device View

representing devices managed by AUS and CNS [5-8](#)

representing migrated Catalyst 6500 Series switches [5-10](#)

reinstalling

after database corruption

using restorebackup.pl [4-8](#)

Common Services [4-8](#)

server software [4-8](#)

warning message [4-8](#)

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

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

removable media drives, security implications if compromised [8-4](#)

requirements

client system [2-5](#)

servers

installation, general [2-1](#)

system [2-3](#)

Resource Manager Essentials (RME)

documentation [1-xiv](#)

- entitlement to install [1-5](#)
- installing [1-5](#)
- installing on a Security Manager server
  - with VirusScan enabled [4-5](#)
  - with VirusScan turned off [4-5](#)
- licensing [1-6](#)
- overview [1-5](#)
- restorebackup.pl
  - reinstalling
    - server software [4-8](#)
- restoring
  - after upgrade [5-5](#)
  - database after downgrade [5-12](#)
  - Security Manager database [5-5](#)
  - using perl script [4-8](#)

---

## S

- SAFE blueprint [1-xii](#)
- Secure Shell (SSH) TCP port [2-2](#)
- security
  - advisories [1-xv](#)
  - incidents, obtaining assistance [1-xv](#)
  - news from Cisco
    - registering to receive [1-xv](#)
    - RSS feed URL [1-xv](#)
  - notices [1-xv](#)
  - PSIRT [1-xv](#)
  - vulnerabilities, reporting [1-xv](#)
- Security Manager database
  - pending data
    - and upgrading [5-2, 5-4](#)
- Security Manager database TCP port [2-3](#)
- Security Monitor [C-4](#)
- sensors
  - See also* IPS Sensors
- server
  - configuration
    - boot settings [3-3](#)
    - date and time settings [3-4](#)
  - downgrading from 3.2 [5-12](#)
  - file locations
    - database files [1-7](#)
    - log files [1-7](#)
    - miscellaneous files [1-7](#)
  - installations
    - best practices [3-1](#)
    - dependencies [2-1](#)
    - procedures [4-1, 5-1](#)
  - performance
    - best practices for enhancing [3-1](#)
    - operating environment [2-3, 4-1](#)
  - preparation checklists [3-1](#)
  - processes, verifying status [8-4](#)
  - traffic
    - required inbound ports [2-2](#)
    - required outbound ports [2-2](#)
  - upgrading [5-4](#)
- service agreement contracts [1-6](#)
- service packs
  - applying to a client [6-11](#)
  - caution against accepting from a third-party [5-12](#)
  - default location on client systems [6-12](#)
  - deleting Temp files on client systems [6-2](#)
  - obtaining [5-12](#)
  - recommendation to delete Temp files on client systems [6-2](#)
  - version mismatch [6-11](#)
- service requests
  - submitting [1-xv](#)
- services
  - minimum required for Windows [3-3](#)
  - required for TCP [2-2](#)
  - required for UDP [2-2](#)
- SNMP polling UDP port [2-2](#)
- SNMP trap UDP port [2-2](#)
- software updates. *See* point patches
- SSL certificate invalidation [3-4](#)

SSL mode (for HTTP server) TCP port [2-2](#)

support

Networking Professionals Connection [1-xv](#)

obtaining from Cisco [1-xv](#)

service agreement contracts [1-6](#)

Software Application Support contracts [1-6](#)

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

Sybase database files, requirement to use correct ODBC version [2-4](#)

Syslog UDP port [2-2](#)

## T

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

TCP

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

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

technical support (TAC)

obtaining [1-xv](#)

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

Telnet TCP port [2-2](#)

Terminal Services

requirements [2-5, 3-4](#)

unsupported configuration [2-5](#)

Tomcat

Ajp13 connector TCP port [2-3](#)

global library files, where stored [1-7](#)

shutdown TCP port [2-3](#)

training, obtaining [1-xv](#)

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

troubleshooting

antivirus scanners [3-2](#)

Cisco Security Agent

blocking a valid operation [A-13](#)

blocking network access [A-12](#)

diagnostic utility [A-13](#)

icon appearance changed in system tray [A-13](#)

obtaining a revised agent from TAC [A-12](#)

recognizing when the agent is disabled [A-13](#)

security level is High [A-12](#)

setting the security level to Medium [A-12](#)

untrusted rootkit detected [A-12](#)

using the log file [A-12](#)

collecting server troubleshooting information [A-14](#)

DCRServer process does not start [3-4](#)

error messages

client installation [A-7](#)

server installation [A-2](#)

server uninstallation [A-5](#)

file contents cannot be unpacked [4-2](#)

file corruption

executable file [4-2](#)

host-based intrusion software [3-2](#)

incorrect GUI [2-5, 8-5, A-3](#)

installation

does not run [A-11](#)

hangs [A-3, A-9](#)

reviewing log files [A-15](#)

interoperation with CS-MARS [3-4](#)

invalid SSL certificate [3-4](#)

java.security.cert errors [3-4](#)

mapped drives [A-4](#)

missing

GUI [A-3](#)

product features [A-3](#)

popup blockers [3-2, 6-1, 6-2](#)

security software conflicts [3-2](#)

server processes

changing [A-14](#)

restarting [A-15](#)

viewing [A-14](#)

server self-test [A-13](#)

time-dependent features [7-2](#)

uninstallation

does not run [A-11](#)

hangs [A-6](#)

using MDCSupport.exe [A-14](#)

troubleshooting guide, obtaining [1-xiii](#)

typographical conventions in this document [1-xii](#)

---

## U

### UDP

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

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

### uninstallation

cautions against

uninstalling from infected servers [4-6](#)

recommendation to restart client systems [6-13](#)

recommendation to restart servers [4-7](#)

servers

deleting CMFLOCK.TXT [4-7](#)

failure to delete CSCOpX/bin folder [4-6](#)

server software [4-6](#)

updates. *See* point patches

### upgrading

earlier versions supported for [5-1, 5-3](#)

migrating Catalyst 6500/7600 switches [5-9](#)

pending data

committing [5-2, 5-4](#)

discarding [5-2, 5-4](#)

taking over a user's session [5-2, 5-4](#)

using

backup and restore [5-5](#)

in place [5-2](#)

### upgrading from

an earlier release [4-6, 5-1](#)

VMS [4-6, 5-1](#)

### upgrading migrating to RME 4.0.5

backing up and restoring RME data to RME 4.0.5 [7-9](#)

upgrading from RME 4.0.x to RME 4.0.5

local upgrade [7-8](#)

remote upgrade [7-8](#)

### user accounts

admin [C-1](#)

casuser [C-1](#)

System Identity [C-1](#)

understanding [C-1](#)

user permissions, understanding [C-2](#)

---

## V

verifying an installation [8-4](#)

### VirusScan

disabled on a Security Manager server

stopping Performance Monitor installation [4-5](#)

stopping RME installation [4-5](#)

failed installation of

RME and Performance Monitor [4-5](#)

installed on a Security Manager server

with Performance Monitor [4-5](#)

with RME [4-5](#)

On-Access Scan feature

running [4-5](#)

turned off [4-5](#)

workaround for

installing Performance Monitor [4-5](#)

installing RME [4-5](#)

---

## W

web context files, where stored [1-7](#)

Windows services, required [3-3](#)