



## INDEX

---

### A

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

---

### B

- backing up
  - across mapped drives [5-4](#)
  - before upgrade [5-3](#)
  - database for downgrade [5-6](#)

- interference with network management applications [5-4](#)

- Security Manager database [5-3](#)

- backup and restore

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

- upgrade using, procedure [5-3](#)

- bootstrapping devices [8-5](#)

- browsers

- requirements

- cache [6-1](#)

- client [2-7](#)

- server [2-4](#)

- See also* Firefox

- See also* Internet Explorer

---

### C

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

- cautions

- regarding

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

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

- CD-ONE

- unsupported use [3-3](#)

- certificates. *See* digital certificates

- 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 Marketplace [i-xv](#)

- Cisco Press [i-xv](#)
- Cisco Product Quick Reference Guide, obtaining [i-xv](#)
- Cisco product security
  - PSIRT [i-xv](#)
  - SAFE blueprint [i-xii](#)
  - vulnerability policy portal [i-xv](#)
- Cisco Security Agent
  - customized, standalone version
    - overwritten during installation [5-4](#)
  - fully configurable version
    - not overwritten during installation [5-4](#)
  - installing with Security Manager server [5-4](#)
  - not uninstalled with server uninstallation [5-4](#)
- 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-11, B-1](#)
  - uninstalling, recommendation against [3-2, A-12](#)
- Cisco Security Manager
  - basic concepts [8-5](#)
  - getting started [8-5](#)
  - interoperability with
    - Performance Monitor 3.1 [1-5](#)
  - late-breaking information about [i-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 [i-xi](#)
- CiscoView Device Manager
  - unsupported use [3-3](#)
- CiscoWorks
  - Common Services, overview [1-2](#)
  - TCP ports
    - Daemon Manager [2-2](#)
    - HTTP [2-2](#)
  - VPN/Security Management Solution (VMS)
    - migrating data to Security Manager [i-xiii](#)
- client software
  - logging in to a server [6-13](#)
  - using [6-13](#)
- client systems
  - deleting Temp files [6-2](#)
- Device View
  - representing devices managed by AUS and CNS
    - after upgrade [5-5](#)
  - file locations on [1-7, 6-11](#)
  - recommendation to delete Temp files [6-2](#)
  - video (graphics) card drivers
    - confirming installed versions [2-6](#)
    - upgrading [2-6](#)
- CMFLOCK.TXT file, deleting [4-7](#)
- CNS-managed devices
  - association with Configuration Engines
    - after migration [5-5](#)
  - migrating
    - Configuration Engines for [5-5](#)

## 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 [5-5](#)
- importing from DCR
  - after migration [5-5](#)
- migrating
  - for devices managed by [5-5](#)

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 credentials repository (DCR)

- inventory file exported from
  - for adding AUS and Configuration Engines [5-5](#)
- server process [3-4](#)
- TCP port [2-3](#)
- troubleshooting [3-4](#)

## Device View

- red X icon
  - representing devices managed by AUS and CNS [5-5](#)

## digital certificates

- requirement to create [8-1](#)
- troubleshooting [3-4](#)

directory encryption, restriction against [2-5, 3-4](#)

## documentation

audience for this [i-xii](#)

on Cisco.com [i-xv](#)

ordering [i-xv](#)

reviewing updated [i-xiii](#)

typographical conventions in [i-xii](#)

## documentation, obtaining

Auto Update Server [i-xiv](#)

Cisco Security Agent [B-1](#)

Cisco Security Manager [i-xiii](#)

Common Services [i-xiv](#)

Resource Manager Essentials (RME) [i-xiv](#)

documentation feedback, sending to Cisco [i-xi, i-xv](#)

domain controllers (primary or backup), unsupported use [2-5](#)

## downgrading

related applications [5-6](#)

requirements to be met [5-6](#)

restoring backed up data [5-6](#)

to earlier supported versions

from 3.2 [5-6](#)

**E**

encrypted directories, restriction against [2-5, 3-4](#)

## evaluation license

upgrading to permanent license [1-5](#)

## Event Services software TCP port requirements

HTTP [2-3](#)

listening [2-3](#)

routing [2-3](#)

services [2-3](#)

**F**

FAQs, in the troubleshooting guide [i-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, 2-7](#)

---

## G

gatekeeper HIPO TCP port [2-2](#)

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 [5-1](#)

running the installer [5-2](#)

installation

planning and preparation [i-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, 2-7](#)

*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](#)

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 [5-6](#)

---

## 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

- file locations for
  - Performance Monitor [1-5](#)
- installing [1-6](#)
- Product Authorization Key (PAK) [1-6](#)
- Security Manager kit part numbers [1-5](#)
- settings [1-5](#)
- Software License Claim Certificate [1-6](#)
- understanding [1-5](#)
- upgrading [1-5](#)
- uploading new [1-5](#)
- working with [1-5](#)

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

---

## M

McAfee Antivirus

- reenabling [6-10](#)

memory (RAM)

- client requirements [2-6](#)
- server requirements [2-4](#)

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

---

## N

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

Networking Professionals Connection [i-xv](#)

network management applications

- backup failure [5-4](#)

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 [i-xv](#)

pending data

- and upgrading [5-2, 5-3](#)
- submitting
  - in non-Workflow mode [5-2, 5-3](#)
  - in Workflow mode [5-2, 5-3](#)
- taking over a user's session
  - before upgrading [5-2, 5-3](#)

Performance Monitor

- license file location [1-5](#)
- overview [1-5](#)
- version 3.1, interoperability with

Security Manager 3.2 [1-5](#)

permanent license, upgrading from evaluation license [1-5](#)

point patches

- applying to a client [6-11](#)
- caution against accepting from a third-party [5-6](#)
- default location on client systems [6-12](#)
- deleting Temp files on client systems [6-2](#)
- obtaining [5-6](#)
- 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 [2-1](#)
- required for UDP [2-1](#)

product registration. *See* licenses

PSIRT [i-xv](#)

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

---

## R

red X icon

- in Device View
  - representing devices managed by AUS and CNS [5-5](#)

reinstalling

- after database corruption
  - using restorebackup.pl [4-7](#)
- Common Services [4-7](#)
- server software [4-7](#)
- warning message [4-7](#)

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

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

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

requirements

client system [2-6](#)

servers

- installation, general [2-1](#)
- system [2-3](#)

Resource Manager Essentials (RME)

- documentation [i-xiv](#)
- entitlement to install [1-4](#)
- installing on a Security Manager server
  - with VirusScan enabled [4-5](#)
  - with VirusScan turned off [4-5](#)
- licensing [1-6](#)
- overview [1-4](#)

restorebackup.pl

reinstalling

- server software [4-7](#)

restoring

- after upgrade [5-4](#)
- database after downgrade [5-6](#)
- Security Manager database [5-4](#)
- using perl script [4-7](#)

---

## S

SAFE blueprint [i-xii](#)

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

security

- advisories [i-xv](#)
- incidents, obtaining assistance [i-xv](#)
- news from Cisco
  - registering to receive [i-xv](#)
  - RSS feed URL [i-xv](#)
- notices [i-xv](#)
- PSIRT [i-xv](#)
- vulnerabilities, reporting [i-xv](#)

Security Manager database

- pending data
  - and upgrading [5-2, 5-3](#)

Security Manager database TCP port [2-2](#)

server

- configuration
  - boot settings [3-3](#)
  - date and time settings [3-4](#)
- downgrading from 3.2 [5-6](#)
- 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 [5-3](#)
- service agreement contracts [1-5](#)
- service packs
  - applying to a client [6-11](#)
  - caution against accepting from a third-party [5-6](#)
  - default location on client systems [6-12](#)
  - deleting Temp files on client systems [6-2](#)
  - obtaining [5-6](#)
  - recommendation to delete Temp files on client systems [6-2](#)
  - version mismatch [6-11](#)
- service requests
  - submitting [i-xv](#)
- services
  - minimum required for Windows [3-3](#)
  - required for TCP [2-1](#)
  - required for UDP [2-1](#)
- 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 [i-xv](#)
  - obtaining from Cisco [i-xv](#)
  - service agreement contracts [1-5](#)
  - Software Application Support contracts [1-5](#)
- 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 [2-1](#)
  - list of required services [2-2](#)
- technical support (TAC)
  - obtaining [i-xv](#)
  - URL for service requests [i-xv](#)
- Telnet TCP port [2-2](#)
- Terminal Services
  - requirements [2-5, 3-4](#)
  - unsupported configuration [2-5](#)
- Tomcat
  - Ajp13 connector TCP port [2-2](#)
  - global library files, where stored [1-7](#)
  - shutdown TCP port [2-2](#)
- training, obtaining [i-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-11](#)
    - diagnostic utility [A-13](#)
    - icon appearance changed in system tray [A-12](#)

- obtaining a revised agent from TAC [A-12](#)
- recognizing when the agent is disabled [A-12](#)
- 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-13](#)
- 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 [2-6, 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-14](#)
  - 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-13](#)
- troubleshooting guide, obtaining [i-xiii](#)
- typographical conventions in this document [i-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 [4-7](#)

- server software [4-6](#)

updates. *See* point patches

### upgrading

- earlier versions supported for [5-2](#)

#### pending data

- committing [5-2, 5-3](#)
- discarding [5-2, 5-3](#)
- taking over a user's session [5-2, 5-3](#)

#### using

- backup and restore [5-3](#)
- in place [5-1](#)

### 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 [7-8](#)
- upgrading from RME 4.0.x to RME 4.0.5
  - local upgrade [7-7](#)
  - 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 [4-6](#)  
installing RME [4-6](#)

---

## W

web context files, where stored [1-7](#)  
Windows services, required [3-3](#)

