Installing Cisco Security Agent for Cisco Intelligent Contact Management Software, Release 6.0(0)

October 2004

This document provides installation instructions and information about Cisco Security Agent for Cisco Intelligent Contact Management (ICM) Software, Release 6.0(0). **You are strongly urged to read this short document in its entirety.**

Cisco Security Agent for ICM 6.0(0) incorporates the appropriate policies for Cisco ICM Enterprise Edition 6.0(0), Cisco IP Customer Contact (IPCC) Enterprise Edition 6.0(0), Cisco Outbound Option (formerly Blended Agent) 6.0(0), Cisco E-Mail Manager 5.0(0), Cisco Web Collaboration Option 5.0(0) [Cisco Collaboration Server 5.0(0), Cisco Dynamic Content Adapter (DCA) 2.0(1), Cisco Media Blender 5.0(0)], Cisco CTI Object Server (CTI OS) 6.0(0), Cisco Agent Desktop (CAD) Enterprise Edition 6.0(0), Cisco Support Tools 1.0(1), and Cisco Remote Monitoring Suite (RMS) 2.0(0).

Contents

This document contains information about the following topics:

CISCO SYSTEMS

Introduction

The standalone Cisco Security Agent (CSA)

- provides intrusion **detection** and **prevention** for Cisco ICM software
- removes potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications
- can defend against previously unknown attacks because it does not require signatures (as antivirus software does)
- reduces downtime, widespread attack propagation and clean-up costs

The Agent is provided free of charge by Cisco Systems for use with Cisco ICM software. The Agent provides Windows platform security (host intrusion detection and prevention) based on a tested set of security rules (policy). The Agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed. A policy controls access to system resources based on:

- what resource is being accessed
- what operation is being invoked
- which application is invoking the action

This process occurs transparently and does not hinder overall system performance.

Cisco Security Agent should not be viewed as providing complete security for servers hosting Cisco ICM software. Rather, it should be viewed as an additional line of defense, which—when used correctly with other standard defenses, such as virus scanning software and firewalls—provides enhanced security for host servers.

The standalone Cisco Security Agent for Cisco ICM uses a static policy that cannot be changed. However, see the section Migrating to the Management Center for Cisco Security Agents, page 15, for additional information.

Follow the installation instructions in this document to install the standalone Cisco Security Agent on all Cisco ICM software servers, including Cisco ICM Router, Logger, Peripheral Gateway (PG), Admin Workstation (AW), Historical Data Server (HDS), Standalone Distributed Diagnostic and Services Network (SDDSN), Outbound Option (formerly Blended Agent) Dialer, Cisco E-Mail Manager, Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender, Cisco CTI OS, Cisco Agent Desktop (CAD) Enterprise, Cisco Support Tools, Cisco Remote Monitoring Suite (RMS).

Specifically, Cisco Security Agent for ICM 6.0(0) incorporates the appropriate policies for:

- Cisco ICM Enterprise Edition 6.0(0)
  Supported: Router, Logger, PGs, AWs, HDS, CTI Server, Support Tools server and agent
  Not Supported: CTI Desktop and Client components; Internet Service Node (ISN)

- Cisco IP Customer Contact (IPCC) Enterprise Edition 6.0(0)
  Supported: ICM servers (see ICM Enterprise Edition 6.0(0) list above)
  Not Supported: Cisco CallManager; Cisco IP IVR; Cisco Customer Response Solutions (CRS);
  Cisco Internet Service Node (ISN)

- Cisco Outbound Option (formerly Blended Agent) 6.0(0)
  Supported: Dialer
  Not Supported: n/a

- Cisco Remote Monitoring Suite (RMS) 2.0(0)
  Supported: Listener, LGArchiver, LGMapper, SDDSN
  Not Supported: AlarmTracker Client Software

- Cisco Web Collaboration Option 5.0(0) [only on Windows platform]

  - Cisco Collaboration Server 5.0(0)
    Supported: Collaboration Server, SQL Server 7.0, SQL 2000 Server
    Not Supported: Oracle

  - Cisco Media Blender 5.0(0)
    Supported: Media Blender Server
    Not Supported: n/a

  - Cisco Dynamic Content Adapter (DCA) 2.0(1)
    Supported: DCA Server
    Not Supported: Agent Desktop, Caller Desktop

- Cisco E-Mail Manager 5.0(0)
  Supported: eManager Server (on Windows platform), SQL Server 7.0
  Not Supported: Oracle

- Cisco CTI Object Server (CTI OS) 6.0(0)
  Supported: CTI OS Server
  Not Supported: CTI Desktop and Client components

- Cisco Agent Desktop (CAD) Enterprise Edition 6.0(0)
  Supported: CAD Server
  Not Supported: Agent Desktop

For servers running Cisco CallManager, see *Installing Cisco Security Agent for Cisco CallManager.*

For servers running Cisco IP IVR, see *Installing Cisco Security Agent for Cisco Customer Response Applications*.

For servers running Cisco ISN, see *Installing Cisco Security Agent for Cisco Internet Service Node*.

Note In addition to being specifically tuned for Cisco ICM software, Cisco Security Agent for Cisco ICM software provides support for a select number of Cisco-approved third-party applications. These are the third-party applications included in the ICM Software 6.0(0) *Bill of Materials*. **No other third-party applications are officially supported.** These third-party applications must be installed into the default directories presented during the installation process, otherwise your applications will not work properly. See the discussion in the section Default Installation Directories, page 4.

The Agent policy is focused on hardening the Windows 2000 operating system, SQL Server, and IIS. Further, if you install the Network Shim, security checks for TCP/IP are provided.

Manual Windows updates are allowed by the current Cisco Security Agent for ICM policy. Should the Windows update mechanism change, you may need to download a more recent version of the standalone Agent software, or contact the Cisco Technical Assistance Center (TAC).

In any event, when a newer version of the Agent becomes available, Cisco strongly recommends that you install the newer version.

If you use a third-party software application that is not Cisco-approved, see the section Migrating to the Management Center for Cisco Security Agents, page 15, for additional information.

Default Installation Directories

Caution To use Cisco Security Agent, you **must always** use the **default directories** when installing **any software** on a server. You need not choose the default disk drive if an option is available (for example, C: or D:), but you **must** use default directories.

Cisco Security Agent leverages rules which incorporate path information. Application actions may be blocked if the application is not installed in the correct directory. For this reason, it is mandatory that applications are installed to the default directories provided by the application installers. Drive letters are not restricted.

If you are not sure whether default directories were used during your installation of ICM and supported third-party software, a number of the more important default directories are given below (for those cases where you can select optional installation directories on ICM servers).

In the notation below, two wildcards (that is, **) indicate a recursive directory path—including all directories, passing down as many levels as exist in a path. All regular expressions given below are case insensitive. Thus, mssql is the same as MSSQL.

Microsoft SQL Server

SQL server should be installed under a directory with at least one of the following strings in the path:
   \MSSQL
   \MSSQL7
   \Microsoft SQL Server"

pcAnywhere

pcAnywhere must be installed under:
   \Program Files\pcAnywhere

AntiVirus Software

Network Associates' VirusScan Enterprise 7.0 must be installed under:
   \Network Associates

Trend Micro must be installed under:
   \Trend\SProtect

ICM Multimedia and ServletExec Components

Component	Should Be Installed under Directory
Cisco Collaboration Server	**\Cisco_CS
Cisco Collaboration Server ServletExec	**\ServletExec ISAPI
Cisco Dynamic Content Adapter	**\dca
Cisco Media Blender	**\CiscoMB
Cisco Media Blender ServletExec	**\ServletExec ISAPI
Cisco E-Mail Manager ServletExec	**\ServletExec ISAPI
Admin Workstation ServletExec	**\ServletExec ISAPI

Customer Applications

Customer applications should generally work without problems. However, should you have problems with a particular customer application, as a convenience, a directory has been created where agent and customer programs can run. If customer programs are installed into this directory, these programs **may** run without generating events. The directory is:

> **\Program Files\ICM_CSA_CustomerApps**\

New Restrictions on Share Directories

Certain applications, namely, Outbound Option and Listener, depend on a remote process (that is, an application running on a different computer) being able to write to a share directory on servers hosting Listener or Outbound Option. In previous releases of these products, there were no restrictions on the location of the share. However, this approach represents a security risk. To reduce this risk, servers running Cisco Security Agent now limit the acceptable names of the share directories for use by these applications. Viruses written to these named directories will not be able to execute and propagate. The restrictions apply only to the names of the directories, not the name of the share which is visible to remote computers.

Given below are the directories that can be used with the Cisco Security Agent for ICM when shares are required.

Outbound Option Changes

When attempting to import customer data files from a computer that is running Cisco Security Agent, make sure that the path to the file begins with

> <drive>\customer\import

This path rule does not apply if the import file is located on the same computer as the import process. Also, make sure that the import process user has network and directory read/write access to the "customer" directory as well as the "import" directory.

This behavior is discussed in the "Import Rule" section in the *Cisco ICM/IP Contact Center Enterprise Edition Outbound Option User Guide*. If you are having problems with the import process, see the "Symptoms and Troubleshooting Actions" section of the same document.

Listener Changes

The DDSN Transfer Process (DTP) on ICM writes to a share directory on the Listener server. With Cisco Security Agent installed on the Listener server, the DTP process (which runs on a remote server) is now only allowed to write to a share directory on the Listener server with the following structure:

<drive>:\customer\<customer name>\import\<file name>

<drive> can be any fixed drive, such as the C or D drive.

<file name> includes any file written to the import directory.

An example of an acceptable directory name is:

C:\customer\cust01\import

Logger Backup Changes

In earlier releases, customers were allowed to backup their ICM database to anywhere on their drive.

Starting with 6.0(0), if the Logger is running Cisco Security Agent, then the SQL Server backup process is constrained to write the backup files to a directory with path restrictions. This approach improves security on these servers. The backup process should only write to a directory path which matches the following:

\MSSQL\BACKUP

Custom-Template Creation Change

In earlier releases, customers using InfoMaker were allowed to directly edit a .pbl file on the Admin Workstation, in order to add or edit a template.

Starting with 6.0(0), if Cisco Security Agent is installed, customers must copy the .pbl from the Admin Workstation to the remote machine on which InfoMaker is running, edit it with InfoMaker, and then copy the .pbl file back to the Admin Workstation.

System Requirements

- Cisco ICM 6.0(0)
- Microsoft Windows 2000 Server (or Advanced Server) in English

Before You Begin the Installation

Before you install the Cisco Security Agent for Cisco ICM software, review the following information:

- Confirm that the computer you are using to install Cisco Security Agent has 20 MB of hard disk space available for the download file and the installed files.
- Cisco ICM software must be installed before you install Cisco Security Agent.

- Before each Cisco ICM upgrade, you must disable the Cisco Security Agent service. You must also be sure that the service does not get enabled at any time during the Cisco ICM installation. For information on how to disable the service, see the section Disabling and Reenabling the Cisco Security Agent Service, page 10.

Caution You must disable the Cisco Security Agent service before performing **any** software installation. This means before every operating system, Cisco ICM and third-party installation and upgrade, including maintenance release, service release, and support patch installations and upgrades.

Ensure that the service does not get enabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade, since the Cisco Security Agent may block part of the installation if not disabled.

After installing or upgrading the software, you must reenable the Cisco Security Agent Service. With the service disabled, the Agent no long provides intrusion detection for the server.

- If Terminal Services software is installed on your system, do not use it to install or upgrade the Cisco Security Agent. If you want to, you can use pcAnywhere or Virtual Network Computing (VNC) to remotely install or upgrade the Agent.
- The Agent installation and rebooting causes a brief spike in CPU usage and may cause processing interruptions on the server. Rebooting should be done immediately after installation, because although the Cisco Security Agent protects the server as soon as you install the software, it does not provide complete functionality until the server is rebooted.

Caution To minimize effects on resources, Cisco recommends that you install/reboot at the end of the business day or during a time when processing is minimal, preferably during a regularly scheduled maintenance window.

- After the installation, you do not need to perform any Agent configuration tasks. The software immediately begins to work as designed. Security events may display in the Message tab of the Agent GUI, as well as in Microsoft Event Viewer and/or in the securitylog.txt file (which is found in <InstallDrive>:\Program Files\Cisco\CSAgent\log).

Tip If you encounter problems with installing or uninstalling the Cisco Security Agent, see the sections Messages, Logs, and Caching, page 12 and Troubleshooting, page 13.

Installing the Cisco Security Agent

Caution Before you upgrade or reinstall the Agent, you must uninstall the Agent. You cannot install one version of the Agent on top of a previously installed version. See the sections Uninstalling the Cisco Security Agent, page 11, and Upgrading the Cisco Security Agent, page 12.

Note An important feature of the Management Center for Cisco Security Agents is that it has a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need to manually stop, uninstall, install, and start CSA on each server. See the section Migrating to the Management Center for Cisco Security Agents, page 15.

Note To install the Cisco Security Agent you must be a System Administrator.

Review the section Before You Begin the Installation, page 6, which provides information to help ensure a successful installation. To install the Cisco Security Agent for ICM software, complete the following steps:

Step 1 From the server on which you are going to perform the installation, go to
http://www.cisco.com/kobayashi/sw-center/sw-custcontact.shtml
and continue with Step 2.

OR

Use the "CSA for ICM" CD and continue with Step 7.

Step 2 Click on Cisco Security Agent.

Step 3 From there you are brought to a page where you should click on the following link:
Apply for 3DES Cisco Cryptographic Software under export licensing controls

Note You must be allowed access to a cryptographic site before you can download the Cisco Security Agent file. If you have not yet applied for such access, you will at this point be directed to a web form. Check the appropriate boxes on that form and click **Submit**. A message appears telling you when you can expect to have download access. If you have already registered, continue with Step 4.

Step 4 On the page that displays, click the link for Cisco Security Agent for ICM.

Step 5 Download the latest version of the Cisco Security Agent file: **CiscoICM-CSA-<*version*>-K9.exe** (for example, CiscoICM-CSA-4.0.1.540-1.0.0-K9.exe, where 4.0.1.540 indicates the engine version and 1.0.0 indicates the policy version).

Note Only one version is available at any given time, and that is the latest version.

Step 6 Note the location where you saved the downloaded file.

Step 7 Double-click **CiscoICM-CSA-<*version*>-K9.exe** to begin the installation.

Step 8 When the Welcome window displays, click **Next**.

Step 9 To accept the license agreement, click **Yes**.

Step 10 Accept the default destination as the location where the software will install; click **Next**.

Step 11 Make sure that the Network Shim box is checked (this is the default), then click **Next** to install the Network Shim.

Caution You must install the Network Shim for the Agent to have full functionality.

Step 12 The "Preparing to transfer files" status window displays the options that you chose. To accept the current settings, click **Next**.

Step 13 Continue to wait while the installation completes; do not click Cancel.

Step 14 Click the radio button **Yes** (the default), then click **Finish** to reboot the server.

⚠
Caution The Agent protects the server as soon as you install the software, but the Agent does not provide complete functionality until you reboot the server. Therefore, Cisco recommends that you reboot immediately after installation. As mentioned above, to minimize affects on resources (such as processing interruptions), Cisco recommends that you install/reboot at the end of the business day or during a time when processing is minimal, preferably during a regularly scheduled maintenance window.

🔎
Tip When the installation completes, a red flag (the Cisco Security Agent icon) displays in the Windows 2000 system tray. Double-click on the red flag. If you do not see the error message "Failed to connect to CsaManager", then the Agent was successfully installed. If you see Security:Enabled in the lower right corner of the window, the Agent is enabled as well.

Step 15 Perform this procedure on each Cisco ICM software server (see the list given in the Introduction).

Checking the Version on the Server

You can check the engine and policy versions of the Agent you installed.

To Check the Engine Version in Use for CSA for Cisco ICM Software

Right-click on the CSA flag in the system tray and select About.

To Check the Policy Version in Use for CSA for Cisco ICM Software

Step 1 Start Regedit.

⚠
Caution Do not make any changes. You should be viewing for verification purposes only.

Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the "Restoring" topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact the Cisco Technical Assistance Center (TAC).

Step 2 Expand the key HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\ICM-CSA Policy\Version.

Step 3 Close Regedit.

Testing the Agent

You may want to test the Agent by attacking your own system. If so, go to the "Attack your system" section in the "Evaluating the Cisco Security Agent" appendix in *Installing Management Center for Cisco Security Agents 4.0*, which can be accessed from http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Disabling and Reenabling the Cisco Security Agent Service

You must disable the CSA service whenever you want to install, upgrade, or uninstall software. This means before every operating system, Cisco ICM and third-party installation and upgrade, including maintenance release, service release, and support patch installations and upgrades.

Ensure that the service does not get enabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade.

After installing or upgrading the software, you must reenable the Cisco Security Agent Service. With the service disabled, the Agent no long provides intrusion detection for the server.

Note You must have Admin rights in order to successfully disable or reenable the Cisco Security Agent.

Caution If you are installing, upgrading, or uninstalling, you **must** **disable** the Agent service. Neither the *net stop CSAgent* command, nor the Suspend Security menu option, disables the Agent service. To disable the Agent service you **must** use the procedure described below. (If you do not disable the Agent service, security is enforced as soon as the system is rebooted; if the installation tries to perform actions after the rebooting, these actions may be blocked.)

Disable

To disable the CSA service, complete the following steps:

Step 1 From the Windows **Start** menu, select **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 In the Services window, right-click **Cisco Security Agent** and choose **Properties**.

Step 3 In the Properties window, click the **General** tab.

Step 4 Click **Stop**.

Step 5 From the **Startup Type** drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Caution In the Services window, verify that the Startup Type of the CSA service is Disabled.

Step 7 Close Services.

Caution You must reenable the Cisco Security Agent service after installing, upgrading, or uninstalling software.

Reenable

To reenable the CSA service, complete the following steps:

Step 1   Choose **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2   In the Services window, right-click **Cisco Security Agent** and choose **Properties**.

Step 3   In the Properties window, click the **General** tab.

Step 4   From the **Startup Type** drop-down list box, choose **Automatic**.

Step 5   Click **Apply**.

Step 6   Click **Start**.

Step 7   After the service has started, click **OK**.

Step 8   Close Services.

Uninstalling the Cisco Security Agent

⚠️ **Caution**   You cannot install one version of the Agent on top of a previously installed version. You must uninstall the Agent and then reinstall the software. When you start the uninstaller, a prompt from the Agent asks whether you want to uninstall the Agent. You have limited time (five minutes) to click Yes to disable the protection. If you choose No or wait to disable the protection, the security mode automatically enables.

✏️ **Note**   An important feature of the Management Center for Cisco Security Agents is that it has a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need to manually stop, uninstall, install, and start CSA on each server. See the section Migrating to the Management Center for Cisco Security Agents, page 15.

To uninstall the security Agent, complete the following steps:

Step 1   Choose **Start > Programs > Cisco Systems > Uninstall Cisco Security Agent**.

Step 2   Click **Yes** in response to all questions you are asked EXCEPT, if you are presented with the options **Yes** and **Yes to All** at any point, click **Yes to All**.

⚠️ **Caution**   After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

✏️ **Note**   The uninstaller does not remove the registry entries where the policy version is stored. If you want them removed, you must manually delete them—after you uninstall. The relevant registries are:
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\ICM-CSA Policy\Version
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\CSA Agent\Product

HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\CSA Agent\Version
Delete everything under, and including, ICM-CSA Policy, and everything under, and including, CSA Agent.

Upgrading the Cisco Security Agent

To upgrade the Cisco Security Agent, perform the following tasks:

1. Uninstall the existing version that is installed on the server.

   See the section Uninstalling the Cisco Security Agent, page 11.

2. Install the new version that you plan to run on the server.

   See the section Installing the Cisco Security Agent, page 7.

Messages, Logs, and Caching

This section discusses additional features of the Cisco Security Agent.

Event Messages and Log Files

- If the Cisco Security Agent has a message for you, the icon (the red flag in the Windows system tray) will wave. To read the message, double-click on the icon, then click on the Messages tab.

  The messages that are displayed are those generated when an action either is denied or generated a query. Only the two most recent messages are displayed.

- The log files are located in <InstallDrive>:\Program Files\Cisco\CSAgent\log.

  – securitylog.txt—this is the main event log; this is where rule violations and other relevant events are logged

  – csalog.txt—this provides Agent startup and shutdown history

  – driver_install.log—this provide a record of the driver installation process

  – Cisco Security AgentInstallInfo.txt—this provides a detailed record of the installation process

- You can view securitylog.txt using Notepad. The field names are given in the first line.
  You can also:

  – Copy the file to a machine that has Excel and change the name to securitylog.csv.

  – Double-click securitylog.csv and it will open as an Excel spreadsheet.

    You may find it most convenient to see the contents of a spreadsheet cell by clicking on the cell and looking at the contents in the field above the spreadsheet matrix.

  For diagnosing problems, the most important fields are DateTime, Severity, Text, and User. Ignore the RawEvent field; it contains essentially the same information that is presented in the other fields, but in an unprocessed, and difficult to read, form.

  The ordering of the severity levels, from least to most severe, is: Information, Notice, Warning, Error, Alert, Critical, Emergency.

Understanding How the Cache Works

Cisco Security Agent caches your responses to queries for one hour. This is a convenience feature, so that you do not have to respond to a popup each time you do a repetitive action. However, in certain situations, this feature may have undesirable results. For example, see the section Second Attempt to Install Software Fails without a Warning, page 13.

Troubleshooting

Please consider the following troubleshooting suggestions before contacting the Cisco Technical Assistance Center (TAC).

Problems with Installing/Uninstalling the Agent

If you encounter problems with installing or uninstalling the Agent, perform the following tasks:

- Verify that you rebooted the server.
- Verify that the Cisco Security Agent service is not disabled and that its Startup Type value is Automatic.
- Obtain the installation logs from <InstallDrive>:\Program Files\Cisco\CSAgent\log. Review the Cisco Security AgentInstallInfo.txt and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log file should state that csanet2k.inf installed. If the Network Shim is not installed, uninstall the Agent and then install the Agent again.
- Verify that you did not use Terminal Services.

Second Attempt to Install Software Fails without a Warning

In the following case, a second attempt to install software will fail without a warning:

1. You try to install software without first stopping and disabling the Cisco Security Agent service. Cisco Security Agent displays the following message:
   Cisco Security Agent: A problem was detected, press one of the action buttons below. Are you installing/uninstalling software? If not, this operation is suspicious.

2. You click No. (This is the action that causes the problem when running the install the next time—see below.)

3. You stop and disable the Cisco Security Agent service.

4. You try to re-run the software installation, but nothing happens.

When you clicked **No** in step 2 above, your answer was cached in memory. The cache is cleared automatically after an hour.

To clear the cache immediately so you can install the software now, perform the following procedure:

Step 1   Reenable the service (as described in the section Reenable, page 11).

Step 2   In the Windows task bar, double-click the Cisco Security Agent icon (the red flag in the Windows system tray).

Step 3   Click the Advanced tab.

Step 4   Click Clear.

Step 5   Close the Cisco Security Agent Control Panel.

✎
Note   Before you retry installing the software on the server, disable the Cisco Security Agent service. After you install the software, reenable the Cisco Security Agent service. See Disabling and Reenabling the Cisco Security Agent Service, page 10.

Problems with Cisco ICM Software or Errors from Cisco Security Agent

Go through the procedure in this section if you encounter problems after installing Cisco Security Agent for Cisco ICM software:

- Are these problems with Cisco ICM software that cannot otherwise be explained?

- Look in the Cisco Security Agent log file
  <InstallDrive>:\Program Files\Cisco\CSAgent\log\securitylog.txt
  for events indicating that an application action was blocked by Cisco Security Agent.

- Are Cisco Security Agent error messages displayed in the Messages tab of the Control Panel?

If you cannot determine the cause of a Cisco Security Agent log entry or error message, contact Cisco TAC. However, before doing so, please refer to the section What to Do before Contacting TAC about a CSA Problem, page 14.

To troubleshoot problems with Cisco ICM software or errors from Cisco Security Agent:

Step 1   In the Windows taskbar, right-click the Cisco Security Agent icon (the red flag in the Windows system tray), and click Suspend Security.

Step 2   Perform the operation that caused the error message.

Step 3   In the Windows taskbar, right-click the Cisco Security Agent icon, and click Resume Security.

Step 4   Perform the operation that caused the error message.

Step 5   If the operation completes successfully with the Cisco Security Agent suspended and continues to fail with the Cisco Security Agent enabled, confirm that the software with which you were having the problem is among the ICM software components or third-party applications included in the ICM Software 6.0(0) *Bill of Materials*.

Step 6   If you are unable to resolve the problem, see What to Do before Contacting TAC about a CSA Problem, page 14.

What to Do before Contacting TAC about a CSA Problem

First go through all the relevant procedures described above to determine if there is really a problem and if it is in fact a CSA problem.

If you feel that it is a CSA problem, and you want to open a TAC case, follow the procedures below:

Step 1   In <InstallDrive>:\Program Files\Cisco\CSAgent\bin, double-click on csainfo.bat. This will collect useful hardware and software data.

Step 2 csainfo will ask if you want to stop the Agent. Click **Yes**. The file csainfo.log is created.

Step 3 Zip up the <InstallDrive>:\Program Files\Cisco\CSAgent\ directory (which includes csainfo.log and securitylog.txt).

Step 4 Determine the version of your CSA engine and of your CSA policy (the method for doing so is described in Checking the Version on the Server, page 9).

Step 5 Contact TAC. Be prepared to provide them with the zipped file you create in Step 3 and the information you collected in Step 4.

Migrating to the Management Center for Cisco Security Agents

An important feature of the Management Center for Cisco Security Agents (CSA MC) is that it has a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need to manually stop, uninstall, install, and start CSA on each server.

Also, while the security Agent included with Cisco ICM software uses a static policy that should not be changed, it is possible to add, change, or delete the policy if you purchase and install Management Center for Cisco Security Agents (CSA MC). However, any such changed policy is **NOT** qualified for use with ICM.

✎
Note If you have used the Management Center for Cisco Security Agents to change the policy associated with the Cisco Security Agent for ICM software, and you encounter problems with running your software, before calling your Cisco ICM support provider, you must first:

1. Remove any third-party software not supported by Cisco from your ICM servers

2. Revert to the original Cisco Security Agent for ICM policy

If the problem persists, then call your support provider.

CSA MC contains two components:

- The Management Center installs on a dedicated server and includes a web server, a configuration database, and a web-based interface. The Management Center allows you to define rules and policies and create Agent kits that are then distributed to managed servers. (Multiple policies for different Cisco products can be managed by a single MC.)

- The Cisco Security Agent (the managed Agent) installs on all Cisco ICM software servers and enforces security policies. The managed Agent registers with the Management Center and can receive configuration and rule updates. It also sends event reports back to its Management Center.

If you are interested in the Management Center, you should obtain the latest version of the following CSA MC documents:

- *Installing Management Center for Cisco Security Agents*
- *Using Management Center for Cisco Security Agents*
- *Release Notes for Management Center for Cisco Security Agents*

You can download these documents at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/csa_4_0/

Ensure that the Management Center component is installed on a separate, dedicated server and the managed Agent is installed on all Cisco ICM servers. Make sure that the server that is intended for the Management Center meets the system requirements that are listed in *Installing Management Center for Cisco Security Agents*.

⚠

Caution If you attempt to install the Management Center on servers where you have installed Cisco ICM software, the Management Center will block operation of ICM components.

Once you have obtained the CSA MC package and documentation, and followed the instructions in *Installing Management Center for Cisco Security Agents* for Installing CSA MC, perform the following procedure to import the ICM policy and install a managed Agent:

Step 1 Download the latest version of the Cisco ICM policy XML file (though an XML file, the extension is .export; for example, CiscoICM-CSA-4.0.1.543-1.0.4.export). You can obtain the policy at

http://www.cisco.com/kobayashi/sw-center/sw-custcontact.shtml

✎

Note Upon accessing this site, see the discussion in the section Installing the Cisco Security Agent, page 7.

Note the location where you saved the downloaded file.

Step 2 Follow the instructions in *Using Management Center for Cisco Security Agents* for importing the policy that you downloaded in Step 1.

Step 3 Use the Quick Start Configuration section of *Installing Management Center for Cisco Security Agents* to perform the following tasks:

- Generate the Rules
- Build an Agent kit using the group created when you imported the policy

Step 4 Uninstall the standalone Cisco Security Agent, if it exists, by following the instructions in the section Uninstalling the Cisco Security Agent, page 11.

Step 5 Distribute and install the new managed Agent that was created in Step 3 by following the instructions in the Cisco Security Agent Installation and Overview section of *Installing Management Center for Cisco Security Agents*.

Obtaining Additional Information about CSA

For additional information about the Cisco Security Agent, do the following:

Step 1 In the Windows 2000 system tray, right-click the flag and choose **Open Control Panel**.

Step 2 In the upper, right corner of the window click the **?** icon.

The Cisco Security Agent documentation displays.

🔍

Tip To obtain the Cisco Security Agent 4.0 documentation, go to:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Obtaining Related Cisco ICM Software Documentation

The latest version of the Cisco ICM software documentation can be found at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html