Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)

July 2005

This document provides installation instructions and information about Cisco Security Agent for Cisco Intelligent Contact Management (ICM) Software, Release 7.0(0). **You are strongly urged to read this document in its entirety.**

Cisco Security Agent for ICM 7.0(0) incorporates the appropriate policies for Cisco ICM Enterprise & Hosted Editions 7.0(0), Cisco IP Customer Contact (IPCC) Enterprise & Hosted Editions 7.0(0), Cisco Outbound Option 7.0(0), Cisco E-Mail Manager 7.0(0), Cisco Web Collaboration Option 7.0(0) [Cisco Collaboration Server 7.0(0), Cisco Dynamic Content Adapter (DCA) 2.0(1), Cisco Media Blender 7.0(0)], Cisco CTI Object Server (CTI OS) 7.0(0), Cisco Agent Desktop (CAD) 7.0(0), Cisco Support Tools 2.0(0), and Cisco Remote Monitoring Suite (RMS) 2.1(0).

Contents

This document contains information about the following topics:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco Security Agent (CSA) provides:

- Intrusion **detection** and **prevention** for Cisco ICM software
- Defense against previously unknown attacks because it does not require signatures (as antivirus software does)
- Reduced downtime, widespread attack propagation and clean-up costs

The standalone 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) that is 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:

- The resources being accessed
- The operation being invoked
- The process invoking the action

This occurs transparently and does not hinder overall system performance.

Caution You should not view Cisco Security Agent for Cisco ICM as providing complete security for Cisco ICM servers. Rather, view Cisco Security Agent as an additional line of defense that, when used correctly with other standard defenses such as virus-scanning software and firewalls, provides enhanced security. Cisco Security Agent for Cisco ICM provides enhanced defense for many different Cisco ICM installations and configurations, and thus cannot enforce network access control rules (which block outbound or inbound network traffic) or act as a host-based firewall.

Other security considerations include keeping the OS updated.
The best starting point for references to security and voice products is http://www.cisco.com/go/ipcsecurity. A specific document to examine is *IP Telephony Security Operations Guide to Best Practices* at http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e47.html
Also refer to the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* at http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html.

The policy for the CSA standalone Agent for ICM is created from the default policy modules that are shipped with Cisco Security Agent 4.5. These default policy modules secure/harden Windows, SQL and IIS. These default policy modules are altered in two ways for CSA for ICM:

- Some rules, which allow processes (such as FTP, NNTP) that are not required for the ICM product family, are altered to not allow these processes.
- Policy changes are made in order to allow the ICM product family, including qualified third-party applications, to run smoothly.

Be aware that, in the interests of security, CSA default policy modules may block what you might consider default Windows activity. These rules have been retained for CSA for ICM when they do not block ICM activity. As examples (and these are just to be taken as examples):

- Usually, if you search for files using Windows File Search Tool, the Find tool accesses Microsoft sa.windows.com and sends the search information to the Microsoft server. CSA blocks this functionality.
- Similarly, you may not be able to access a web proxy server running on port 80 or 443.

Also in the interests of security, **remote file access is generally denied**. For the three exceptions, see Restrictions on Share Directories, page 6.

A further security measure to be noted is that CSA will **query you if you try to change the domain membership of a machine**. This is by design: preventing unknown processes from writing to the core registry hive without user confirmation. The query will look something like this:
The process 'E:\WINDOWS\system32\lsass.exe' is attempting to modify user account settings. Do you wish to allow this?

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 16, 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 Dialer, Network Gateway; Cisco E-Mail Manager, Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender, Cisco CTI OS, Cisco Agent Desktop (CAD), Cisco Support Tools, Cisco Remote Monitoring Suite (RMS).

Specifically, Cisco Security Agent for ICM 7.0(0) incorporates the appropriate policies for (see the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* for supported versions of third-party software):

- Cisco ICM Enterprise Edition 7.0(0)
  Supported: Router, Logger, PGs, AWs, HDS, CTI Server, Network Gateway, Support Tools server and agent
  Not Supported: CTI Desktop and Client components; Customer Voice Portal (CVP)
- Cisco IP Customer Contact (IPCC) Enterprise Edition 7.0(0)
  Supported: ICM servers (see ICM Enterprise Edition 7.0(0) list above)
  Not Supported: Cisco CallManager; Cisco IP IVR; Cisco Customer Response Solutions (CRS); Customer Voice Portal (CVP)
- Cisco Outbound Option 7.0(0)
  Supported: Dialer
  Not Supported: n/a

- Cisco Remote Monitoring Suite (RMS) 2.1(0)
  Supported: Listener, LGArchiver, LGMapper, SDDSN
  Not Supported: AlarmTracker Client Software
- Cisco Web Collaboration Option 7.0(0) [only on Windows platform]
  - Cisco Collaboration Server 7.0(0)
    Supported: Collaboration Server, SQL Server
    Not Supported: Oracle, Agent Desktop, Caller Desktop
  - Cisco Media Blender 7.0(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 7.0(0)
  Supported: eManager Server (on Windows platform), SQL Server
  Not Supported: Oracle, Agent Desktop
- Cisco CTI Object Server (CTI OS) 7.0(0)
  Supported: CTI OS Server
  Not Supported: CTI Desktop and Client components
- Cisco Agent Desktop (CAD) Enterprise Edition 7.0(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 CVP, see *Installing Cisco Security Agent for Cisco Customer Voice Portal*.

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 *Cisco Intelligent Contact Management Software Release 7.0(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 5.

The Agent policy is focused on hardening the Windows operating system, SQL Server, and IIS. Further, enabling the Network Shim provides network protocol stack hardening capabilities, such as protection against TCP SYN flood. (However, disabling the Network Shim does not disable Network Access Control capabilities.)

Automatic Windows updates are allowed by the current Cisco Security Agent for ICM policy. By default Automatic Windows Update downloads and installs the updates from the following folders (** indicates a recursive directory path):
<%systemroot%>\SoftwareDistribution\Download**
<drive>:\Program Files\WindowsUpdate\
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 16, 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. As just stated, 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

Note Refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* for the specific versions of the AV software that is supported.

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

Symantec AntiVirus must be installed under:

\Norton*

\Symantec*

Trend Micro must be installed under:

\Trend*

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\

Restrictions on Share Directories

Certain applications, namely, WebView, 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 WebView, Outbound Option, or Listener. 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 to 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.

WebView: Custom-Template Creation

Effective with ICM 7.0(0), you must **not** install Sybase InfoMaker on an ICM Server. In particular, whereas installing InfoMaker on an Admin Workstation was formerly allowed, this is no longer allowed.

However, the remote machine on which InfoMaker is running can connect to an Admin Workstation to read/write .pbl files. The following restrictions are relevant:

- the remote server can edit **only** .pbl files

- the .pbl files **must** live under the folder **\icm**\aw\custom\

Outbound Option

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 *Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions*. If you are having problems with the import process, see the “Troubleshooting” appendix of the same document.

Listener

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 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

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

System Requirements

- Cisco ICM 7.0(0)
- Microsoft Windows Server 2003, Standard Edition (or Enterprise Edition) in English
  Microsoft Windows 2000 Server (or Advanced Server) in English
- Disk Space 20 MB
- Typical CPU Load (under normal circumstances): less than 5%

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 11.

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.

Note Setup for ICM and IPCC will offer to disable and reenable CSA for you; in these cases, the actions described above do not have to be performed manually. (Note: If CSA has been disabled, and then a drastic system failure occurs, you may need to reenable CSA manually.)

- If Terminal Services software is installed on your system, do not use it to install or upgrade the Cisco Security Agent (unless logged into session :0 with console access). If you want to, you can use pcAnywhere or Virtual Network Computing (VNC) to remotely install or upgrade the Agent.
- 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. In particular, the following limitations exist if the system is **not** rebooted:
  - Network Shield rules are not applied
  - Network access control rules only apply to new socket connects (though stopping and restarting network server service will provide full network access control security, even without a system reboot)
  - Data access control rules are not applied (though stopping and restarting the web server service will apply data access control security, even without a system reboot)

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 Messages window of the Agent GUI (double-click the Cisco Security Agent icon—the red flag in the Windows system tray; then click on Message, on the left, under Status), as well as in Microsoft Event Viewer and/or in the securitylog.txt file (see Event Messages and Log Files, page 13).

Tip If you encounter problems with installing or uninstalling the Cisco Security Agent, see the sections Messages, Logs, and Caching, page 13 and Troubleshooting, page 14.

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 12, and Upgrading the Cisco Security Agent, page 13.

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 16.

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

Review the section Before You Begin the Installation, page 8, 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 6.

Step 2 On the page that displays, click on Cisco Security Agent.

Step 3 On the page that displays, click on CSA for ICM, IPCC Enterprise and Hosted.

Step 4 Download the latest version of the Cisco Security Agent file: **CiscoICM-CSA-<*version*>-K9.exe** (for example, CiscoICM-CSA-4.5.1.616-2.0.0-K9.exe, where 4.5.1.616 indicates the engine version and 2.0.0 indicates the policy version).

Caution Be sure that you click on the .exe file for **ICM 7.0**. Read the description for the file to make sure that you are **not** downloading the wrong file.

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. Fill out the 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 5.

Step 5 Note the location where you saved the downloaded file.

Step 6 Double-click **CiscoICM-CSA-<*version*>-K9.exe** to begin the installation.

Step 7 When the Welcome window displays, click **Next**.

Step 8 To accept the license agreement, click **Yes**.

Step 9 Accept the default destination as the location where the software will install; click **Next**.

Step 10 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 11 The "Preparing to transfer files" status window displays the options that you chose. To accept the current settings, click **Next**.

Step 12 Continue to wait while the installation completes; do not click Cancel.

Step 13 Click the radio button **Yes** (the default), then click **Finish** to reboot the server.

Caution As mentioned earlier, 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 system tray. Double-click on the red flag. If you see Security:Medium in the lower right corner of the Cisco Security Agent window, this implies that security is enabled.

Step 14 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 do so, double-click on the CSA flag in the system tray. Included in the Status section of the Cisco Security Agent window is the Product ID, which will look something like: Cisco ICM CSA 4.5.1.616 Policy 2.0.0

In this case, 4.5.1.616 is the engine version and 2.0.0 is the policy version.

If for some reason the CSA flag is not available, the engine and policy versions can be obtained as follows:

- Open the text file <*InstallDrive*>:\Program Files\Cisco Systems\CSAgent\cfg\agent.bundle

- The value of the key STD.PRODUCT_ID contains the engine and policy version.

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.

Disable

To disable the CSA service, complete the following steps:

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

Note The above instructions, and those that follow, assume Windows Server 2003. The Windows 2000 Server instructions occasionally differ slightly, for example, for Windows 2000 Server, step 1 above would be:

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

However, the differences between the two should not be such as to cause confusion.

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 At this point you are challenged by CSA. Click the Yes radio button; click **Apply**; enter the displayed letters in the Challenge field; click **OK**.

At this point, CSA is stopped. This is indicated by a white target with a red bull's-eye being displayed on top of the red flag that is the CSA icon.

Step 6 From the **Startup Type** drop-down list box, choose **Disabled**.

Step 7 Click **OK**.

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

Step 8 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 From the Windows **Start** menu, select **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 16.

To uninstall the security Agent, complete the following steps:

Step 1 From the Windows **Start** menu, select **All Programs > Cisco Security Agent > Uninstall Cisco Security Agent**.

Step 2 Click **Yes** in response to all questions you are asked. (And remember the five-minute time limit referred to in the Caution above).

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 system tray, the Messages window in the graphical user interface (GUI) displays errors, but the software does not provide protection.

Note The following is relevant if you are uninstalling CSA 4.0.x for ICM 5.0(0) or CSA for ICM 6.0(0) in order to upgrade to CSA for ICM 7.0(0). However, **no such registry keys exist for CSA for ICM 7.0(0)**.

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 12.
2. Install the new version that you plan to run on the server.

   See the section Installing the Cisco Security Agent, page 9.

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 Messages (on the left, under Status).

  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 Systems\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 (it contains events as well; but securitylog.txt also contains the events, and is easier to read)
  - driver_install.log—this provide a record of the driver installation process
  - CSAgent-Install.log—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. This can be done by:
  - Double-clicking the Cisco Security Agent icon—the red flag in the Windows system tray.
  - Then click on Messages (on the left, under Status).

– Then click **View log**. (Clicking on **Purge log** deletes all events stored in securitylog.txt, though csalog.txt will continue to contain that information.)

You can also:

– Copy securitylog.txt 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. This is a convenience feature, so that you do not have to respond to a popup each time you do a repetitive action.

When users are queried, the Agent can remember the response permanently or temporarily. This way, if the same rule is triggered again, the action is allowed, denied, or terminated based on what answer was given previously with no popup query box appearing again either permanently or for some period of time.

For example, if a user is queried as to whether an application can talk on the network and the user responds by selecting the **Yes** radio button and clicking a **Don't ask me again** checkbox, the Yes response is remembered permanently and that response appears in the edit field in the User Query Response window (double-click on the flag icon, then click on User Query Response, on the left, under Status). But if the user is queried as to whether setup.exe can install software on the system and the user responds by selecting the **Yes** radio button, but there is no **Don't ask me again** checkbox or it is there but the user does not select it, this response is remembered temporarily and it does not appear in the User Query Response window.

If the user response is only cached temporarily (for approximately an hour), the user can click the **Clear** button in User Query Response window to delete all temporarily cached responses. To clear permanent responses listed in the edit field, the user must select the response in the edit field and press the Delete key.

Note Permanent responses are remembered across reboots. Temporarily cached responses are not remembered across reboots. Also note, a query response is tied to the user who responded. On multi-user machines, multiple users may be asked the same question.

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 Systems\CSAgent\log. Review the CSAgent-Install.log and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log file should state that csanet 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.

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?
- Are Cisco Security Agent error messages displayed (double-click on the flag icon, then click on Messages, on the left, under Status)?
- Look in the Cisco Security Agent log file, securitylog.txt, for events indicating that an application action was blocked by Cisco Security Agent.
- As explained in the section Understanding How the Cache Works, page 14, CSA can cache user responses either temporarily or permanently. There are occasions where knowing about caching is important.
  For example, you run ICM Setup. CSA prompts you to confirm that you want to run Setup. You inadvertently respond No. At this point, CSA will not allow you to run ICM Setup for approximately an hour, unless you clear the cache as described in Understanding How the Cache Works, page 14.
- CSA can mark suspicious processes as untrusted; for example, recently downloaded content that gets executed immediately. Also, CSA maintains states such as Install State, Virus infected, and so forth. If you believe that CSA is behaving abnormally, or suspect that CSA is doing something it never did before and is thereby blocking something it should not be blocking, reset the agent back to its original (that is, when newly installed) state. Resetting the agent will clear up the temporary and permanent caches, as well as clear agent states and the untrusted applications list. To reset:
  Start > All Programs > Cisco Security Agent > Reset Cisco Security Agent
- Never hide the flag icon while service is running (by selecting Exit). Make sure the flag is visible in the system tray as long as the service is running. If the service is running and the flag is not visible, you can make it visible by doing the following:
  Start > All Programs > Cisco Security Agent > Cisco Security Agent

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 16.

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

Step 1 Disable CSA as described in Disable, page 11.

Step 2 Perform the operation that caused the error message.

Step 3 Reenable CSA as described in Reenable, page 12.

Step 4 Perform the operation that caused the error message.

Step 5 If the operation completes successfully with the Cisco Security Agent turned off 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 *Cisco Intelligent Contact Management Software Release 7.0(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 16.

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 Run the Cisco Security Agent Diagnostics program:
Start > All Programs > Cisco Security Agent > Cisco Security Agent Diagnostics

This causes the agent to gather self-describing diagnostic information on the system and on the agent itself (for example, information pertaining to any configured system states). Be patient, because it may take some time to collect this data.

The diagnostic utility temporarily disables agent security while it executes. If you are queried to disable agent security, you should respond **Yes**, to allow the diagnostics program to run. Security is automatically reenabled when the utility finishes collecting data.

Step 2 When the collection is complete, a message appears informing you that a csa-diagnostics.zip file has been created in the <*InstallDrive*>:\Program Files\Cisco Systems\CSAgent\log directory.

Step 3 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 10).

Step 4 Contact TAC. Be prepared to provide them with the zipped file mentioned in Step 2 and the information you collected in Step 3.

Migrating to the Management Center for Cisco Security Agents

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.

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. 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.

Management Center for Cisco Security Agent 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 Management Center for Cisco Security Agent documents:

- *Installing Management Center for Cisco Security Agents 4.5*
- *Using Management Center for Cisco Security Agents 4.5*
- *Release Notes for Management Center for Cisco Security Agents 4.5*

You can download these documents at:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html

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 4.5*.

Caution Do not install the Management Center on servers where you have installed Cisco ICM software. If you attempt to do so, either the installation will fail, or the Management Center will block operation of ICM components.

Once you have obtained the Management Center for Cisco Security Agent package and documentation, and followed the instructions in *Installing Management Center for Cisco Security Agents 4.5* for Installing Management Center for Cisco Security Agent, perform the following procedure to import the ICM policy and install a managed Agent:

Step 1 Uninstall the Cisco Security Agent, if it exists, by following the instructions in the section Uninstalling the Cisco Security Agent, page 12.

Step 2 Download the latest version of the Cisco ICM policy XML file (though an XML file, the extension is .export; for example, CiscoICM-CSA-4.5.1.616-2.0.0.export). You can obtain the policy at

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

Note On accessing this site, see the discussion in the section Installing the Cisco Security Agent, page 9.

Note the location where you saved the downloaded file. Note also that, for identification purposes, all ICM policies are prepended with the "word" **ICM**.

Tip All policy variables, including Group Name, Policy Name, Rule Module Name, File Sets Name, Application Class Name, Registry Set Name and so on, literally everything that can have a name (only Rules do not have names), starts with "ICM".

So, a File Set with the name "ICM All Files" means All Files on the system.
While a File Set with the name "ICM All ICM Files" means All files related to the ICM product.

This use of the first word in all these variables is just a way to distinguish ICM variables in your Management Center from variables associated with other policies; for example, policies supplied for Cisco Customer Voice Portal (CVP) or Cisco CallManager.

Step 3 Follow the instructions in *Using Management Center for Cisco Security Agents 4.5* ("Exporting and Importing Configurations") for importing the policy that you downloaded in Step 1.

Step 4 Use the "Quick Start Configuration" section of *Installing Management Center for Cisco Security Agents 4.5* to perform the following tasks:

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

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 4.5*.

Obtaining Additional Information about CSA

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

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

Step 2 Click the **Help** button.

The Cisco Security Agent documentation displays.

Tip To obtain the Cisco Security Agent 4.5 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/techsupport

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Cisco will continue to support documentation orders using the Ordering tool:

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

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

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm
- 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 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco 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 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, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- 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