



Installing Cisco Security Agent for Cisco Unified Communications Manager

This document provides installation instructions and information about Cisco Security Agent (CSA) for the following Cisco Unified Communications Manager (formerly Cisco Unified CallManager) releases:

- Release 4.x
- Release 5.x
- Release 6.x
- Release 7.x



Note

Cisco Security Agent automatically installs for Releases 5.x and later.

If Cisco Unified Communications Manager resides on the same server with Cisco Customer Response Solutions (CRS), you can use this document or the *Installing Cisco Security Agent for Cisco Customer Response Solutions* document to install the agent on that coresident server, because both products use identical security policies.

Contents

This document contains information on the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [Before You Begin the Installation, page 3](#)
- [Installing the Cisco Security Agent for Cisco Unified Communications Manager Release 4.x, page 6](#)
- [Checking the Agent and Policy Versions on the Server, page 7](#)
- [Disabling and Reenabling the Cisco Security Agent Service for Release 4.x, page 7](#)
- [Disabling and Reenabling the Cisco Security Agent Service for Release 5.x and Later, page 9](#)
- [Uninstalling the Cisco Security Agent, page 10](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Upgrading the Cisco Security Agent, page 10](#)
- [Migrating to the Management Center for Cisco Security Agents, page 11](#)
- [Testing the Cisco Security Agent, page 12](#)
- [Messages and Logs, page 13](#)
- [Troubleshooting for Release 4.x, page 14](#)
- [Troubleshooting for Release 5.x and Later, page 16](#)
- [Obtaining Additional Information About the Cisco Security Agent, page 17](#)
- [Obtaining Related Cisco Unified Communications Manager Documentation, page 18](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 19](#)

Introduction

Cisco Security Agent provides intrusion detection and prevention for the Cisco Unified Communications Manager cluster. Cisco Systems provides it free of charge as a standalone security agent for use with servers in the Cisco Unified Communications Manager voice cluster. The agent provides platform security that is based on a tested security rules set (policy), which has rigorous levels of host intrusion detection and prevention. The agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed.

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



Note

In addition to being specifically tuned for the Cisco Unified Communications Manager and Cisco CRS software, Cisco Security Agent for Cisco Unified Communications Manager provides support for many Cisco-approved, third-party applications. The agent also provides security for web and database services. In addition, CSA provides security checks for TCP/IP if you install the Network Shim, which serves as a host-based intrusion detection system. When a later version of the agent becomes available, Cisco strongly recommends that you install the later version.

Cisco strongly recommends that you run this agent in conjunction with the latest Cisco-provided operating system service releases and upgrades. To obtain the Cisco-provided operating system service releases and upgrades, see [Table 1](#).

In some cases, you may have to uninstall Cisco Security Agent for Cisco Unified Communications Manager before you can run DMA. Refer to the *Data Migration Assistant User Guide Release 5.1(1)* and later for more information.

The standalone Cisco Security Agent uses a static policy that cannot be changed. However, if you want to change the policy for non-Cisco Unified Communications Manager and non-Cisco Unified Contact Center Express purposes, see the [“Migrating to the Management Center for Cisco Security Agents” section on page 11](#) for more information.

Follow the installation instructions in this document to install CSA on all servers within the voice cluster, including Cisco Unified Communications Manager, Cisco CRS, Remote Database, voice, and speech servers. Do not install the agent on client machines.

The policy that is included with Cisco Security Agent for Cisco Unified Communications Manager provides support for many Cisco-approved, third-party monitoring tools, including the following applications:

- BMC Patrol
- Concord eHealth Monitor
- Diskeeper Server Standard Edition 8.0.478.0
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research Prognosis
- McAfee VirusScan 7.0
- Micromuse Netcool
- NAI Epolicy Agent
- NetIQ Vivinet Manager
- RealVNC
- Symantec Corporate Edition 8.0
- Trend Anti-Virus

**Note**

Cisco Unified Communications Manager Release 5.x and later do not support the preceding applications.

If you use a third-party software tool that is not Cisco-approved, see the [“Migrating to the Management Center for Cisco Security Agents” section on page 11](#) for more information.

System Requirements

The following requirements apply to Cisco Unified Communications Manager Release 4.x:

- Cisco Unified Communications Manager—The *Cisco Unified Communications Manager Software Compatibility Guide* includes supported Cisco Unified Communications Manager releases. To obtain the *Cisco Unified Communications Manager Software Compatibility Guide*, see [Table 1](#).
- Microsoft Windows 2000 Server or Windows Server 2003 in English

The following requirements apply to Cisco Unified Communications Manager Release 5.x and later:

- The administrator must have local administrative privileges for Cisco Unified Communications Operating System Administration.
- Cisco Security Agent automatically installs during initial installation of the Cisco Unified Communications Manager platform.

Before You Begin the Installation

Before you install the Cisco Security Agent for Cisco Unified Communications Manager, review the following information:

- Cisco Security Agent automatically installs with Cisco Unified Communications Manager Release 5.x and later.

- The Cisco Security Agent supports any Cisco Media Convergence Server (MCS) or customer-provided, Cisco-approved server where Cisco Unified Communications Manager and Cisco-provided operating system are installed, unless the *Cisco Unified Communications Manager Software Compatibility Guide* indicates otherwise. To obtain the *Cisco Unified Communications Manager Software Compatibility Guide*, see [Table 1](#).
- Install this security agent on every server in the Cisco Unified Communications Manager cluster, including coresident servers where Cisco Unified Communications Manager and Cisco Customer Response Solutions/Cisco Customer Response Applications run.
- Install the agent first on the publisher database server and verify that the installation completed successfully; then, install the agent on all subscriber servers serially, that is, on one server at a time.
- Do not install the agent between the operating system and Cisco Unified Communications Manager installation.



Note The preceding statement does not apply to Release 5.x and later.

- Before each Cisco Unified Communications Manager upgrade, you must disable the Cisco Security Agent service by using the procedure that is shown in the [“Disabling and Reenabling the Cisco Security Agent Service for Release 4.x”](#) section on page 7 and the [“Disabling and Reenabling the Cisco Security Agent Service for Release 5.x and Later”](#) section on page 9. You must also ensure that the service does not get reenabled at any time during the Cisco Unified Communications Manager installation.



Caution

You must disable the Cisco Security Agent service before installing, uninstalling, or upgrading any software, including the operating system, Cisco Unified Communications Manager, maintenance releases, service releases, support patches, and plug-ins.

You must disable the agent by using the method that is described in the [“Disabling and Reenabling the Cisco Security Agent Service for Release 4.x”](#) section on page 7 and the [“Disabling and Reenabling the Cisco Security Agent Service for Release 5.x and Later”](#) section on page 9. Ensure that the service does not get reenabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade.

After the software installation or upgrade, you must reenble the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

- Before you install or upgrade the agent, back up your Cisco Unified Communications Manager data. For more information on how to perform this task, refer to the appropriate version of the Cisco Unified Communications Manager backup documentation. To obtain the Cisco Unified Communications Manager backup documentation, see [Table 1](#).
- Before you install or upgrade the agent, back up all applications that run in the cluster. Refer to the appropriate backup documentation for more information.
- Do not use Terminal Services to install or upgrade the agent. Cisco installs Terminal Services, so Cisco Technical Assistance Center can perform remote management and configuration tasks. Do not use Integrated Lights Out to install or upgrade the agent.

If you want to do so, you can use Virtual Network Computing (VNC) to install or upgrade the agent. To obtain VNC documentation, see [Table 1](#).



Note Cisco Unified Communications Manager Release 5.x and later do not support VNC.

**Caution**

If you currently run Cisco HIDS Agent (Entercept) on the server, you must uninstall the software from Add/Remove Programs before you install the Cisco Security Agent. If you fail to uninstall the Cisco HIDS Agent before the Cisco Security Agent installation, the installation deletes the TCP stack, and the Cisco Security Agent does not install the firewall component that is necessary for security. This applies to only Cisco Unified Communications Manager Release 4.x.

- The agent installation causes a brief spike in CPU usage. To minimize call-processing interruptions, Cisco recommends that you install the agent during a time when call processing is minimal. 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.

**Caution**

Rebooting the server may cause call-processing interruptions. Cisco recommends that you reboot the server at the end of the business day or during a time when call processing is minimal.

- For Cisco Unified Communications Manager Release 4.x, before you upgrade the agent or reinstall the agent on the server, you must uninstall the agent and then do the upgrade or reinstall.

When you uninstall the agent by using Add/Remove Programs or **Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Security Agent**, a prompt asks whether you want to uninstall the agent. You have limited time to click **Yes** to disable the protection. If you choose **No** or wait to disable the protection, the security mode automatically enables, and the installation aborts.

**Caution**

After you uninstall the software from a Cisco Unified Communications Manager Release 4.x server, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows system tray, and the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

- After the installation, you do not need to perform any agent configuration tasks. The software immediately begins to work as designed. For Cisco Unified Communications Manager Release 4.x, security logs display in the Message tab of the agent GUI, in Microsoft Event Viewer, and in the securitylog.txt file (<InstallDrive>\Program Files\Cisco\CSAgent\log).
- The Cisco Unified Communications Manager Backup and Restore Utility does not back up the log files or text file that the agent generates.

If you need to restore the Cisco Unified Communications Manager data to the server for any reason, you must reinstall the agent after you restore the Cisco Unified Communications Manager data.

**Tip**

If you encounter problems with installing or uninstalling the agent, see the [“Troubleshooting for Release 4.x”](#) section on page 14 and the [“Troubleshooting for Release 5.x and Later”](#) section on page 16.

Installing the Cisco Security Agent for Cisco Unified Communications Manager Release 4.x

Review the “[Before You Begin the Installation](#)” section on page 3, which provides information to help ensure a successful installation.



Note

You must have access to the Cisco Unified Communications Manager cryptographic site before you can download the Cisco Security Agent file. If you have not yet applied for download access, go to <http://www.cisco.com/kobayashi/sw-center/telephony/crypto/voice-apps/>. Click **Apply for Cisco 3DESCryptographic Software under export licensing control**. On the window that displays, choose Communications Manager from the drop-down list of products and click **Submit**. A form displays; check the appropriate check boxes on the form and click **Submit**. A message displays that tells you when you can expect to have download access.

To install the Cisco Security Agent, perform the following procedure:

Procedure

Step 1 From the Cisco Unified Communications Manager server, go to the Communications Manager & Voice Apps Crypto Software Download site at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>

Step 2 Choose the latest version of the Cisco Unified Communications Manager CSA file from the list of files.



Note

The filename structure follows the format *CUCM-CSA-n.n.n.nnn-n.n.n-K9.exe*, where *n.n.n.nnn-n.n.n* specifies the version of the agent and policy. For example, the filename CUCM-CSA-4.0.1.539-1.1.4-K9.exe specifies the agent version 4.0.1.539 and the policy version 1.1.4.

Choose the file with the latest agent version and the latest policy version.

Step 3 Note the location where you saved the downloaded file.

Step 4 To begin the installation, double-click the downloaded file.

Step 5 When the Welcome window displays, click **Next**.

Step 6 To accept the license agreement, click **Yes**.

Step 7 To accept the default location (C:\Program Files\Cisco\CSAgent), click **Next**.



Caution

Because the Cisco Unified Communications Manager policy rules are directory specific, you must use the default directory.

Step 8 The status window displays the options that you chose. To accept the current settings, click **Next**.

Step 9 Continue to wait while the installation completes; do not click Cancel.

Step 10 To reboot the server, click **Yes**.

**Caution**

If you want to do so, you can reboot the server at the end of the business day. Rebooting the server may cause call-processing interruptions. 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.

Step 11 Click **Finish**.

**Tip**

When the installation completes, a red flag displays in the Windows system tray. You can also verify that the software installed by locating the Cisco Security Agent in the Add/Remove Programs window.

Step 12 Perform this procedure on every server in the cluster.

Checking the Agent and Policy Versions on the Server

For Cisco Unified Communications Manager Release 4.x

To verify and display the agent and policy versions on the server, double-click the CSA red flag icon and go to Status.

For Cisco Unified Communications Manager Release 5.x and Later

To view the CSA agent and policy version, enter the following CLI command:

show packages active csa

In addition to the preceding CLI command, you can perform the following steps to view CSA information:

1. View and collect CSA logs (csalog and securitylog.txt) by using the Trace & Log Central tool of Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT).
2. Use the Collect Files option and choose Cisco Security Agent in System Logs.
3. Use Remote Browse option to view the logs.
4. Choose Collect CSA log files by using the Trace & Log Central tool.
5. To view the CSA log files by using Remote Browse option, double-click the **csalog** file that displays in the window.

Disabling and Reenabling the Cisco Security Agent Service for Release 4.x

You must disable the CSA service whenever you want to perform a task that requires the server to be restarted, such as installing, upgrading, or uninstalling software. If you disable the CSA service, you must reenabling it before it starts monitoring the Cisco Unified Communications Manager server again.

**Caution**

You can suspend the CSA by using the “net stop csagent” command in a command shell or the suspend option available by right clicking the CSA icon (red flag in the system tray). However, these methods do not actually disable the agent; they merely suspend it. Cisco does not recommend suspending the agent and does not support suspending the agent because, in the event the installer reboots your machine and continues with installation activity, the reactivated CSA service might interfere with the installation of other software.

**Caution**

You must disable the CSA service by using this method before installing, uninstalling, or upgrading any software, including the operating system, Cisco Unified Communications Manager, maintenance releases, service releases, support patches, and plug-ins. Ensure that the service does not get reenabled at any time during the installation/upgrade. Failure to do so may cause problems with the installation or upgrade.

After installing, upgrading, or uninstalling the software, you must reenable the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

**Caution**

Cisco recommends that you perform the following procedure serially, that is, on one server at a time. After you complete installing, upgrading, or uninstalling the software, you can reenable the service on the server; then, you can disable the service on the next server where you plan to perform the same software operation.

Disabling the CSA

To disable the CSA service for Cisco Unified Communications Manager Release 4.x, perform the following procedure:

Procedure

- 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** In the Service Status area, 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 the Services window.
- Step 8** Perform this procedure on every server where you plan to install or upgrade Cisco Unified Communications Manager.

**Caution**

You must reenble the Cisco Security Agent service after installing, upgrading, or uninstalling software. See the [“Reenabling the CSA” section on page 9](#)

Reenabling the CSA

To reenble the Cisco Security Agent service for Cisco Unified Communications Manager Release 4.x after installing, upgrading, or uninstalling software, perform the following procedure:

Procedure

-
- 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 the Services window.
-

Disabling and Reenabling the Cisco Security Agent Service for Release 5.x and Later

You must disable the CSA service whenever you want to perform a task that requires the server to be restarted, such as installing, upgrading, or uninstalling software. If you disable the CSA service, you must reenble it before it starts monitoring the Cisco Unified Communications Manager server again.

**Note**

During a Cisco Unified Communications Manager upgrade, CSA automatically gets stopped before the upgrade and started after the upgrade. If for some reason CSA does not automatically stop and start, you can manually disable and enable CSA.

To manually stop CSA, use the Command Line Interface (CLI) that is available with Cisco Unified Communications Operating System Administration.

To stop CSA, enter the following CLI command:

utils csa disable

To start CSA, enter the following CLI command:

utils csa enable

To check the status of CSA, enter the following CLI command:

`utils csa status`



Note

Stop/start disables/reinstates all rules on an Agent system.

Uninstalling the Cisco Security Agent

This following section does not apply to Cisco Unified Communications Manager Release 5.x and later. For information about upgrading software with Release 5.x and later, see the *Cisco Unified Communications Operating System Administration Guide*.

Review the [“Before You Begin the Installation” section on page 3](#), which provides information about uninstalling the Cisco Security Agent.



Caution

You cannot install the same version of the agent on top of a previously installed version. You must uninstall the agent and then reinstall the software. When you uninstall the agent, a prompt asks whether you want to uninstall the agent. You have limited time to click **Yes** to disable the protection. If you choose **No** or wait to disable the protection, the security mode automatically enables.

To uninstall the security agent from Cisco Unified Communications Manager Release 4.x, perform the following procedure:

Procedure

- Step 1** Choose **Start > Programs > Cisco Systems > Uninstall Cisco Security Agent**.
- Step 2** Click **Yes** or **Yes to All** in response to all questions.
- Step 3** Reboot the server.



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 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.

Upgrading the Cisco Security Agent

For Cisco Unified Communications Manager Release 4.x

Before you upgrade the Cisco Security Agent on a Cisco Unified Communications Manager Release 4.x server, perform the following tasks:

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

See the “Uninstalling the Cisco Security Agent” section on page 10.

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

See the “Installing the Cisco Security Agent for Cisco Unified Communications Manager Release 4.x” section on page 6.

For Cisco Unified Communications Manager Release 5.1(3) and later

Cisco provides CSA upgrades in Cisco Unified Communications Manager releases. To ensure that you are running the latest CSA software, Cisco strongly recommends that you install the latest Cisco Unified CallManager service release on all servers in the cluster. You can obtain the latest downloads at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>

Migrating to the Management Center for Cisco Security Agents

This section does not apply to Cisco Unified Communications Manager Release 5.x and later.

The security agent that is included with Cisco Unified Communications Manager uses a static policy that cannot be changed or viewed. You can add, change, delete, or view policies if you purchase and install the fully managed console product, Management Center for Cisco Security Agent (CSA MC). Be aware, however, that any such changed policy does NOT qualify for use with Cisco CRS.

CSA MC contains two components:

- The Management Center installs on a secured 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 agents that are installed on other network systems and servers.
- The Cisco Security Agent (the managed agent) installs on all Cisco Unified Communications Manager servers in the cluster and enforces security policies. The managed agent registers with the Management Center and can receive policy and rule updates. It also sends event log reports back to its Management Center.

Before you begin, 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/en/US/customer/products/sw/cscowork/ps5212/>

In a Cisco Unified Communications Manager environment, ensure that the Management Center component is installed on a separate, secured server and the managed agent component is installed on all Cisco Unified Communications Manager servers in the cluster. 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

Do not install the Management Center on servers where you have installed Cisco Unified Communications Manager. If you attempt to do so and the CSA MC installation detects that a version of Microsoft SQL Server runs on the server, the managed console installation automatically aborts.

After you have obtained the CSA MC package and documentation, perform the following procedure:

Procedure

-
- Step 1** On a separate (non-Cisco Unified Communications Manager) server, download the latest version of the Cisco Unified Communications Manager .export file from the Communications Manager & Voice Apps Crypto Software Download site at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.
- Step 2** Note the location where you saved the downloaded file.
- Step 3** Uninstall the Cisco Security Agent, if it exists, by following the instructions in the “[Uninstalling the Cisco Security Agent](#)” section.
- Step 4** Follow the instructions in *Installing Management Center for Cisco Security Agents* for installing the CSA MC.
- Step 5** Follow the instructions in *Using Management Center for Cisco Security Agents* for importing the policy file that you downloaded in [Step 1](#).
- Step 6** Follow the instructions in *Installing Management Center for Cisco Security Agents* for completing the configuration of the CSA MC.
-

Note About Running the memRegRepair Utility

This section describes how to run the memRegRepair utility (CiscoCM-CSA-memRegRepair-k9.exe) for MCS-7845-XX. Run the memRegRepair utility if you are running managed agent or standalone agent 3.0(6) or earlier. A general rule is that you should run the utility after every CSA installation in which the agent kit is generated by the Management Center for CSA.

Note the following:

- On a new installation of the Cisco 7845 Series server that is running MCS-OS 2003, run the memRegRepair utility after Cisco Security Agent is installed and before the server reboots.
- On the Cisco 7845 Series server that is running MCS-OS 2003 SR:
 - If Cisco Security Agent is pre-installed, there is no need to run the utility.
 - If Cisco Security Agent is installed after the platform upgrade, running the utility is needed.
- On the Cisco 7845 Series server that is running MCS-OS 2003, if for any reason Cisco Security Agent is uninstalled and reinstalled, running the utility is needed.

The memRegRepair utility may be obtained at the following URL:

[http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=3.0\(6\)&mdfid=280771554&sftType=Security+Agent+System+Software+for+Unified+Communications+Manager%2FCallManager&optPlatform=&nodecount=7&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+4.3&treeMdfid=278875240&modifmdfid=null&imname=&treeName=Voice+and+Unified+Communications&hybrid=Y&imst=N](http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=3.0(6)&mdfid=280771554&sftType=Security+Agent+System+Software+for+Unified+Communications+Manager%2FCallManager&optPlatform=&nodecount=7&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+4.3&treeMdfid=278875240&modifmdfid=null&imname=&treeName=Voice+and+Unified+Communications&hybrid=Y&imst=N)

Testing the Cisco Security Agent

In addition to verifying that the Agent is installed, you may want to test the Agent by attacking your own system. If so, go to the “Attack your system” section in the appendix “Evaluating the Cisco Security Agent” in *Installing Management Center for Cisco Security Agents 4.0*, which can be accessed from http://www.cisco.com/en/US/partner/docs/security/csa/csa52/install_guide/AppexB.html

Messages and Logs

For Cisco Unified Communications Manager Release 4.x

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

The messages that display comprise those that were generated when an action either was denied or generated a query. Only the two most recent messages display.

Find the log files in <InstallDrive>:\Program Files\Cisco\CSAgent\log.

- securitylog.txt—This main event log includes logs of rule violations and other relevant events.
- csalog.txt—This file provides Agent startup and shutdown history.
- driver_install.log—This log file provides a record of the driver installation process.
- Cisco Security AgentInstallInfo.txt—This file provides a detailed record of the installation process.

You can view the securitylog.txt file by using Notepad, or, to read the file more easily, you can

1. Copy the file to a computer on which Excel or another spreadsheet is installed.
2. Rename the file to securitylog.csv.
3. Double-click it to view it in the spreadsheet application.

The field names display in the first line of the spreadsheet. You may find it more convenient to see the contents of a spreadsheet cell by clicking the cell and looking at the contents in the field above the spreadsheet matrix.

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

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



Note

Under normal circumstances, you should see very few entries in the log. A flurry of entries that appear at a particular time indicates that something of interest is occurring. You can usually tell from the text that describes the events whether this is due to some internal problem (such as someone trying to install software without disabling the Agent) or an external problem (such as an attack on the system that the Agent is detecting and preventing).

For Cisco Unified Communications Manager Release 5.x and later

Perform the following steps to view CSA information:

1. View and collect CSA logs (csalog and securitylog.txt) by using the Trace & Log Central tool of Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT).
2. Use the Collect Files option and choose Cisco Security Agent in System Logs.
3. Use Remote Browse option to view the logs.
4. Choose Collect CSA log files by using the Trace & Log Central tool.
5. To view the CSA log files by using Remote Browse option, double-click the **csalog** file that displays in the window.



Tip

For more information on trace collection, refer to the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

Troubleshooting for Release 4.x

Review the troubleshooting tips in this section before contacting the Cisco Technical Assistance Center (TAC).

Problems with Installing or 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 you did not use Terminal Services to install/upgrade the software.
- Verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Obtain the installation logs from <InstallDrive>:\Program Files\Cisco\CSAgent\log. Inspect the Cisco Security AgentInstallInfo.txt and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log should state that the csanet2k.inf installed. If the Network Shim is not installed, uninstall the agent and then install the agent again.

Problems Running Cisco Unified Communications Manager or CSA Errors

Perform the procedure in this section if you encounter any of the following problems after installing Cisco Security Agent for Cisco Unified Communications Manager:

- Problems with Cisco Unified Communications Manager that cannot otherwise be explained
- CSA errors in the Windows event log or in the CSA log file (<InstallDrive>:\Program Files\Cisco\CSAgent\log\securitylog.txt)
- CSA error messages that display

If you cannot determine the cause of a CSA log entry or error message, contact Cisco TAC. However, before doing so, refer to the [“Before You Call TAC” section on page 16](#).

To troubleshoot problems with Cisco Unified Communications Manager or errors from Cisco Security Agent, perform the following procedure:

Procedure

-
- Step 1** Disable Cisco Security Agent. See the [“Disabling the CSA” section on page 8](#).
 - Step 2** Perform the operation that caused the error message.
 - Step 3** In the Windows task bar, 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 all the software applications that are running on the Cisco Unified Communications Manager server are supported third-party applications that are shown in the [“Introduction” section on page 2](#).

If unsupported software is installed on the server, remove the unsupported software and repeat this procedure.

If you cannot resolve the problem, refer to the [“Before You Call TAC” section on page 16](#).

Second Attempt to Install Software Fails Without a Warning

Cisco Security Agent caches your responses to queries for 1 hour. This convenience feature means that you do not have to respond to a popup each time that you do a repetitive action; however, in certain situations, this feature may have undesirable results.

In the following case, an 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 action causes the problem when running the install the next time—see below.)
3. You stop and disable the Cisco Security Agent service.
4. You attempt to install the software a second time, but nothing happens.

When you clicked **No** in step 2 above, the system cached your answer in memory. The system clears the cache automatically after an hour.

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

Procedure

- Step 1** Reenable the service, as described in the section [Reenabling the CSA, page 9](#).
- Step 2** In the Windows task bar, double-click the Cisco Security Agent icon in the Windows system tray (the red flag).
- Step 3** Click User Query Response.
- 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 the [“Disabling and Reenabling the Cisco Security Agent Service for Release 4.x” section on page 7](#).

Before You Call TAC

If you cannot identify the problem after reviewing the troubleshooting tips, follow the procedure below before calling Cisco TAC:

Procedure

-
- Step 1** In <InstallDrive>\Program Files\Cisco\CSAgent\bin, double-click csainfo.bat. This will collect useful hardware and software data.
 - Step 2** csainfo will ask whether you want to stop the Agent. Click **Yes**. The file csainfo.log gets 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 section [Checking the Agent and Policy Versions on the Server](#), page 7, describes the method for doing this).
 - Step 5** Contact TAC. Be prepared to provide them with the zipped file that you created in Step 3 and the information that you collected in Step 4.
-

Troubleshooting for Release 5.x and Later

Review the troubleshooting tips in this section before contacting the Cisco Technical Assistance Center (TAC).

Types of Support

The following Cisco Unified Communications Manager policy-related issues exist:

- Performance of Cisco Unified Communications Manager Release 5.x and later and approved third-party applications is restricted.
- System remains vulnerable to attacks.

The following CSA Application issues exist:

- CSA Application crashes
- System memory leaks

Make sure that the problem applies to Cisco Unified Communications Manager Release 5.x and later or approved third-party applications. For these approved programs, you must ensure that they are installed in the default installation path.

Collecting Troubleshooting Information for TAC

Cisco Systems TAC requires the following information to resolve the problem:

- Collect relevant information about the customer environment; for example, operating system, service pack, hardware configuration.

- Examine log files. You may not need to do this if the problem can be reproduced and understood. If the problem is not reproducible and looking at the log files is necessary, the support staff will do so.
- Access the log files for the CSA Agent by using RTMT; the log file names are csalog and securitylog.txt.

**Note**

You can also access the log file with this CLI command: **utils create report csa**. Refer to the Cisco Unified Communications Operating System Administration Guide for more information about starting a CLI session and using CLI commands.

- Access any memory dump files, if applicable.

If call processing is down because of CSA, stop the CSA Agent by entering the CLI command **utils csa disable** and gather the requested data. Follow the same escalation process as is used in other cases. If the problem turns out to be legitimate, a new Policy will get generated, and a new CSA install will get posted to CCO.

Obtaining Additional Information About the Cisco Security Agent

The following section does not apply to Cisco Unified Communications Manager Release 5.x and later. For additional information on the Cisco Security Agent, perform the following procedure:

Procedure

- Step 1** Perform one of the following tasks:
- In the Windows system tray, right-click the flag and choose **Open Control Panel**; go to [Step 2](#).
 - Choose **Start > Programs > Cisco Security Agent > Cisco Security Agent**; go to [Step 2](#).
- Step 2** In the upper, right corner of the window, click the ? icon.
The Cisco Security Agent documentation displays.

**Tip**

To obtain Cisco Security Agent documentation, click the following URL:

<http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html>

Obtaining Related Cisco Unified Communications Manager Documentation

Click the URLs in [Table 1](#) to navigate to related Cisco Unified Communications Manager documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm Note This information applies to Cisco Unified Communications Manager that runs on a Windows platform.
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
<i>Cisco Unified Communications Manager Software Compatibility Guide</i>	Refer to the Cisco Unified Communications Manager Release Notes to find the appropriate compatibility matrix link for your software release
Cisco Unified Communications Manager documentation	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Unified Communications Manager backup and restore documentation	For Cisco Unified Communications Manager Release 4.x: http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm For Cisco Unified Communications Manager Release 5.x and later (find the <i>Disaster Recovery System Administration Guide</i> for your release): http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html Note Use <i>Disaster Recovery System Administration Guide</i> Release 6.0(1) for Release 5.1.
Cisco Unified Communications Manager, SQL Server, and operating system service releases, upgrades, and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml Note The operating system and SQL Server 2000 service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco Unified Communications Manager software page. This information applies to Cisco Unified Communications Manager that runs on a Windows platform.
Related Cisco IP telephony application documentation	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Emergency Responder	http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wl/export/crypto/tool/stqrg.html>

If you require further assistance, please contact us by sending email to export@cisco.com.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installing Cisco Security Agent for Cisco Unified Communications Manager
Copyright © 2009 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.