Installing Cisco Security Agent for Cisco Customer Response Solutions

This document provides installation instructions and information about Cisco Security Agent (CSA) for Cisco Customer Response Solutions (CRS). If Cisco CRS resides on the same server with Cisco Unified Communications Manager, you can use this document or the *Installing Cisco Security Agent for Unified Communications Manager* document to install the agent on that co-resident server, because both products use identical security policies.

Note When Cisco Unified Communications Manager is installed on the Linux operating system, Cisco CRS and Cisco Unified Communications Manager cannot reside on the same machine. Use this document to install CSA for Cisco CRS on the Microsoft Windows operating system.

Contents

This document includes the following sections:

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

Introduction

The standalone CSA provides:

- Intrusion detection and protection for Cisco CRS.
- Defense against previously unknown attacks because CSA does not require signatures, as anti-virus software does.
- Reduction in downtime, in widespread attack propagation, and in clean-up costs.

The Agent is provided free of charge by Cisco Systems for use with Cisco CRS software. The Agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested security rules set (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 Do not view CSA for Cisco CRS as providing complete security for Cisco CRS servers. Rather, view the Agent as an additional line of defense that, when used with other standard defenses such as virus-scanning software and firewalls, provides enhanced security. CSA for Cisco CRS provides enhanced defense for many different Cisco CRS 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 operating system updated. The source for many security references is the *IP Telephony Security Operations Guide to Best Practices* found at this location:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e47.html

The standalone CSA uses a static policy that cannot be changed or viewed. However, see the section Migrating to the Management Center for CSA, page 8, for additional information.

Follow the installation instructions in this document to install the standalone CSA on all servers within the CRS cluster, including the CRS Engine, Database, and Voice over IP Monitoring components. Do not install the agent on client machines, such as those running the Cisco Desktop Product Suite or MRCP servers.

Note If CSA has already been installed on a server where both Cisco Unified Communications Manager and Cisco CRS reside, do not install CSA again on that server. Both products conform to the same CSA policies for the Microsoft Windows operating system. However, if Cisco Unified Communications Manager has been installed on the Linux operating system, install Cisco CRS on a separate machine running the Microsoft Windows operating system.

System Requirements

- Cisco Customer Response Solutions.

  Supported Cisco CRS releases are published in the *Cisco CRS Software and Hardware Compatibility Guide*:

  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_technical_reference_list.html
- Microsoft Windows 2003 Server in English.
- Windows Automatic Update configured so that it does not automatically download updates to the CRS server.

Before You Begin the Installation

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

- CSA supports any Cisco Media Convergence Server (MCS) or customer-provided, Cisco-approved server where Cisco CRS and Cisco-provided operating system are installed, unless the *Cisco CRS Software and Hardware Compatibility Guide* indicates otherwise.
- Confirm that the computer you are using to install CSA has up to 20 MB of hard disk space for the download file and the installed files.
- Do not install the agent between the operating system and Cisco Unified Communications Manager installation.
- Before each Cisco CRS upgrade, you must disable the CSA service. You must also make sure that the service does not get enabled at any time during the Cisco CRS installation. For information about how to disable the service, see the section Disabling and Reenabling the CSA Service, page 6.
- You must disable the CSA service before every operating system or Cisco CRS 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 operating system, Cisco CRS, service release, or support patch, you must enable the CSA Service. When you disable the service, the agent no longer provides intrusion detection for the server.
- Before you install or upgrade CSA, back up your Cisco CRS data. For more information about how to perform this task, refer to the *Cisco CRS Administration Guide* located here:

  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- Before you install or upgrade CSA, back up all applications that run in the voice cluster. Refer to the appropriate backup documentation for more information.

- Do not use Terminal Services to install or upgrade CSA. Cisco installs Terminal Services so the Cisco Technical Assistance Center (TAC) 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.

Caution If you currently run Cisco HIDS Agent (Entercept) on the server, you must uninstall the software from Add/Remove Programs before you install CSA. If you fail to uninstall the Cisco HIDS Agent before the Cisco Security Agent installation, the installation deletes the TCP stack, and CSA does not install the firewall component that is necessary for security.

- The agent installation causes a brief spike in CPU usage. To minimize call-processing interruptions, install CSA during a time when call processing is minimal. CSA protects the server as soon as you install the software but does not provide complete functionality until you reboot the server.

Caution Rebooting the server might cause call-processing interruptions. Reboot the server at the end of the business day or during a time when call-processing is minimal.

- Before you upgrade the agent or reinstall the agent on the server, you must uninstall the agent and then reinstall the software. When you uninstall the agent by using Add/Remove Programs or **Start > Programs > Cisco Security Agent > Uninstall Cisco 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, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2003 system tray, 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. Security logs display in the Message tab of the agent GUI, in Microsoft Event Viewer, and in the securitylog.txt file (C:\Program Files\Cisco\CSAgent\log).
- The Cisco IP Telephony Applications Backup Utility does not back up the log files or text file that the agent generates. If you need to restore the Cisco CRS data to the server for any reason, you must reinstall CSA after you restore the data.

Tip If you encounter problems with installing or uninstalling CSA, see the section Troubleshooting, page 10.

Installing CSA

Review the section Before You Begin the Installation, 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 3DES**

Cryptographic Software under export licensing control. On the page that appears, select **CallManager** from the drop-down list of products and click **Submit**. A web form appears; check the appropriate boxes on that form and click **Submit**. A message appears telling you when you can expect to have download access.

To download and install the CSA software, complete the following steps:

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

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

Note The filename structure is *CiscoCM-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 file name CiscoCM-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.

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

Step 4 Double-click the downloaded file to begin the installation.

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

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

Step 7 Click **Next** to accept the default destination where the software will install;.

Caution The Cisco CRS policy rules are directory specific, so the default directory must be used.

Step 8 Click **Next** to install the Network Shim.

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

Step 9 The status window displays the options that you chose. To accept the current settings, click **Next**.

Step 10 Continue to wait while the installation completes; do not click Cancel.

Step 11 Click **Yes**.

Caution The installation process can affect the performance of Cisco CRS, so it is best to install CSA for CRS and then reboot the server after regular business hours. Rebooting the server might 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 12 Click **Finish** to reboot the server.

Tip When the installation completes, a red flag displays in the Windows 2003 system tray. You can also verify that the software installed by locating CSA in the Add/Remove Programs window.

Step 13 Perform this procedure on every server in the CRS cluster.

Checking the Agent and Policy Versions on the Server

To determine the agent and policy versions, complete the following steps:

Step 1 Double-click the red flag icon in the system tray area.

Step 2 Choose **Status** to view the Product ID information.

Disabling and Reenabling the CSA Service

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 reenable it before it starts monitoring the Cisco CRS server again.

Use "Services" selected from the Microsoft Administrative Tools Control Panel to disable the Cisco Security Agent. It is best to shut down CSA and then deliberately start it up again.

Caution It is possible to suspend CSA using the "net stop csagent" command in a command shell. This method does not actually disable the agent; it merely suspends it. Suspending the agent is not supported 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.

Disabling the CSA Service

To disable the CSA service, complete the following steps:

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

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

Step 3 In the Properties window, verify that the General tab displays.

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 CRS.

Caution You must reenable the CSA service after every Cisco CRS installation or upgrade.

Reenabling the CSA Service

To reenable the CSA service after installing, upgrading, or uninstalling software, complete the following steps:

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

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

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

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

Step 5 Click **Apply**.

Step 6 Click **Start**.

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

Step 8 Close the Services window.

Uninstalling CSA

Review the section Before You Begin the Installation, page 3, which provides information about uninstalling CSA.

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 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, complete the following steps:

Step 1 Choose **Start > Programs > Cisco Security Agent > 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 2003 system tray, the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

Please note that the way in which the version number is reported changed in CSA 4.5 (file name starting with CiscoCM-CSA-4.5...) as compared to CSA 4.0 (file name starting with CiscoCM-CSA-4.0...). In CSA 4.5, the version number is integrated with the Standalone Agent as described in Checking the Agent and Policy Versions on the Server, page 6. In CSA 4.0, the version is obtained by selecting **Start > Cisco OS Version**. When uninstalling CSA 4.5, the policy version is removed along with the Standalone Agent. When uninstalling CSA 4.0 and selecting **Start > Cisco OS Version**, the old information

continues to appear unless you manually delete it by using regedit to remove the entry "CCM-CSA Policy" at HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems, Inc.\System Info\CCM-CSA Policy. If you have never installed a CSA 4.0-based policy, then this does not apply.

Upgrading CSA

Before you upgrade CSA, perform the following tasks:

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

   See the section Uninstalling CSA, page 7.

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

   See the section Installing CSA, page 4.

Migrating to the Management Center for CSA

The security agent included with Cisco CRS uses a static policy that cannot be changed or viewed. It is possible to add, change, delete, or view policies if you purchase and install the fully-managed console product, Management Center for Cisco Security Agent (CSA MC). However, any such changed policy is **NOT** qualified 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 installed on other network systems and servers.
- CSA (the managed agent) installs on all Cisco CRS servers in the voice 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/prod_technical_documentation.html

In a Cisco CRS environment, ensure that the Management Center component is installed on a separate, secured server and that the managed agent component is installed on all Cisco CRS 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*.

Once you have obtained the CSA MC package and documentation, perform the following procedure.

Step 1 On a separate (non-Cisco CRS) server, download the latest version of the Cisco Unified Communications Manager policy XML file (CiscoCM-CSA-*n.n.n.nnn-n.n.nn*.export) from the Cisco Unified 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 save the downloaded file.

Step 3 Uninstall CSA, if it exists, following the instructions in the Uninstalling CSA 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.

Messages, Logs, and Caching

This section provides information about how the cache works and discusses event messages and log files.

Event Messages and Log Files

If CSA 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 following 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 following these steps:

1. Double-click the CSA icon (the red flag in the Windows system tray)
2. Click **Messages** (on the left under Status)
3. Click **View Log** and a pop-up window displays the text of the log file.

You can also use Microsoft Excel to read the file more easily, by following these steps:

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

The field names display in the first line of the spreadsheet. You might find it more 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 include DateTime, Severity, Text, and User. Ignore the RawEvent field; it contains essentially the same information 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 describing the events whether these entries are 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).

Understanding How the Cache Works

CSA caches your responses to queries. This is a convenience feature so that you do not have to respond to a pop-up each time you do a repetitive action. The Agent can remember query responses either permanently or temporarily.

The Agent remembers responses to queries permanently based on user input. For example, if a user is queried as to whether an application can talk on the network, and the user responds by selecting **Yes** and clicking **Don't ask again**, the Agent remembers the Yes response permanently and that response appears in the right pane of the window that appears when you double-click the red flag icon and select **Status > User Query Responses** in the left pane.

The Agent remembers responses to queries temporarily if, for example, the user is queried as to whether setup.exe can install software on the system and the user selects **Yes**, but is not given the option of selecting **Don't ask again**. Then the query does not appear when you select **Status > User Query Responses**.

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

Troubleshooting

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 or uninstall CSA.
- For installations, verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Verify that the CSA service is not disabled and that its Startup Type value is Automatic.
- Obtain the installation logs from <*Install Drive*>:\Program Files\Cisco Systems\CSAgent\log. Review the CSAgent-Install.log and driver_install.log files.

Before You Call Cisco TAC

If you cannot identify the problem after reviewing the troubleshooting tips, follow the procedure below before calling the Cisco Technical Assistance Center (TAC):

Step 1 Check the CSA diagnostics by selecting **Start > Programs > Cisco Security Agent > Cisco Security Agent Diagnostics**.

Step 2 Respond **Yes** when asked if you want to stop the Agent. A command window shows files being copied. When the operation is complete, a message box indicates the location of the csa-diagnostics.zip file.

Step 3 Click **OK.** The Agent restarts.

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 6, describes the method to do so).

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

Obtaining Additional Information About CSA

For additional information about CSA, perform the following procedure:

Step 1 Perform one of the following tasks:

- In the Windows 2003 system tray, right-click the flag and choose **Open Control Panel**; go to Step 2.
- Choose **Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent**; go to Step 2.

Step 2 In the lower right corner of the window click the **Help** button.

The CSA documentation displays.

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

Obtaining Related Cisco CRS Documentation

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

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	**Boldface** font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit > Find**. • Click **Finish**.
italic font	*Italic* font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window` font	`Window` font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems,Inc. </title></html>`
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and 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