Installing Cisco Security Agent for Cisco Customer Response Applications, Releases 2.2(5), 3.0(3), and 3.1(2)

This document provides installation instructions and information about Cisco Security Agent 4.01.539-1.1(3) for Cisco Customer Response Applications (CRA), Releases 2.2(5), 3.0(3), and 3.1(2). If Cisco CRA resides on the same server with Cisco CallManager, you can use this document or the *Installing Cisco Security Agent for Cisco CallManager Releases 3.2(3), 3.3, and 4.0* document to install the agent on that co-resident server, because both products use identical security policies.

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

Cisco Security Agent provides intrusion detection and protection for Cisco CRA. It is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with servers in the Cisco CRA voice cluster. The agent provides Windows platform security based on a tested security rules set (policy). The policy has rigorous levels of host intrusion detection and prevention. The agent verifies whether an action is allowed or denied before system resources are accessed. This process occurs transparently and does not hinder overall system performance.

The standalone Cisco Security Agent uses a static policy that cannot be changed or viewed. If you want to make changes to the policy you must purchase the Management Center for Cisco Security Agent. See the section Migrating to the Management Center for Cisco Security Agent, page 7, for additional information.

Follow the installation instructions in this document to install the standalone Cisco Security Agent on all servers within the voice cluster, including Cisco CRA, Remote Database, voice, and speech servers. Do not install the agent on client machines.

Note If Cisco Security Agent has already been installed on a server where both Cisco CallManager and Cisco CRA reside, do not install Cisco Security Agent again on that server. Both products conform to the same Cisco Security Agent policies.

System Requirements

- Cisco CRA, 2.2(5), 3.0(3), or 3.1(2).
- Microsoft Windows 2000 Server in English
- Windows Automatic Update configured so that it does not automatically download updates to the CRA server.

Before You Begin the Installation

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

- Confirm that the computer you are using to install Cisco Security Agent has up to 20 MB of hard disk space for the download file and the installed files.
- Before each Cisco CRA 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 CRA installation. For information on how to disable the service, see the section Disabling the Cisco Security Agent Service, page 5.
- You must disable the Cisco Security Agent service before every operating system or Cisco CRA 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 CRA, service release, or support patch, you must enable 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 Cisco Security Agent, back up your Cisco CRA data. For more information on how to perform this task, refer to the appropriate version of the Cisco CRA backup documentation.
- Before you install or upgrade the Cisco Security Agent, 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 the Cisco Security Agent. 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 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.

- The agent installation causes a brief spike in CPU usage. To minimize call-processing interruptions, Cisco recommends that you install the Cisco Security Agent during a time when call processing is minimal. The Cisco Security Agent 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. Cisco recommends that you 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 Systems > 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 install 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 2000 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 Customer Response Applications data to the server for any reason, you must reinstall the agent after you restore the Cisco CRA data.

Tip If you encounter problems with installing or uninstalling the Cisco Security Agent, see the section Troubleshooting, page 8.

Installing the Cisco Security Agent

Review the section Before You Begin the Installation, page 2, which provides information to help ensure a successful installation. To install the Cisco Security Agent, complete the following steps:

Step 1 From the CRA Server, go to the Voice Software Download page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

The Cisco Security Agent and policies post on the voice products cryptographic software page. You can navigate to the site from the Voice Software Download page.

Step 2 Download the latest version of the Cisco Security Agent file, **CiscoCM-CSA-4.0.1.539-1.1.3-K9.exe**.

Step 3 Note the location where you saved 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 Choose a location where the software will install; click **Next**

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** to reboot the server.

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 12 Click **Finish**.

Tip When the installation completes, a red flag displays in the Windows 2000 system tray. You can also verify that the software installed by locating the Cisco Security Agent in the Add/Remove Programs window.

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

Verifying the Agent Version on the Server

Complete the following steps to verify the Cisco Security Agent version on the server:;

Step 1 Use Windows Explorer to browse to the following folder:

C:\utils\MCSver.exe

Step 2 Locate the agent version.

Disabling the Cisco Security Agent Service

Review the section Before You Begin the Installation, page 2, which provides information about disabling the Cisco Security Agent Service.

Perform the following procedure(s) serially; that is, on one server at a time. After you complete the operating system, Cisco CRA, service release/support patch installation or upgrade, you can enable the service on the server; then, you can disable the service on the next server where you plan to install or upgrade the operating system, Cisco CRA, or service release/ support patch.

You can disable the Cisco Security Agent service in one of the following three ways:

- Using Microsoft Administrative Tools Control Panel
- Using the netstop command
- Using the Cisco Security Agent tool bar icon

Caution Cisco Systems recommends that you use the Microsoft Administrative Tools Control Panel to disable the Cisco Security Agent. It is better to shut down the Cisco Security Agent and then deliberately start it up again. If you use one of the other methods, the service is suspended but not actually disabled, and in the event the installer reboots your machine, the reactivated service might interfere with the installation of other software.

Using Microsoft Administrative Tools Control Panel

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.**

Step 7 Perform this procedure on every server where you plan to install or upgrade Cisco Customer Response Applications.

Caution You must enable the Cisco Security Agent service after the Cisco CRA installation or upgrade.

Using the net stop Command

Complete the following steps:

Step 1 Open a DOS command line window by clicking **Start > Run**, entering **cmd** in the Open field, and clicking **OK**.

Step 2 Type **net stop csagent** and press **Enter**.

A message appears confirming that the security agent service was successfully stopped.

Step 3 Type **exit** and press **Enter** to close the window.

Caution After you have finished the installation or upgrade, restart the service by performing the above procedure using the command **net start csagent**, or reboot the machine and the service will restart automatically.

Using the Tool Bar Icon

Complete the following steps:

Step 1 Right-click on the Cisco Security Agent red flag icon in the system tray in the right corner of your desktop.

Step 2 Select **Suspend Security** and click **Yes.**

Caution After you have finished the installation or upgrade, you can restart the service by right-clicking the icon and then selecting **Resume Security**, or reboot the machine and the service will restart automatically.

Uninstalling the Cisco Security Agent

Review the section Before You Begin the Installation, page 2, which provides information about uninstalling the Cisco Security Agent.

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 Perform one of the following tasks:

- Choose **Start > Control Panel > Add/Remove Programs**; click **Remove** for the Cisco Security Agent; go to Step 2.
- Choose **Start > Programs > Cisco Systems > Uninstall Cisco Security Agent**; go to Step 2.

Step 2 To stop the agent, click **Yes**.

Step 3 To uninstall the agent, click **Yes**.

Step 4 Reboot the server.

Upgrading the Cisco Security Agent

Before you 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 6.

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

   See the section Installing the Cisco Security Agent, page 4.

Migrating to the Management Center for Cisco Security Agent

The security agent included with Cisco CRA uses a static policy that cannot be changed or viewed. To add, change, delete, or view policies included in Cisco Security Agent for Cisco CRA, or to add support for non-Cisco approved third-party applications, you must purchase and install the fully-managed console product, Management Center for Cisco Security Agent (CSA MC).

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.
- The Cisco Security Agent (the managed agent) installs on all Cisco CRA 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 even 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/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/csa_4_0/

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

Step 1 Uninstall the Cisco Security Agent following the instructions in the Uninstalling the Cisco Security Agent section of this document.

Step 2 Download the latest version of the Cisco Customer Response Applications policy XML file. You can obtain the policy on the Voice Software Download page at:

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

Note The Cisco Security Agent and policies post on the voice products cryptographic software page. You can navigate to the site from the voice application software page.

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

Step 4 Follow the instructions in *Installing Management Center for Cisco Security Agents* for Installing CSA MC.

Step 5 Follow the instructions in *Using Management Center for Cisco Security Agents* for importing the policy.

Troubleshooting

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.
- For installations, verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Verify that the Cisco Security Agent service is not disabled and that its Startup Type value is Automatic.
- Obtain the installation logs from C:\Program Files\Cisco\CSAgent\log. Review the Cisco Security AgentInstallInfo.txt and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log file should state that the csanet2k.inf installed. If the Network Shim is not installed, uninstall the agent and then install the agent again.

Obtaining Additional Information About CSA

For additional information about the Cisco Security Agent, perform the following procedure:

Step 1 Perform one of the following tasks:

- In the Windows 2000 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 upper, right corner of the window click the **?** icon.

The Cisco Security Agent documentation displays.

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

Obtaining Related Cisco CRA Documentation

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/english/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

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

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL;

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

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

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.

- Priority level 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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..

Cisco TAC Website

The Cisco TAC Website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC Website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Website. The Cisco TAC Website requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Website, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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