Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal

Release 8.0(1)

May 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.

Copyright 2010 Cisco Systems, Inc. All rights reserved.

Table of Contents

Preface 1
Purpose 1
Related Documentation 1
Conventions....1
Obtaining Documentation and Submitting a Service Request....2
Documentation Feedback....2

1. Introduction....3
Installation Directories....5

2. System Requirements....7

3. Before You Begin Installation....9

4. Installing Cisco Security Agent....11
How to Install Cisco Security Agent....11
Checking the Version on the Server....13

5. Disabling and Re-enabling Cisco Security Agent Service....15
How To Stop and Disable the Cisco Security Agent Service....15
How To Re-enable the Cisco Security Agent Service....16

6. Uninstalling Cisco Security Agent....17
How To Uninstall Cisco Security Agent....17

7. Upgrading Cisco Security Agent....19
How To Upgrade Cisco Security Agent....19

8. Messages, Logs, and Caching....21
Event Messages and Log Files....21
Understanding How the Cache Works....22

9. Troubleshooting....25
Problems Installing/Uninstalling the Agent....25
Problems with Unified CVP Software or Errors from Cisco Security Agent....25
How to Troubleshoot CVP Software or CSA Errors....26
What To Do Before Contacting TAC About A CSA Problem....26

10. Migrating to the Management Center for Cisco Security Agent....29
Importing the Unified CVP Policy....30
Important: Using Your Own CSA Management Center....31
Rebase CSA Agent....31
Upgrading Your CSA Management Center....32
Using CSA Management Center to Protect Against TCP Flood Attacks....33
Obtaining Additional Information about CSA....35

List of Figures

Figure 1: Open Agent Panel.....35

Preface

Purpose

This document provides installation instructions and information about Cisco Security Agent for Cisco Unified Customer Voice Portal (Unified CVP) Software. **You are strongly urged to read this document in its entirety.**

Related Documentation

Find the latest version of the Unified CVP software documentation at: **http://cisco.com/en/US/products/sw/custcosw/ps1006/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:

Convention	Description
	• 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Chapter 1

Introduction

The standalone Cisco Security Agent (CSA) provides:

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

Cisco Systems provides Cisco Security Agent for use with Unified CVP software at no charge. The Agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested set of security rules (policy). The Agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed.

A policy controls access to system resources based on:

- Resources being accessed
- Operation being invoked
- Process invoking the action

This occurs transparently and does not hinder overall system performance.

Note: Cisco also provides a set of policies that you may want to import to your own CSA Management Center if you want managed agents. The Cisco Security Agent and policies are available at no charge, but the Management Center (used to define the policies) is not. See Migrating to the Management Center for Cisco Security Agent (page 29) for more information.

Caution: Cisco Security Agent for Unified CVP does not provide complete security for Unified CVP servers. Cisco Security Agent is an additional line of defense that, when used correctly with other standard defenses such as virus-scanning software and firewalls,

provides enhanced security. Cisco Security Agent for Unified CVP provides enhanced defense for many different Unified CVP installations and configurations, and thus cannot act as a host-based firewall.

Other security considerations include keeping the OS updated.

The best starting point for references to security and voice products is **http://www.cisco.com/go/ipcsecurity**. A specific document to examine is the **IP Telephony Security Operations Guide to Best Practices** (http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e47.html).

The policy for the CSA standalone Agent for Unified CVP is created from the default policy modules that are shipped with Cisco Security Agent 6.0. These default policy modules secure/harden the system. These default policy modules are altered in order to allow Unified CVP including qualified third-party applications to run smoothly.

The standalone Cisco Security Agent for Unified CVP uses a static policy that can not be changed. However, the Management Center for Cisco Security Agents allows you to add, change, or delete the policy. Migrating to the Management Center for Cisco Security Agent (page 29), provides more information about how to run the managed agent to allow for policy modifications.

The CVP standalone Cisco Security Agent should be used where Unified CVP and Unified ICME components co-reside.

For servers running Cisco Unified ICME only, refer to the **Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions** (http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_installation_guides_list.html).

For servers running Cisco Unified Communications Manager (Unified CM), see **Installing Cisco Security Agent for Unified Communications Manager** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html).

For servers running Cisco Unified IP IVR, see **Installing Cisco Security Agent for Cisco Unified Contact Center Express** (http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html).

In addition to being specifically tuned for Unified CVP software, Cisco Security Agent for Unified CVP software provides support for a select number of Cisco-approved third-party applications. These are the third-party applications included in the **Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software** (http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html). **No other third-party applications are officially supported.** You must install third-party applications that are part of the Unified CVP installer using the Unified CVP installer (such as, Apache Tomcat). Other third-party applications (such as, IBM WebSphere and Microsoft Internet Explorer) must be installed in their default directories presented during the installation process—otherwise your applications will not work properly. See the discussion in Installation Directories (page 5).

If you use a third-party software application that is not Cisco-approved, see Migrating to the Management Center for Cisco Security Agent (page 29), for additional information.

Note:

- CSA for Unified CVP is not supported for Cisco Unified Call Studio.
- Automatic Windows updates are not allowed by the current Cisco Security Agent for Unified CVP policy. Only Windows update scans can be performed with CSA enabled. CSA must be disabled to perform Windows updates.
- When a newer version of the Agent becomes available, Cisco strongly recommends that you install the newer version for your specific version of Unified CVP. Check the Cisco.com web site for this information.
- CSA for Unified CVP does not cover third-party Media Servers because of the number of suppliers that exist and the resulting test effort involved.

Installation Directories

Cisco Security Agent leverages rules that incorporate path information. Application actions may be blocked if the application is not installed in the correct directory. For this reason, software must be installed to the default directories provided by the application installers.

Caution: Always use the default directories when installing software on a server, when not using the Unified CVP installer. You need not choose the default disk drive if an option is available (for example, C: or D:), but you must use default directories.

Chapter 2

System Requirements

The following are the system requirements for CSA in a CVP environment:

- Unified CVP 8.0(1) (see the **Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software** (http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html))
- Disk Space 25 MB
- Typical CPU Load (under normal circumstances): less than 5%

Chapter 3

Before You Begin Installation

Note:

- In Unified CVP 8.0(1), a newer standalone version of CSA for Unified CVP, based on the CSA engine version 6.0 is available. This means that the CSA agent kits and policies that worked with previous Unified CVP releases do NOT work with Unified CVP 8.0(1). Consequently, you must uninstall your previous version of CSA before upgrading to Unified CVP 8.0(1).

- New CSA agent kits and policies are available at: **http://www.cisco.com/cisco/web/download/index.html**. You must then log in using your Cisco support login information. Select **Voice and Unified Communications** then **Customer Contact > Cisco Unified Self Service Products > Cisco Unified Customer Voice Portal** then finally click **Cisco Security Agent for Speech Self Service**.

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

- Confirm that the computer you are using to install Cisco Security Agent has 25 MB of hard disk space available for the download file and the installed files.

- Either Unified CVP software must be installed before you install Cisco Security Agent, or you must make sure that Cisco Security Agent is disabled before you install Unified CVP.

- Before each Unified CVP upgrade, you must first stop and then disable the Cisco Security Agent service. You must also be sure that the service does not become enabled at any time during the Unified CVP installation. See Disabling and Re-enabling Cisco Security Agent Service (page 15) for instructions on disabling and re-enabling the service.

Caution: The Cisco Security Agent service must be disabled and stopped before any software installation is performed. This means before every operating system, Unified CVP and third-party installation and upgrade, including maintenance release, service release, Windows updates, and support patch installations and upgrades. Failure to do so may cause problems with the installation or upgrade, since the Cisco Security Agent may block part of the installation if not disabled. After installing or upgrading the software,

you must re-enable and start the Cisco Security Agent service before it can provide Windows platform security for the server.

- Terminal Services software is not supported for installation or upgrade of the Cisco Security Agent (unless you are logged into session :0 with console access). Virtual Network Computing (VNC) and pcAnywhere are supported for remote installation or upgrade of the Agent.

- The Agent installation and rebooting—as well as agent service startup—causes a brief spike in CPU usage and may cause processing interruptions on the server. Rebooting is automatically done immediately after installation. Although the Cisco Security Agent protects the server as soon as you install the software, it does not provide complete functionality until the server reboots.

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

- After the installation, you do not need to perform any Agent configuration tasks. The software immediately begins to work as designed. Security events may display in the Messages window of the Agent GUI (double-click the Cisco Security Agent icon—the red flag in the Windows system tray; then click on Message, on the left, under Status), as well as in Microsoft Event Viewer and/or in the securitylog.txt file (see Event Messages and Log Files).

  Note: If you encounter problems installing or uninstalling Cisco Security Agent, see Messages, Logs, and Caching (page 21) and Troubleshooting (page 25).

Chapter 4

Installing Cisco Security Agent

Caution: Before you upgrade or reinstall the Agent, you should uninstall the Agent. Do not install a newer version of the Agent on top of a previously installed version. See Uninstalling Cisco Security Agent (page 17) and Upgrading Cisco Security Agent (page 19).

Note:

- An important feature of the Management Center for Cisco Security Agents is that it has a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need to manually uninstall, install, and start CSA on each server. See Migrating to the Management Center for Cisco Security Agent (page 29).
- To install the Cisco Security Agent, you must be a System Administrator.

Review the section Before You Begin the Installation, which provides information to help ensure a successful installation. You must have access to a cryptographic site before you can download the Cisco Security Agent file. If you have not yet applied for such access, you will be directed to a web form. Complete the form and click Submit. You will receive a message to indicate when you can expect to have download access.

This chapter contains the following topics:

- How to Install Cisco Security Agent, page 11
- Checking the Version on the Server, page 13

How to Install Cisco Security Agent

To install the Cisco Security Agent for Unified CVP software, perform the following steps.

Step 1 From the server, browse to **http://www.cisco.com/cisco/web/download/index.html**. You must then log in using your Cisco support login information. Select **Voice and Unified Communications** then **Customer Contact > Cisco Unified Self Service Products > Cisco**

Unified Customer Voice Portal then click **Cisco Security Agent for Speech Self Service** and select your release of Unified CVP.

Step 2 Download the latest version of the Cisco Security Agent file: **CiscoCVP-CSA-<version>-K9.exe**.

For example, CiscoCVP-CSA-5.2.0.238-3.0.1-W_K9.exe, where 5.2.0.238 indicates the engine version and 3.0.1 indicates the policy version).

Step 3 Note the location where you saved the downloaded file(s).

Step 4 Double-click **CiscoCVP-CSA-<version>-K9.exe** to begin the installation.

Step 5 The Welcome window displays. Click **Next**.

The license agreement displays.

Step 6 Review the agreement. Click **Yes**.

The Choose Destination Location window displays.

Step 7 Accept the default destination or choose an alternate location. Click **Next**.

The Preparing to transfer files status window displays.

Step 8 Review the selections. To accept these settings, click **Next**.

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

Step 10 Ensure the radio button is set to **Yes** (the default), then click **Finish** to reboot the server.

Caution: As mentioned earlier, the Agent protects the server as soon as you install the software, but the Agent does not provide complete functionality until the server is rebooted. Rebooting is automatically done immediately after installation. Although the Cisco Security Agent protects the server as soon as you install the software, it does not provide complete functionality until the server is rebooted. To minimize affects on resources (such as processing interruptions), Cisco recommends that you install/reboot at the end of the business day or during a time when processing is minimal, preferably during a regularly scheduled maintenance window.

Note: When the installation completes, a red flag (the Cisco Security Agent icon) displays in the Windows system tray. Double-click on the red flag. When Security:Medium displays in the lower right corner of the Cisco Security Agent window, security is enabled.

Perform this procedure on each Unified CVP software server. As noted, Cisco Security Agent for Unified CVP should not be installed on the Media Server and Call Studio machines.

Checking the Version on the Server

To verify the engine and policy versions of the Agent, double-click on the CSA flag in the system tray. The Product ID is included in the Status section of the Cisco Security Agent window. For example, the Product ID might display as Unified CVP CSA 5.2.0.238 Policy 3.0.1. In this example, 5.2.0.238 is the engine version and 3.0.1 is the policy version.

If the CSA flag is not available, retrieve it by clicking Cisco Security Agent in the Start menu.

Chapter 5

Disabling and Re-enabling Cisco Security Agent Service

You must stop and then disable the Cisco Security Agent service prior to installing, upgrading, or uninstalling software. This means before every operating system, Unified CVP and third-party installation and upgrade, including maintenance release, service release, Windows updates, and support patch installations and upgrades.

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

After installing or upgrading the software, you must re-enable and start the Cisco Security Agent service before it can provide Windows platform security for the server.

This chapter contains the following topics:

- How To Stop and Disable the Cisco Security Agent Service, page 15
- How To Re-enable the Cisco Security Agent Service, page 16

How To Stop and Disable the Cisco Security Agent Service

To stop and disable the Cisco Security Agent service, perform the following steps:

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

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

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

Step 4 Click **Stop**.

CSA is stopped. This is indicated by a small red X in the bottom left corner CSA icon in the system tray.

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

Step 6 Click **OK**.

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

Step 7 Close **Services**.

Note: You must re-enable the Cisco Security Agent service after installing, upgrading, or uninstalling software.

How To Re-enable the Cisco Security Agent Service

To re-enable the Cisco Security Agent service, perform the following steps:

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

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

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

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

Step 5 Click **Apply**.

Step 6 Click **Start**.

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

Step 8 Close **Services**.

Chapter 6

Uninstalling Cisco Security Agent

Caution: Do not install one version of the Agent on top of a previously installed version. Cisco strongly recommends that you uninstall the Agent and then reinstall the software. When you start the uninstaller, the Agent prompts you to confirm the uninstall. You have a limited amount of time (five minutes) to disable the protection. If you do not disable the protection, the security mode automatically enables.

Note: The Management Center for Cisco Security Agents features a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need for you to manually uninstall, install, and start CSA on each server. See Migrating to the Management Center for Cisco Security Agent (page 29).

How To Uninstall Cisco Security Agent

To uninstall the Cisco Security Agent, perform the following steps:

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

Step 2 Click **Yes** in response to all prompts.

Caution: After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows system tray. The Messages window in the graphical user interface (GUI) displays errors, but the software does not provide protection.

Chapter 7

Upgrading Cisco Security Agent

How To Upgrade Cisco Security Agent

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

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

See Uninstalling Cisco Security Agent (page 17).

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

See Installing Cisco Security Agent (page 11).

Chapter 8

Messages, Logs, and Caching

This section discusses additional features of the Cisco Security Agent.

Event Messages and Log Files

- If the Cisco Security Agent has a message for you, the icon (the red flag in the Windows system tray) waves. To read the message, double-click on the icon, then click **Messages** (on the left, under Status).

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

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

  – securitylog.txt

    This is the main event log where rule violations and other relevant events are logged.

  – csalog.txt

    This provides Agent startup and shutdown history. It also contains events as well, but the securitylog.txt also contains the events and is easier to read.

  – driver_install.log

    This log provides a record of the driver installation process.

  – CSAgent-Install.log

    This log provides a detailed record of the installation process.

- View securitylog.txt using Notepad. The field names are given in the first line. To view the log:

- Double-click the **Cisco Security Agent icon**—the white shield with a red flag in the Windows system tray.
- Click **Events** (on the left, in the Tasks section).
- Click **View**.

  Note: Clicking **Purge** deletes all events stored in securitylog.txt. However, csalog.txt still contains that information.

- You can also:

  Copy **securitylog.txt** to a machine that has Excel and change the name to *securitylog.csv*.

  Double-click **securitylog.csv**, opening it as an Excel spreadsheet.

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

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

The ordering of the severity levels, from least to most severe, is:

- Information
- Notice
- Warning
- Error
- Alert
- Critical
- Emergency

Understanding How the Cache Works

Cisco Security Agent caches your responses to queries. This is a convenience feature, so that you do not have to respond to a popup each time you do a repetitive action.

When you are queried, the Agent remembers the response permanently or temporarily. This way, when the same rule is triggered again, the action is allowed, denied, or terminated based on the answer that was provided previously with no popup query box appearing again either permanently or for some period of time.

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

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

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

Chapter 9

Troubleshooting

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

Problems Installing/Uninstalling the Agent

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

- Verify the server has been rebooted.
- Verify that the Cisco Security Agent service is not disabled and that its Startup Type value is *Automatic*.
- Obtain the installation logs from <*InstallDrive*>:\Program Files\Cisco\CSAgent\log. Review the CSAgent-Install.log and driver_install.log files.
- Verify that you did not use Terminal Services.
- If, after uninstalling CSA, you cannot access the server remotely, examine the firewall settings. These settings may be preventing remote access.

Note: The Windows firewall is automatically disabled by the CSA installation because CSA cannot run concurrently with it. The Windows firewall is automatically reenabled when CSA is uninstalled.

Problems with Unified CVP Software or Errors from Cisco Security Agent

If you encounter problems after installing Cisco Security Agent for Unified CVP software, review the steps in this section and consider the following:

- Are these problems with Unified CVP software that cannot otherwise be explained?

- Are Cisco Security Agent error messages displayed (double-click on the flag icon, then click on Messages, on the left, under Status)?
- Look in the Cisco Security Agent log file (securitylog.txt) for events indicating that an application action was blocked by Cisco Security Agent.

If you cannot determine the cause of a Cisco Security Agent log entry or error message, contact Cisco TAC. However, before doing so, see What To Do Before Contacting TAC About A CSA Problem (page 26).

How to Troubleshoot CVP Software or CSA Errors

To troubleshoot problems with Unified CVP software or errors from Cisco Security Agent, perform the following steps:

Step 1 Disable CSA as described in How To Stop and Disable the Cisco Security Agent Service (page 15).

Step 2 Perform the operation that caused the error message.

Step 3 Reenable CSA as described in How To Re-enable the Cisco Security Agent Service (page 16).

Step 4 Perform the operation that caused the error message.

Step 5 If the operation completes successfully with the Cisco Security Agent turned off and continues to fail with the Cisco Security Agent enabled, confirm that the software with which you were having the problem is among the Unified CVP software components or third-party applications included in the **Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software** (http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html)

Step 6 If you are unable to resolve the problem, see What To Do Before Contacting TAC About A CSA Problem (page 26).

What To Do Before Contacting TAC About A CSA Problem

If you continue to experience a problem installing or uninstalling the Agent and you have performed all of the relevant troubleshooting steps outlined in this section, open a TAC case.

To run the CSA diagnostics utility and open a TAC case, follow the procedures below:

Step 1 Run the Cisco Security Agent Diagnostics program: **Start > All Programs > Cisco >Cisco Security Agent > Cisco Security Agent Diagnostics**

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

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

Step 2 When the collection is complete, a message appears informing you that a csa-diagnostics.zip file has been created in the <*InstallDrive*>\Documents and Settings\Administrator\Local Settings\Temp directory.

Step 3 Determine the version of your CSA engine and of your CSA policy (see Checking the Version on the Server (page 13) for instructions).

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

Chapter 10

Migrating to the Management Center for Cisco Security Agent

While the Security Agent included with Unified CVP software uses a static policy that should not be changed, it is possible to add, change, or delete the policy if you purchase and install Management Center for Cisco Security Agents. However, any such changed policy is NOT qualified for use with Unified CVP.

Note:

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

- Remove any third-party software not supported by Cisco from your Unified CVP servers.
- Revert to the original Cisco Security Agent for Unified CVP policy. If the problem persists, then call your support provider.

Management Center for Cisco Security Agent contains two components:

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

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

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

- If you are interested in the Management Center, obtain the latest version of the following Management Center for Cisco Security Agent documents:
  - **Installing Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)
  - **Using Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)
  - **Release Notes for Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)

This chapter contains the following topics:

- Importing the Unified CVP Policy, page 30
- Important: Using Your Own CSA Management Center, page 31

Importing the Unified CVP Policy

Ensure that the Management Center component is installed on a separate, dedicated server and the managed Agent is installed on all Unified CVP servers. Make sure that the server that is intended for the Management Center meets the system requirements that are listed in **Installing Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html).

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

Once you have obtained the Management Center for Cisco Security Agent package and documentation, and followed the CSA installation instructions in **Installing Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html), perform the following to import the Unified CVP policy and install a managed Agent:

Step 1 Uninstall the Cisco Security Agent, if it exists, by following the instructions in the section Uninstalling Cisco Security Agent (page 17).

Step 2 Download the latest version of the Unified CVP policy XML file (though an XML file, the extension is .export; for example, CiscoCVP-CSA-5.2.0.238-3.0.1.export).

Note: For information on how to obtain the policy for your Unified CVP version see the section Checking the Version on the Server (page 13).

Note the location where you saved the downloaded file. Also note that, for identification purposes, all Unified CVP policies are prepended with the "CVP".

Note:

- A File Set with the name "CVP All Files" means All Files on the system.
- While a File Set with the name "CVP All CVP Files" means All files related to the Unified CVP product. This use of the first word in all these variables is just a way to distinguish Unified CVP variables in your Management Center from variables associated with other policies; for example, policies supplied for Cisco Unified ICME or Unified CM.

Step 3 Follow the instructions in the *Exporting and Importing Configurations*section of **Using Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html) for importing the policy that you downloaded in Step 1.

Step 4 Use the *Quick Start Configuration* section of **Installing Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html) to perform the following tasks:

- Configure a group.
- Attach the downloaded policy named CiscoCVP-CSA-<version>.export to the group.
- Generate the Rules.
- Build an Agent kit.

Step 5 Distribute and install the new managed Agent that was created in Step 3 by following the instructions in the Cisco Security Agent Installation and Overview section of **Installing Management Center for Cisco Security Agents** (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html).

Important: Using Your Own CSA Management Center

If you are using your own CSAMC and not the CSA stand-alone agent provided by Unified CVP, please adhere to the instructions in this section.

Rebase CSA Agent

If you are using your own CSAMC and not the CSA stand-alone agent provided by Unified CVP, you must rebase your agents before installing them on a Unified CVP server. If CSA is not rebased, it can not be installed in a Unified CVP reporting server because it prevents the database from running. The rebased agent behaves exactly as the original agent kit; however, it just does not reside in the middle of the database memory space.

Unified CVP provides customers with a stand-alone Cisco Security Agent (CSA) that has been rebased. That is, the base address at which the DLL loads has been modified.

To rebase your CSA agent, complete the following steps:

Step 1 On the server where CSAMC is installed, download the agent kit generated on the CSA MC and copy it to a directory.

Step 2 Use a MS-DOS command window and issue the following command to extract all the files: **run <agentKitFileName> -x**.

A subdirectory is created, for example, "{D....}"

Step 3 In the MS-DOS command window, navigate to the new directory "{D....}" and execute the following command: **C:\Program Files\Cisco\CSAMC\CSAMC60\bin\bundler.exe" /sRebasedAgentKit.exe /esetup.exe /p"--autolevel=1 --rebase=0xC000000-0x70000000" /n_Setup.dll /nagent.bundle /nagent.rul /nagent.var /ndata1.cab /ndata1.hdr /ndata2.cab /nicon.ico /nISSetup.dll /nlayout.bin /nsetup.exe /nsetup.ini /nsetup.inx /nsetup.iss /nsslca.crt**

Step 4 Rename the new RebasedAgentKit.exe.

Step 5 Use the new Agent kit (from Step 4) to install CSA on your Unified CVP servers.

Upgrading Your CSA Management Center

If you are using your own CSAMC and would like to upgrade it to a newer version, you must first uninstall CSA on each of the reporting servers that have rebased agents. Then, upgrade the Management Center and reinstall a rebased agent on the reporting servers. To do this, complete the following steps:

Step 1 Uninstall the CSA on each of the reporting servers that are currently running rebased agents.

Step 2 Upgrade the Management Center by following the instructions in Migrating to the Management Center for Cisco Security Agent (page 29).

Step 3 Create a new agent kit and rebase it by following the instructions in Rebase CSA Agent (page 31).

Step 4 Install the new rebased agent kit on each of the reporting servers that you uninstalled during Step 1.

Note: The above-procedure is necessary because pushing a software update to the agents modifies the dll files that are rebased, which returns them to their original settings.

Using CSA Management Center to Protect Against TCP Flood Attacks

You can configure CSA management center to protect your servers against several types of TCP flood attacks, such as:

- ESTABLISHED
- FIN-WAIT
- CLOSING

The protection against flood attacks is provided by enabling Connection Rate Limit Rules. The steps below detail how to create Connection Rate Limit Rules to protect a server from flood attacks, however, you must consult the CSA documentation, modify the rules to your specific deployment, and test your configuration in a non-production environment before deploying the rules.

To protect against flood attacks, you use CSA management center to create two connection rate limit rules. The first rule that allows (Priority Allow) network connection from IP addresses that belong to Unified Communications Manager, Gateways, Unified Contact Center Enterprise, and other servers that require a connection to Unified CVP. The second rule denies all network connections when the machine is acting as a server. The general steps for creating this configuration are below. For specific details about using this configuration in CSA Management Center, see the documentation for CSA Management Center.

Step 1 Using the CSA Management Center, create the first Connection Rate Limit rule (Priority Allow). This rule allows IP addresses to connect to the Unified CVP server. Since this is a Priority Allow rule, the rule has priority over the second rule that you create to deny traffic to the server.

To create the first rule:

1. Expand the Rules area of the Rules module to which you are going to add the Priority Allow rule and click **Add**.
2. Select the *Connection Rate Limit* rule. The configuration view for this rule opens.
3. Enter the following information for this rule:
   - **Description**: Provide a description for this rule, for example "Allow Call Center Server Traffic".
   - **Enabled**: Verify this box is checked.
   - **Log**: Check this box to enable logging for this rule.
4. In the **Take the following action** field, select **Priority Allow**.
5. In the **When Applications in any of the following selected classes** field, verify **<All Applications>** (default entry) is selected.

6. In the **But not in the following class** field, verify **<none>** (default entry) is selected.
7. In the **Attempt to act as a** field, select **server**.
8. In the **for network services** field, enter **TCP/0-65535**.
9. In the **Communicating with** field, select **specific** from the drop-down menu (specific hosts).
10. In the **having addresses** field, enter the IP addresses for the machines that you want to allow to establish TCP connections with the server, for example, IP addresses for Unified Communications Manager, Unified Contact Center Enterprise (ICM) servers, and gateways).
11. In the field **Using these local interfaces**, select **<all>** (default entry).
12. In the field **Under the limit of** select, for example, **<10000>** network connections in **<1>** minutes. Enter numbers in these fields based on the expected number of connections. Verify that the numbers entered here do not prevent the server from operating normally. At a minimum, these values must be set to handle expected peak network connections.
13. Click **Save**.

Step 2 Using the CSA Management Center, create the second Connection Rate Limit rule to deny all network traffic when the machine is acting as a server (Deny Rule). This rule denies network traffic except the traffic allowed by the Priority Allow rule created above.

To create the second rule:

1. Add a new rule to the rule module by clicking **Add**.
2. Select the *Connection Rate Limit* rule. The configuration for this rule opens.
3. Enter the following information for this rule:
   - **Description**: Provide a description for this rule, for example "Deny Server Traffic".
   - **Enabled**: Verify this box is checked.
   - **Log**: Check this box to enable logging for this rule.
4. In the **Take the following action** field, select **Deny**.
5. In the **When Applications in any of the following selected classes** field, verify **<All Applications>** (default entry) is selected.
6. In the **But not in the following class** field, verify **<none>** (default entry) is selected.
7. In the **Attempt to act as a** field, select **server**.
8. In the **for network services** field, enter **TCP/0-65535**.

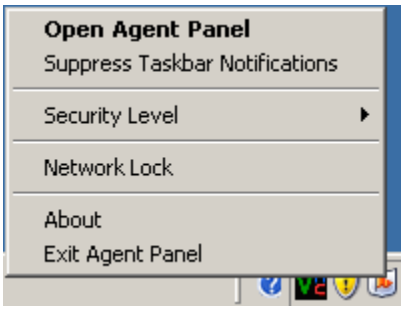
9. In the **Communicating with** field, select **specific** from the drop-down menu (specific hosts).
10. In the **having addresses** field, select **<all>**.
11. In the field **Using these local interfaces**, select **<all>** (default entry).
12. In the field **Over the limit of** select, for example, **<1>** network connections in **<1>** minutes. This will block all network traffic coming into this server.
13. Click **Save**.

Obtaining Additional Information about CSA

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

Step 1 In the Windows system tray, right-click the **Cisco Security Agent icon** (the white shield with the red flag) and choose **Open Agent Panel**.

Figure 1: Open Agent Panel



Step 2 Click **Help**.

The Cisco Security Agent documentation provides detailed information on using the Cisco Security Agent options such as Reset and other functions found in the Agent Panel.

Note: refer to the **Cisco Security Agent documentation** (http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html).

Important: Using Your Own CSA Management Center