



Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal, Release 4.1(1)

November 2007

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.**

Contents

This document contains information about the following topics:

- Introduction, page 2
- System Requirements, page 3
- Before You Begin the Installation, page 4
- Installing the Cisco Security Agent, page 5
- Checking the Version on the Server, page 6
- Disabling and Reenabling the Cisco Security Agent Service, page 7
- Uninstalling the Cisco Security Agent, page 8
- Upgrading the Cisco Security Agent, page 8
- Messages, Logs, and Caching, page 8
- Troubleshooting, page 10
- Migrating to the Management Center for Cisco Security Agents, page 11
- Obtaining Additional Information about CSA, page 13
- Obtaining Related Unified CVP Software Documentation, page 14
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 14



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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

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

The Agent is provided free of charge by Cisco Systems for use with Unified CVP software. The Agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested set of security rules (policy). The Agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed. A policy controls access to system resources based on:

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

This occurs transparently and does not hinder overall system performance.



Caution

You should not view Cisco Security Agent for Unified CVP as providing complete security for Unified CVP servers. Rather, view Cisco Security Agent as an additional line of defense that, when used correctly with other standard defenses such as virus-scanning software and firewalls, provides enhanced security. Cisco Security Agent for 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/ipsecurity>. A specific document to examine is *IP Telephony Security Operations Guide to Best Practices* at

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

The policy for the CSA standalone Agent for Unified CVP is created from the default policy modules that are shipped with Cisco Security Agent 5.2. These default policy modules secure/harden the Windows operating system and Apache. These default policy modules are altered in order to allow Unified CVP, including qualified third-party applications, to run smoothly.

Also in the interests of security, do not use network shares.

The standalone Cisco Security Agent for Unified CVP uses a static policy that cannot be changed.

However, see the section Migrating to the Management Center for Cisco Security Agents, page 11, for additional information.

Follow the installation instructions in this document to install the standalone Cisco Security Agent on all Unified CVP software servers, including Call Server, Operations Console, and VXML Server.

For servers running Cisco Unified ICME, see *Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

For servers running Cisco Unified Communications Manager (Unified CM), see *Installing Cisco Security Agent for Unified Communications Manager*.

For servers running Cisco Unified IP IVR, see *Installing Cisco Security Agent for Cisco Customer Response Solutions*.



Note

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 Release 4.1(1)*. **No other third-party applications are officially supported.** Third-party applications that can be installed through the Unified CVP installer (such as Apache Tomcat) must be so installed, other third-party applications (such as IBM WebSphere and Microsoft Internet Explorer) must be installed into the default directories presented during their installation process—otherwise your applications will not work properly. See the discussion in the section Installation Directories, page 3.

Note CSA for Unified CVP is not for Cisco Unified Call Studio.

Unified CVP can be collocated on the ICM VRU PG, but only one policy can be installed. The Unified CVP policy supports both products.

*Note that 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.

If you use a third-party software application that is not Cisco-approved, see the section Migrating to the Management Center for Cisco Security Agents, page 11, for additional information.



Note

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 which incorporate path information. Application actions may be blocked if the application is not installed in the correct directory. For this reason, it is mandatory that applications be installed through the Unified CVP installer (where this is possible) or, where this is not possible, be installed to the default directories provided by the application installers.



Caution

You **must always** use the **default directories** when installing **any 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.

System Requirements

- Unified CVP 4.1(1) (see the *Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software Release 4.1(1)*)
- Disk Space 20 MB
- Typical CPU Load (under normal circumstances): less than 5%

Before You Begin the Installation



Note

In Unified CVP 4.1(1), a newer standalone version of CSA for Unified CVP, based on the CSA engine version 5.2 is available. This means that the CSA agent kits and policies that worked with Unified CVP 4.0(1) will **NOT** work with Unified CVP 4.1(1). Hence, you must uninstall CSA 4.5 prior to upgrading to Unified CVP 4.1(1). New CSA agent kits and policies are available for download on cisco.com.

If you are upgrading from Unified CVP 4.0(2), the upgrade process to CSA 5.2 will have already been performed during the Unified CVP 4.0(2) upgrade process.

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 20 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 disable the Cisco Security Agent service. You must also be sure that the service does not get enabled at any time during the Unified CVP installation. For information on how to disable the service, see the section *Disabling and Reenabling the Cisco Security Agent Service*, page 7.



Caution

You must disable the Cisco Security Agent service before performing **any** software installation. 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, since the Cisco Security Agent may block part of the installation if not disabled.

After installing or upgrading the software, you must reenabling the Cisco Security Agent Service. With the service disabled, the Agent no longer provides intrusion detection for the server.

Note, however, that virus scan engine and .dat file updates, both manual and automatic, are supported—though the user may be queried to allow them.

- 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). pcAnywhere and Virtual Network Computing (VNC) are supported for remotely installing or upgrading 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 should be done immediately after installation (you will be prompted), because although the Cisco Security Agent protects the server as soon as you install the software, it does not provide complete functionality until the server is rebooted. In particular, the following limitations exist if the system is **not** rebooted:
 - Network Shield rules are not applied.
 - Network access control rules only apply to new socket connects (though stopping and restarting network server service will provide full network access control security, even without a system reboot).

- Data access control rules are not applied (though stopping and restarting the web server service will apply data access control security, even without a system reboot).

**Caution**

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

- After the installation, you do not need to perform any Agent configuration tasks. The software immediately begins to work as designed. Security events may display in the Messages window of the Agent GUI (double-click the Cisco Security Agent icon—the red flag in the Windows system tray; then click on Message, on the left, under Status), as well as in Microsoft Event Viewer and/or in the securitylog.txt file (see Event Messages and Log Files, page 9).

**Tip**

If you encounter problems with installing or uninstalling the Cisco Security Agent, see the sections Messages, Logs, and Caching, page 8 and Troubleshooting, page 10.

Installing the Cisco Security Agent

**Caution**

Before you upgrade or reinstall the Agent, you must uninstall the Agent. You cannot install one version of the Agent on top of a previously installed version. See the sections Uninstalling the Cisco Security Agent, page 8, and Upgrading the Cisco Security Agent, page 8.

**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 the section Migrating to the Management Center for Cisco Security Agents, page 11.

**Note**

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

Review the section Before You Begin the Installation, page 4, which provides information to help ensure a successful installation. To install the Cisco Security Agent for CVP software, complete the following steps:

- Step 1** From the server, browse to http://www.cisco.com/kobayashi/sw-center/contact_center/csa/
- Step 2** From the page that displays, click [CSA for CVP](#).
- Step 3** Download the latest version of the Cisco Security Agent file: **CiscoCVP-CSA-<version>-K9.exe**.

For example, CiscoCVP-CSA-5.2.0.203-2.2.1-W-K9.exe, where 5.2.0.203 indicates the engine version and 2.2.1 indicates the policy version).

**Note**

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 at this point be directed to a web form. Fill out the form and click **Submit**. A message appears telling you when you can expect to have download access. If you have already registered, continue with Step 4.

- Step 4** Note the location where you saved the downloaded file(s).
- Step 5** Double-click **CiscoCVP-CSA-<version>-K9.exe** to begin the installation; the Welcome window displays.
- Step 6** Click **Next**. The license agreement displays.
- Step 7** Click **Yes**.
- Step 8** Accept the default destination where the software installs, then click **Next**.
- Step 9** The “Preparing to transfer files” 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 the radio button **Yes** (the default), then click **Finish** to reboot the server.

**Caution**

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

**Tip**

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

- Step 12** Perform this procedure on each Unified CVP software server. [As noted, Cisco Security Agent for Unified CVP should **not** be installed on SDDSN, Media Server, and Call Studio machines.]

Checking the Version on the Server

You can check the engine and policy versions of the Agent. To do so, double-click on the CSA flag in the system tray. Included in the Status section of the Cisco Security Agent window is the Product ID, which will look something like: Unified CVP CSA 5.2.0.203 Policy 2.2.1

In this case, 5.2.0.203 is the engine version and 2.2.1 is the policy version.

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

Disabling and Reenabling the Cisco Security Agent Service

You must disable the CSA service whenever you want to install, upgrade, or uninstall software. This means before every operating system, 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 reenabling the Cisco Security Agent Service. With the service disabled, the Agent no longer provides intrusion detection for the server.



Note

You must have Admin rights in order to successfully disable or reenabling the Cisco Security Agent.

Disable

To disable the CSA service, complete 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**.
 - Step 5** At this point you are challenged by CSA. Click the Yes radio button; click **Apply**; enter the displayed letters in the Challenge field; click **OK**.

At this point, CSA is stopped. This is indicated by a white target with a red bull's-eye being displayed on top of the red flag that is the CSA icon.
 - Step 6** From the **Startup Type** drop-down list box, choose **Disabled**.
 - Step 7** Click **OK**.



Caution

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

- Step 8** Close Services.



Caution

You must reenabling the Cisco Security Agent service after installing, upgrading, or uninstalling software.

Reenable

To reenabling the CSA service, 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 Services.

Uninstalling the Cisco Security Agent



Caution

You cannot install one version of the Agent on top of a previously installed version. You must uninstall the Agent and then reinstall the software. When you start the uninstaller, a prompt from the Agent asks whether you want to uninstall the Agent. You have limited time (five minutes) to click **Yes** to disable the protection. If you choose **No** or wait to disable the protection, the security mode automatically enables.



Note

An important feature of the Management Center for Cisco Security Agents is that it has a scheduled update program that automatically updates the Agents that are being managed. This eliminates the need to manually uninstall, install, and start CSA on each server. See the section Migrating to the Management Center for Cisco Security Agents, page 11.

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



Caution

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

Upgrading the Cisco Security Agent

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

1. Uninstall the existing version that is installed on the server.
See the section Uninstalling the Cisco Security Agent, page 8.
2. Install the new version that you plan to run on the server.
See the section Installing the Cisco Security Agent, page 5.

Messages, Logs, and Caching

This section discusses additional features of the Cisco Security Agent.

Event Messages and Log Files

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

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

- The log files are located in <InstallDrive>:\Program Files\Cisco\CSAgent\log.
 - securitylog.txt—this is the main event log; this is where rule violations and other relevant events are logged
 - csalog.txt—this provides Agent startup and shutdown history (it contains events as well; but securitylog.txt also contains the events, and is easier to read)
 - driver_install.log—this provide a record of the driver installation process
 - CSAgent-Install.log—this provides a detailed record of the installation process
- You can view securitylog.txt using Notepad. The field names are given in the first line. This can be done by:
 - Double-clicking the Cisco Security Agent icon—the red flag in the Windows system tray.
 - Then click on Messages (on the left, under Status).
 - Then click **View log**. (Clicking on **Purge log** deletes all events stored in securitylog.txt, though csalog.txt will continue to contain that information.)

You can also:

- Copy securitylog.txt to a machine that has Excel and change the name to securitylog.csv.
- Double-click securitylog.csv and it will open as an Excel spreadsheet.

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

For diagnosing problems, the most important fields are DateTime, Severity, Text, and User. Ignore the RawEvent field; it contains essentially the same information that is presented in the other fields, but in 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 users are queried, the Agent can remember the response permanently or temporarily. This way, if the same rule is triggered again, the action is allowed, denied, or terminated based on what answer was given previously with no popup query box appearing again either permanently or for some period of time.

For example, if a user is queried as to whether an application can talk on the network and the user responds by selecting the **Yes** radio button and clicking a **Don't ask again** checkbox, the Yes response is remembered permanently and that response appears in the edit field in the User Query Response window (double-click on the flag icon, then click on User Query Response, on the left, under Status).

But if the user is queried as to whether setup.exe can install software on the system and the user responds by selecting the **Yes** radio button, but there is no **Don't ask again** checkbox or it is there but the user does not select it, this response is remembered temporarily and it does not appear in the User Query Response window.

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



Note

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

Troubleshooting

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

Problems with Installing/Uninstalling the Agent

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

- Verify that you rebooted the server.
- Verify that the Cisco Security Agent service is not disabled and that its Startup Type value is Automatic.
- Obtain the installation logs from <InstallDrive>:\Program Files\Cisco\CSAgent\log. Review the CSAgent-Install.log and driver_install.log files.
- Verify that you did not use Terminal Services.

Problems with Unified CVP Software or Errors from Cisco Security Agent

Go through the procedure in this section if you encounter problems after installing Cisco Security Agent for Unified CVP software:

- 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, please refer to the section What to Do before Contacting TAC about a CSA Problem, page 11.

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

-
- Step 1** Disable CSA as described in Disable, page 7.

- Step 2** Perform the operation that caused the error message.
- Step 3** Reenable CSA as described in Reenable, page 7.
- 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 CVP software components or third-party applications included in the *Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software Release 4.1(1)*.
- Step 6** If you are unable to resolve the problem, see What to Do before Contacting TAC about a CSA Problem, page 11.

What to Do before Contacting TAC about a CSA Problem

First go through all the relevant procedures described above to determine if there is really a problem and if it is in fact a CSA problem.

If you feel that it is a CSA problem, and you want to open a TAC case, follow the procedures below:

-
- Step 1** Run the Cisco Security Agent Diagnostics program:
Start > Programs > Cisco Security Agent > Cisco Security Agent Diagnostics
This causes the agent to gather self-describing diagnostic information on the system and on the agent itself (for example, information pertaining to any configured system states). Be patient, because it may take some time to collect this data.
The diagnostic utility temporarily disables agent security while it executes. If you are queried to disable agent security, you should respond **Yes**, to allow the diagnostics program to run. Security is automatically reenabled when the utility finishes collecting data.
 - Step 2** When the collection is complete, a message appears informing you that a csa-diagnostics.zip file has been created in the <InstallDrive>\Program Files\Cisco Systems\CSAgent\log directory.
 - Step 3** Determine the version of your CSA engine and of your CSA policy (the method for doing so is described in Checking the Version on the Server, page 6).
 - Step 4** Contact TAC. Be prepared to provide them with the zipped file mentioned in Step 2 and the information you collected in Step 3.

Migrating to the Management Center for Cisco Security Agents

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

Also, 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 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 with running your software, before calling your Unified CVP support provider, you must first:

1. Remove any third-party software not supported by Cisco from your Unified CVP servers.
 2. 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.

If you are interested in the Management Center, you should obtain the latest version of the following Management Center for Cisco Security Agent documents:

- *Installing Management Center for Cisco Security Agents 5.2*
- *Using Management Center for Cisco Security Agents 5.2*
- *Release Notes for Management Center for Cisco Security Agents 5.2*

You can download these documents at:

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

Ensure that the Management Center component is installed on a separate, dedicated server and the managed Agent is installed on all 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 5.2*.

**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 instructions in *Installing Management Center for Cisco Security Agents 5.2* for Installing Management Center for Cisco Security Agent, perform the following procedure 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 the Cisco Security Agent, page 8.
 - 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-5.2.0.203-2.2.1.export). You can obtain the policy from http://www.cisco.com/kobayashi/sw-center/contact_center/csa/



Note On accessing this site, see the discussion in the section *Installing the Cisco Security Agent*, page 5.

Note the location where you saved the downloaded file. Note also that, for identification purposes, all Unified CVP policies are prepended with the “word” **CVP**.



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

So, 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 *Using Management Center for Cisco Security Agents 5.2* (“Exporting and Importing Configurations”) for importing the policy that you downloaded in Step 1.
- Step 4** Use the “Quick Start Configuration” section of *Installing Management Center for Cisco Security Agents 5.2* 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 5.2*.

Obtaining Additional Information about CSA

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

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

Step 2 Click the **Help** button.

The Cisco Security Agent documentation displays.



Tip To obtain the Cisco Security Agent 5.2 documentation, go to:
<http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html>

Obtaining Related Unified CVP Software Documentation

The latest version of the Unified CVP software documentation can be found at this URL:

http://cisco.com/en/US/products/sw/custcosw/ps1006/tsd_products_support_series_home.html

The *Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software Release 4.1(1)* can be found at this URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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 UCB's 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.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0708R)