Release Notes for Cisco Security Agent for Cisco Unity, Release 2.0(3)

Published March 6, 2006

These release notes provide download, installation, and upgrade instructions, information on new and changed support, and caveats for Cisco Security Agent for Cisco Unity, Release 2.0(3).

Cisco Security Agent for Cisco Unity is supported for use with Cisco Unity and with Cisco Unity Connection.

Cisco Security Agent for Cisco Unity software is available on the Cisco Unity Crypto Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d.

Contents

These release notes contain the following sections:

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

Introduction

Cisco Security Agent for Cisco Unity is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with Cisco Unity and Cisco Unity Connection installations that meet the requirements specified in the "Requirements and Supported Software" section on page 2.

The standalone Cisco Security Agent provides:

- Intrusion detection and prevention for Cisco Unity and Cisco Unity Connection software.
- Defense against previously unknown attacks because it does not require signatures, as antivirus software does.
- Reduced downtime, attack propagation, and cleanup costs.

The agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested set of security rules known as a policy. The policy allows or denies specific system actions before system resources are accessed, based on the following criteria:

- The resources being accessed.
- The operation being invoked.
- The process invoking the action.

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

Version 2.0(3) of the standalone Cisco Security Agent for Cisco Unity is compiled with Cisco Security Agent version 4.5.1, build 639.

Caution Do not view Cisco Security Agent for Cisco Unity as providing complete security for Cisco Unity or Cisco Unity Connection installations. Instead, view it as an additional line of defense that, when used correctly with other standard defenses such as antivirus software and firewalls, provides enhanced security. Cisco Security Agent for Cisco Unity provides enhanced defense for many different Cisco Unity and Cisco Unity Connection installations and configurations, and therefore cannot enforce network access control rules, which block outbound or inbound network traffic, or act as a host-based firewall.

The best starting point for references to security and voice products is http://www.cisco.com/go/ipcsecurity. We recommend the *IP Telephony Security Operations Guide to Best Practices*.

In addition, refer to the *Cisco Unity Security Guide, Release 4.x*:

- The Domino version of the guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea53.html.
- The Exchange version of the guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea54.html.

Requirements and Supported Software

See the applicable section, depending on the product:

- Software Requirements—Cisco Unity, page 3

Software Requirements—Cisco Unity

- Cisco Unity version 4.0(1) or later running on the Cisco Unity server.
- Microsoft Windows Server 2003 in English, Windows 2000 Server in English, or Windows 2000 Advanced Server in English running on the Cisco Unity server. Other language versions are not supported.
- A qualified message store:
  - If the message store is installed on the Cisco Unity server, Microsoft Exchange 2000 or Exchange 5.5 for the message store.
  - If the message store is not installed on the Cisco Unity server, IBM Lotus Domino, Exchange 2003, Exchange 2000, or Exchange 5.5 for the message store.
- Cisco Security Agent for Cisco Unity can be installed on the message store server(s) and/or on the domain controller/global catalog server (DC/GC) only when Cisco Unity is installed in a Voice Messaging configuration.

  Do not install Cisco Security Agent for Cisco Unity on the message store server(s) or the DC/GC when Cisco Unity is installed in a Unified Messaging configuration.

Note If you install Cisco Security Agent for Cisco Unity on a server running Windows in Japanese, the display of some non-ASCII characters will be corrupted.

Supported Optional Software—Cisco Unity

Only the following optional software has been qualified for use on a Cisco Unity server that is running Cisco Security Agent for Cisco Unity:

- Adobe Acrobat Reader, version 4 and later.
- McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 and later.
- NetIQ AppManager for Cisco Voice Mail, version 6.0 and later. (Install only the agent on the Cisco Unity server.)
- Symantec
  - AntiVirus Corporate Edition, version 8.1 and later.
  - Norton AntiVirus for Microsoft Windows NT and Windows 2000, version 5.02 and later.
- Trend Micro
  - ScanMail for Microsoft Exchange 2000, version 5 and later.
  - ServerProtect for Microsoft Windows, version 5.5.

- VERITAS
  - Backup Exec for Microsoft Windows NT and Windows 2000, version 8.6.
  - NetBackup, version 4.5 and later.
- Windows Automatic Update. It must be configured not to automatically download updates to the Cisco Unity server.
- WinZip, version 7 and later.

The support policy for optional software on the Cisco Unity server is available in the applicable version of *Supported Hardware and Software, and Support Policies for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Software Requirements—Cisco Unity Connection

- Cisco Unity Connection version 1.1(1) or later when installed on a Cisco Unity Connection or voice-recognition server.

  To allow Cisco Security Agent for Cisco Unity to support a variety of deployments, the agent does not enforce network access control based on inbound ports and protocols. For Connection, the Windows Server 2003 firewall enforces network access control based on inbound ports and protocols. The firewall is configured with exceptions for Connection functionality during Connection Setup. To change the firewall configuration or to disable the firewall, use the Cisco Unity Connection Network Security wizard (NetworkSecurityWizard.exe) in the directory G:\Cisco Systems\Cisco Unity Connection\TechTools on the Connection server.
- Microsoft Windows Server 2003 Standard Edition in English running on the Cisco Unity Connection server. Other language versions are not supported.

Note If you install Cisco Security Agent for Cisco Unity on a server running Windows in Japanese, the display of some non-ASCII characters will be corrupted.

Supported Optional Software—Cisco Unity Connection

Only the following optional software has been qualified for use on a Cisco Unity Connection or voice-recognition server that is running Cisco Security Agent for Cisco Unity:

- Adobe Acrobat Reader, version 4 and later.
- Computer Associates eTrust Antivirus, version 7.0 and later
- McAfee VirusScan Enterprise 8.0i
- Symantec AntiVirus Corporate Edition, version 9.0 and later
- Trend Micro Server Protect for Microsoft Windows, version 5.56 and later
- Windows Automatic Update. It must be configured not to automatically download updates to the Cisco Unity server.
- WinZip, version 7 and later.

The support policy for optional software on the Cisco Unity Connection or Connection voice-recognition server is available in the applicable version of *Cisco Unity Connection System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Support Policy for Optional Software

Cisco support policy is that customers can deploy supported third-party software, including modified CSA policies, on the Cisco Unity, Cisco Unity Connection, or Connection voice-recognition server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with Cisco Unity or Cisco Unity Connection before the products are deployed, to mitigate the risk of problems being discovered within the production environment between Cisco Unity or Cisco Unity Connection and the third-party products loaded on the server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Cisco Unity, Cisco Unity Connection, or Connection voice-recognition server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and Cisco Unity or Cisco Unity Connection was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Cisco Unity, Cisco Unity Connection, or Connection voice-recognition server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Cisco Unity or Cisco Unity Connection system.

Before installing any qualified optional service pack on the Cisco Unity, Cisco Unity Connection, or Connection voice-recognition server, confirm that the manufacturer of any optional software or hardware that you plan to install on the server—or that is already installed—also supports the service pack for use with its product.

Determining the Software Version

The version of Cisco Security Agent for Cisco Unity and the version of the policy that the agent was created with are the same. Do the following procedure to determine the version for both the agent and the policy.

To Determine the Cisco Security Agent for Cisco Unity Version and Policy Version in Use

Step 1 Double-click the Cisco Security Agent taskbar icon.

Step 2 In the tree control on the left of the Cisco Security Agent Panel, click **Status**.

Step 3 The version number in the Product ID field applies both to Cisco Security Agent for Cisco Unity and to the policy that the agent was created with.

To Determine the Version of the Cisco Security Agent Engine

Right-click the Cisco Security Agent taskbar icon, and click **About**.

Related Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmap09186a00801179df.html.

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Cisco Unity Connection Documentation Guide*. The document is shipped with Cisco Unity Connection and is available at http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.

New and Changed Support—Release 2.0(3)

This section contains information about new and changed support in the Cisco Security Agent for Cisco Unity Release 2.0(3) time frame only. Refer to the release notes of the applicable version for information about new and changed support with earlier versions of Cisco Security Agent for Cisco Unity. Release notes for all versions of Cisco Security Agent for Cisco Unity are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

NetIQ AppManager for Cisco Voice Mail Version 6.0

Cisco Security Agent for Cisco Unity supports NetIQ AppManager for Cisco Voice Mail version 6.0. Install the AppManager agent on the Cisco Unity server.

Caution Install only the agent on the Cisco Unity server, or Cisco Unity will not function properly.

Installing AppManager on a Cisco Unity Connection server is not currently supported.

Installation and Upgrade Information

Downloading Cisco Security Agent for Cisco Unity 2.0(3)

See the applicable section, depending on the product:

Downloading Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation

To Download Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation

Step 1 Confirm that the computer you are using has up to 20 MB of hard-disk space for the download file and the installed files.

Step 2 On a computer with a high-speed Internet connection, go to the Cisco Unity Crypto Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d.

Note To access the software download page, you must be logged on to Cisco.com as a registered user.

Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unity, you need to fill out a brief questionnaire. Follow the on-screen prompts.

Step 3 Click **CiscoUnity-CSA-4.5.1.639-2.0.3-K9.exe**.

Step 4 Follow the on-screen prompts to complete the download.

Step 5 If you plan to install Cisco Security Agent for Cisco Unity from a compact disc, burn the CD.

Downloading Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Connection Installation

With Cisco Unity Connection, Cisco Security Agent for Cisco Unity is a part of the Cisco Unity Connection Server Updates wizard. Although you can download Cisco Security Agent for Cisco Unity separately, as described in the "Downloading Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation" section on page 7, we recommend that you download and run the latest Server Updates wizard to install Cisco Security Agent for Cisco Unity and the latest Microsoft updates recommended for use with Connection.

(For a list of Microsoft updates that are installed by the wizard, refer to *Software Installed by the Cisco Unity Connection Server Updates Wizard* at http://www.cisco.com/en/US/products/ps6509/prod_pre_installation_guide09186a008055e2d4.html.)

To Download the Cisco Unity Connection Server Updates Wizard

Step 1 On a computer with a high-speed Internet connection, go to the Cisco Unity Connection Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unityconnection.

Note To access the software download page, you must be logged on to Cisco.com as a registered user.

Step 2 Confirm that the computer you are using has sufficient hard disk space for the downloaded file and for the extracted wizard. You will need approximately two times the total of the download file size. (The download file sizes appear on the Cisco Unity Connection Software Download page.)

Step 3 Click the name of the Cisco Unity Connection Server Updates wizard file.

Step 4 Follow the on-screen prompts to complete the download.

Step 5 Extract the Cisco Unity Connection Server Updates wizard to the hard disk:

a. In Windows Explorer, double-click the file.

b. In WinZip, specify the directory to which the wizard will be extracted.

Step 6 Burn a CD for the wizard, and label it "Cisco Unity Connection Server Updates wizard <date>."

If you have a Cisco Unity Connection Server Updates wizard CD shipped from Cisco, set it aside so you do not accidentally use the wrong CD during installation.

Step 7 When you are done extracting the wizard, delete the downloaded .exe file to free disk space.

Installing Cisco Security Agent for Cisco Unity 2.0(3)

See the applicable section, depending on the product:

- Installing Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation, page 8
- Installing Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Connection Installation, page 9

Installing Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation

Note If you are upgrading Cisco Security Agent for Cisco Unity to version 2.0(3), see the "Upgrading to Cisco Security Agent for Cisco Unity 2.0(3)" section on page 10.

We recommend that you install Cisco Security Agent for Cisco Unity after regular business hours because the installation process will affect Cisco Unity performance. In addition, when the installation completes, you must restart the Cisco Unity server for Cisco Security Agent for Cisco Unity to start working.

Caution Do not install Cisco Security Agent for Cisco Unity by using Windows Terminal Services, or the installation will fail.

To Install Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Installation

Step 1 Log on to the server by using an account that is a member of the Administrators group or the Local Administrators group.

Step 2 Confirm that the server has at least 20 MB of hard-disk space available for the download file and the installed files.

Step 3 If another intrusion-detection application is installed on the server, uninstall the application before installing Cisco Security Agent for Cisco Unity. Refer to the applicable documentation.

Step 4 If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.

Step 5 If antivirus software is installed on the server, disable and stop the scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first virus-scanning service.

c. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

d. Click **Stop** to stop the service immediately.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Step 6 In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Unity file, and double-click **CiscoUnity-CSA-4.5.1.639-2.0.3-K9.exe**.

Step 7 Follow the on-screen prompts.

Caution Do not change any of the default values, or Cisco Security Agent for Cisco Unity may not function properly.

Step 8 When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.

Cisco Security Agent for Cisco Unity begins to work as soon as you restart the server. You do not need to configure the application.

Step 9 If antivirus software is installed on the server, re-enable and start the virus-scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first scanning service.

c. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

d. Click **Start** to start the service.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Installing Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Connection Installation

Note If you are upgrading Cisco Security Agent for Cisco Unity to version 2.0(3), see the "Upgrading to Cisco Security Agent for Cisco Unity 2.0(3)" section on page 10.

Run the Cisco Unity Connection Server Updates wizard on the Connection server and on the voice-recognition server, if any.

To Install Cisco Security Agent for Cisco Unity 2.0(3) for a Cisco Unity Connection Installation

Step 1 Log on to the server by using an account that is a member of the local Administrators group.

Step 2 If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.

Step 3 If antivirus software is installed on the server, disable and stop the scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first virus-scanning service.

c. On the General tab, click **Stop** to stop the service immediately.

d. In the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Step 4 Insert the Cisco Unity Connection Server Updates Wizard CD into the DVD drive.

Step 5 Browse to the root directory, and double-click **ServerUpdatesWizard.exe**.

Step 6 Follow the on-screen prompts to complete the installation of Cisco Security Agent for Cisco Unity and Microsoft updates.

Note If you are accessing the server by using Remote Desktop or a VNC client, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

Step 7 When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.

Cisco Security Agent for Cisco Unity begins to work as soon as you restart the server. You do not need to configure the application.

Step 8 If antivirus software is installed on the server, re-enable and start the scanning services:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click the name of the first virus-scanning service.

c. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

d. Click **Start** to start the service.

e. Click **OK** to close the Properties dialog box.

f. Repeat Step b through Step e for each of the remaining virus-scanning services.

g. When the services have been disabled, close the Services MMC.

Upgrading to Cisco Security Agent for Cisco Unity 2.0(3)

Use the task list in this section to upgrade to version 2.0(3) of the Cisco Security Agent for Cisco Unity. The tasks refer to sections in these release notes.

Upgrade Task List

1. Download the software. See the "Downloading Cisco Security Agent for Cisco Unity 2.0(3)" section on page 6.
2. Stop and disable the Cisco Security Agent service. See the procedure "To Stop and Disable the Cisco Security Agent Service" in the "Disabling and Re-enabling the Cisco Security Agent Service" section on page 11.
3. Uninstall the previous version. See the "Uninstalling Cisco Security Agent for Cisco Unity" section on page 12.

4. Install version 2.0(3). See the "Installing Cisco Security Agent for Cisco Unity 2.0(3)" section on page 8. When the installation is complete, the Cisco Security Agent service is enabled automatically.

Installation and Upgrade Notes

Disabling and Re-enabling the Cisco Security Agent Service

The Cisco Security Agent service must be stopped and disabled before you install or upgrade any software on a server on which Cisco Security Agent for Cisco Unity is installed.

(For information on other situations in which you must disable the Cisco Security Agent service, see the "Cisco Security Agent Service Must Be Disabled for Specific Tasks" section on page 12.)

This section contains two procedures:

- To Stop and Disable the Cisco Security Agent Service, page 11
- To Re-enable and Start the Cisco Security Agent Service, page 11

Caution When you stop and disable the Cisco Security Agent service, you must re-enable and start it before it can monitor the server again.

To Stop and Disable the Cisco Security Agent Service

Step 1 On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

Step 2 In the right pane, double-click **Cisco Security Agent**.

Step 3 On the General tab, click **Stop** to stop the service immediately.

Step 4 In the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 6 When the service has been disabled, close the Services MMC.

To Re-enable and Start the Cisco Security Agent Service

Step 1 On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

Step 2 In the right pane, double-click **Cisco Security Agent**.

Step 3 On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

Step 4 Click **Start** to start the service.

Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 6 When the service has been re-enabled, close the Services MMC.

Uninstalling Cisco Security Agent for Cisco Unity

To Uninstall Cisco Security Agent for Cisco Unity

Step 1 Stop the Cisco Security Agent service:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click **Cisco Security Agent**.

c. On the General tab, click **Stop** to stop the service immediately.

d. Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 2 On the Windows Start menu, click **Programs** > **Cisco Systems** > **Uninstall Cisco Security Agent**.

Step 3 Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unity.

Step 4 Click **Yes** again to restart the server.

Important Notes on Using Cisco Security Agent for Cisco Unity

The following sections contain information on using Cisco Security Agent for Cisco Unity:

Cisco Security Agent Service Must Be Disabled for Specific Tasks

The Cisco Security Agent service must be disabled and stopped in the following situations:

- For Cisco Unity only, before you use any tool in:
  - The CommServer\Utilities directory.
  - The CommServer\TechTools directory.
- For Cisco Unity Connection only, before you use any tool in:
  - The Cisco Unity Connection\Utilities directory.
  - The Cisco Unity Connection\TechTools directory.
- Before you use any tool that you download from the Cisco Unity Tools website.
- Before you install any software on a server on which Cisco Security Agent for Cisco Unity is installed.
- For Cisco Unity only, before you run the Configure Cisco Unity Failover wizard.

- Before you upgrade any software on a server on which Cisco Security Agent for Cisco Unity is installed. This also applies to automatic upgrades (for example, installing service packs by using group policy objects or custom scripts). Cisco Security Agent for Cisco Unity allows supported antivirus applications to automatically download and install upgrades to antivirus components.
- Before you add, change, or delete values in the Windows registry.
- Before you change Windows system or boot files.

Caution When you disable and stop the Cisco Security Agent service, you must re-enable and start it before it can monitor the server again.

For instructions on disabling and re-enabling the service, see the "Disabling and Re-enabling the Cisco Security Agent Service" section on page 11.

Locations in Which Cisco Security Agent Logs Events

Cisco Security Agent logs events in the following three locations:

Windows application event log	Events that are generated by Cisco Security Agent have an event source of CSAgent.
Securitylog.txt	Cisco Security Agent logs one event per line. The data in the file is in comma-separated-value format. In general, there should not be many entries in the file, so you should be able to read it in a text editor, for example, Notepad. (You might want to turn off word wrap.) If there are a lot of entries, you can view the data more easily if you copy the file to a computer on which a spreadsheet application is installed, change the file-name extension from .txt to .csv, and open the file in the spreadsheet application. To view the log, double-click the Cisco Security Agent taskbar icon. In the tree control on the left of the Cisco Security Agent Panel, click **Messages**. Then click **View Log**. (The log appears in the Program Files\Cisco Systems\CSAgent\Log directory.)
Current messages	To display events that have occurred since you logged on to Windows, double-click the Cisco Security Agent taskbar icon. In the Cisco Security Agent Panel, click **Messages**.

Custom SQL Server Backups Must Be Written to a SQLBackups Directory (Cisco Unity Only)

If you use custom scripts to trigger a backup of the SQL Server or MSDE database for Cisco Unity, and if you are backing up to a location other than the directory in which SQL Server or MSDE was installed, create a directory named SQLBackups and save backups to that directory. This will avoid problems caused by Cisco Security Agent restrictions on the SQL Server process.

The SQLBackups directory can be anywhere in the path, for example, D:\SQLBackups or G:\Backups\SQLBackups\UnityDBBackups.

Note Cisco Unity Connection does not support third-party backup software.

Web Browsing from the Cisco Unity, Cisco Unity Connection, or Connection Voice-Recognition Server

Caution Do not use the Cisco Unity, Cisco Unity Connection, or Connection voice-recognition server for web browsing, or you may inadvertently download malicious content. Some Cisco Security Agent protections for Internet Explorer were removed from Cisco Security Agent for Cisco Unity to allow the Cisco Unity Administrator and Cisco Unity Connection Administration to function properly.

Caveats

This section describes Severity 1, 2, and 3 caveats.

You can find the latest caveat information for Cisco Security Agent for Cisco Unity 2.0(3)—in addition to caveats of any severity for any release—by using Bug Toolkit, an online tool available for customers to query defects according to their own needs. Bug Toolkit is available at http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl.

Note To access Bug Toolkit, you must be logged on to Cisco.com as a registered user.

This section contains caveat information for Cisco Security Agent for Cisco Unity 2.0(3) only. Refer to the release notes of the applicable version for caveat information for earlier versions of Cisco Security Agent for Cisco Unity. Release notes for all versions of Cisco Security Agent for Cisco Unity are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Open Caveat—Release 2.0(3)

There are no open caveats for Cisco Security Agent for Cisco Unity Release 2.0(3).

Resolved Caveats—Release 2.0(3)

Click a link in the Caveat Number column to view the latest information on the caveat in Bug Toolkit. (Caveats are listed in order by severity, then by component, then by caveat number.)

Table 1 Cisco Security Agent for Cisco Unity Release 2.0(3) Resolved Caveats

Caveat Number	Component	Severity	Description
CSCsc56607	voicecsa	3	Unity Connection Disaster Recovery Tool (DiRT) fails with CSA enabled
CSCsc79687	voicecsa	3	New registry activity causes conflict with CSA

Troubleshooting Information

The following sections contain information on troubleshooting Cisco Security Agent for Cisco Unity:

Problems with Accessing the Cisco Personal Communications Assistant or Cisco Unity Inbox

When the Cisco Security Agent for Cisco Unity is installed on a subscriber workstation, a false-positive malicious-code detection dialog box may appear during initial logon to the Cisco Personal Communications Assistant (PCA) or initial use of the Cisco Unity Inbox. In addition, the Media Master control bar may be unavailable in the Cisco Unity Inbox or the Cisco Unity Assistant. The text that appears in the dialog box can vary, depending on the Cisco Security Agent for Cisco Unity policies in use, but it will always begin with “Cisco Security Agent: A problem was detected, press one of the actions below.”

Do the applicable steps in the following procedure if a Cisco Security Agent for Cisco Unity dialog box appears when a subscriber tries to log on to the Cisco PCA or to access the Cisco Unity Inbox.

To Resolve Cisco PCA or Cisco Unity Inbox Access Problems When Using Cisco Security Agent for Cisco Unity on a Subscriber Workstation

Step 1 In the Cisco Security Agent for Cisco Unity dialog box, click **Yes** or **Yes to All**, which acknowledges that software is being installed. The action is required to allow use of the Media Master control bar. No additional steps are required.

If the subscriber clicked No or No to All instead of Yes or Yes to All prior to reporting the problem, do Step 2 through Step 8.

Step 2 Log off of the Cisco PCA.

Step 3 In the Windows taskbar, double-click the **Cisco Security Agent** icon.

Step 4 In the tree control on the left of the Cisco Security Agent Panel, click **User Query Responses**.

Step 5 Click **Clear**.

Step 6 Click **OK** to close the Cisco Security Agent Panel.

Step 7 Log on to the Cisco PCA. If applicable, then access the Cisco Unity Inbox.

Step 8 If a Cisco Security Agent for Cisco Unity dialog box appears, click **Yes** or **Yes to All**. The Media Master control bar will appear.

Blue-Screen Condition (Cisco Unity Only)

Cisco Security Agent for Cisco Unity may cause a blue screen on a Cisco Unity 4.0(3) or earlier server running Windows 2000 Advanced Server and Cisco Unity-CM TSP version 7.0(3) or earlier (Cisco Unity caveat CSCed14125).

To prevent or fix the problem, install Cisco Unity version 4.0(4) or later and Cisco Unity-CM TSP version 7.0(4) or later.

MAPI Network Error (Cisco Unity Only)

The Cisco Unity system may experience network-type problems, including subscribers unable to access their mailboxes and a MAPI error in the event log indicating a network problem (Cisco Unity caveat CSCee13192). Such problems have been seen on heavily loaded Cisco Unity 4.0(4) and earlier systems with Cisco Security Agent for Cisco Unity installed, and running on four-processor servers with hyperthreading turned on. Once the symptoms start occurring, 5 percent to 10 percent of all calls are affected.

To prevent or fix the problem, either disable hyperthreading in the BIOS on the Cisco Unity server, or install Cisco Unity-CM TSP version 7.0(4b) or later and keep hyperthreading turned on.

Problems with Cisco Unity, Cisco Unity Connection, or Voice Recognition, or Errors from Cisco Security Agent

Do the procedure in this section if you encounter any of the following problems after installing Cisco Security Agent for Cisco Unity:

- Problems with Cisco Unity, Cisco Unity Connection, or voice recognition that cannot otherwise be explained.
- Cisco Security Agent errors in the Windows event log or in the Cisco Security Agent log file, <Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt.
- Cisco Security Agent error messages displayed on the screen.

If you cannot determine the cause of a Cisco Security Agent log entry or error message, contact Cisco TAC.

To Troubleshoot Problems with Cisco Unity, Cisco Unity Connection, or Voice Recognition, or Errors from Cisco Security Agent

Step 1 Stop the Cisco Security Agent service:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click **Cisco Security Agent**.

c. On the General tab, click **Stop** to stop the service immediately.

d. Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 2 Do the operation that caused the error message.

Step 3 Restart the Cisco Security Agent service:

a. On the Windows Start menu, click **Programs** > **Administrative Tools** > **Services**.

b. In the right pane, double-click **Cisco Security Agent**.

c. On the General tab, click **Start** to restart the service.

d. Click **OK** to close the Cisco Security Agent Properties dialog box.

Step 4 Do the operation that caused the error message.

Step 5 If the operation completes successfully with the Cisco Security Agent suspended and continues to fail with the Cisco Security Agent enabled, confirm that all of the software running on the Cisco Unity server is listed as supported in the "Requirements and Supported Software" section on page 2.

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

Step 6 If you are unable to resolve the problem, contact Cisco TAC and send them the Cisco Security Agent log file, <Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt.

Second Attempt to Install Software Fails Without a Warning

In the following case, an attempt to install software will fail without a warning:

1. You tried to install software without first stopping and disabling the Cisco Security Agent service.
2. Cisco Security Agent displayed the message

   "Cisco Security Agent: A problem was detected, press one of the action buttons below. Are you installing/uninstalling software? If not, this operation is suspicious."
3. You clicked **No**.
4. You stopped and disabled the Cisco Security Agent service.
5. You tried again to install the software, but nothing happened.

When you clicked No in Step 3., your answer was cached in memory. The cache is cleared automatically after an hour. To clear the cache immediately so you can install the software now, do the following procedure.

To Clear the Cisco Security Agent Memory Cache So You Can Install Software

Step 1 In the Windows taskbar, double-click the **Cisco Security Agent** icon.

Step 2 In the tree control on the left of the Cisco Security Agent Panel, click **User Query Responses**.

Step 3 Click **Clear**.

Step 4 Click **OK** to close the Cisco Security Agent Panel.

Step 5 Before you retry installing software on the server, stop and disable the Cisco Security Agent service. See the procedure "To Stop and Disable the Cisco Security Agent Service" section on page 11.

Step 6 After you install the software, re-enable and restart the Cisco Security Agent service. See the procedure "To Re-enable and Start the Cisco Security Agent Service" section on page 11.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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