



Release Notes for Cisco Security Agent for Cisco Unity, Release 3.1(6)

Published December 12, 2008

These release notes provide download, installation, and upgrade instructions, and caveats for Cisco Security Agent for Cisco Unity, Release 3.1(6).

Cisco Security Agent for Cisco Unity software is available from the Cisco Download Software website. (The location is provided in the download procedure later in these release notes.)

Contents

These release notes contain the following sections:

- [Introduction, page 1](#)
- [Requirements and Supported Software, page 2](#)
- [Related Documentation, page 7](#)
- [New and Changed Requirements and Support—Release 3.1\(6\), page 8](#)
- [New and Changed Functionality—Release 3.1\(6\), page 8](#)
- [Installation and Upgrade Information, page 8](#)
- [Important Notes on Using Cisco Security Agent for Cisco Unity, page 10](#)
- [Caveats, page 13](#)
- [Troubleshooting Information, page 14](#)
- [Obtaining Documentation and Submitting a Service Request, page 16](#)

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 the following products:

- Cisco Unity software



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

- Cisco Unity voice-recognition software
- Cisco Unity Connection version 1.x software
- Cisco Unity Connection version 1.x voice-recognition software
- Cisco Unity Bridge software

The standalone Cisco Security Agent provides the following benefits:

- Intrusion detection and prevention.
- 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 3.1(6) of the standalone Cisco Security Agent for Cisco Unity is compiled with Cisco Security Agent version 5.2.0, build 272.



Caution

Do not view Cisco Security Agent for Cisco Unity as providing complete security for the supported software. 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 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, see the applicable version of the *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Requirements and Supported Software

See the applicable section:

- [Requirements and Supported Software—Cisco Unity and Cisco Unity Voice-Recognition Servers, page 3](#)
- [Requirements and Supported Software—Cisco Unity Connection 1.x and Connection 1.x Voice-Recognition Servers, page 4](#)
- [Requirements and Supported Software—Cisco Unity Bridge Server, page 6](#)
- [Determining the Software Version, page 7](#)

Requirements and Supported Software—Cisco Unity and Cisco Unity Voice-Recognition Servers

See the applicable section:

- [Software Requirements—Cisco Unity Server, page 3](#)
- [Software Requirements—Cisco Unity Voice-Recognition Server, page 3](#)
- [Supported Optional Software—Cisco Unity and Cisco Unity Voice-Recognition Servers, page 4](#)

Software Requirements—Cisco Unity Server

- 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.



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.

- A qualified message store:
 - If the message store is installed on the Cisco Unity server, Microsoft Exchange 2003, 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, Microsoft Exchange 2007, Exchange 2003, Exchange 2000, or Exchange 5.5 for the message store.
- Cisco Security Agent for Cisco Unity can be installed on Exchange 2003 or Exchange 2000 server(s) and/or on the domain controller/global catalog server (DC/GC) only when the Cisco Unity server is installed in a Voice Messaging configuration.

Do not install Cisco Security Agent for Cisco Unity on the following servers:

- On the message store server(s) or the DC/GC when the Cisco Unity server is installed in a Unified Messaging configuration.
- On a Domino server.
- On a server running a 64-bit version of Windows.

Software Requirements—Cisco Unity Voice-Recognition Server

- Cisco Unity version 5.0(1) or later voice-recognition software running on the Cisco Unity voice-recognition server.
- Microsoft Windows Server 2003 in English running on the Cisco Unity voice-recognition 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 and Cisco Unity Voice-Recognition Servers

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

- Adobe Acrobat Reader, version 4 and later.
- CA Anti-Virus for the Enterprise version 8.0 and later (formerly called eTrust Antivirus)
- 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 and later.
- VERITAS
 - Backup Exec for Microsoft Windows NT and Windows 2000, version 8.6 and later.
 - 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 Cisco Unity and Cisco Unity voice-recognition servers 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.

If you want to use third-party software (including modified Cisco Security Agent policies) that is not supported for use with Cisco Security Agent for Cisco Unity, you can use a licensed version of Management Center for Cisco Security Agents to create, customize, deploy, and manage Cisco Security Agents that are compatible with the desired third-party software. For more information, see the “Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents” section on page 13.

Requirements and Supported Software—Cisco Unity Connection 1.x and Connection 1.x Voice-Recognition Servers

See the applicable section:

- [Software Requirements—Cisco Unity Connection 1.x and Connection 1.x Voice-Recognition Servers, page 5](#)
- [Supported Optional Software—Cisco Unity Connection 1.x and Connection 1.x Voice-Recognition Servers, page 5](#)

Software Requirements—Cisco Unity Connection 1.x and Connection 1.x Voice-Recognition Servers

- Cisco Unity Connection version 1.x when installed on a Cisco Unity Connection or Connection voice-recognition server.



Note For Cisco Unity Connection 2.x and later, Cisco Security Agent is part of the installation of the Linux operating system and Connection software, and cannot be installed or upgraded separately.

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 1.x and Connection 1.x Voice-Recognition Servers

Only the following optional software has been qualified for use on a Cisco Unity Connection 1.x or Connection 1.x voice-recognition server that is running Cisco Security Agent for Cisco Unity:

- Adobe Acrobat Reader, version 4 and later.
- CA eTrust Antivirus, version 7.0.
- McAfee VirusScan Enterprise 8.0i and later.
- 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 Cisco Unity Connection or Connection voice-recognition servers is available in *Cisco Unity Connection 1.x System Requirements, and Supported Hardware and Software* at

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/1x/requirements/1xsysrq.html.

If you want to use third-party software (including modified Cisco Security Agent policies) that is not supported for use with Cisco Security Agent for Cisco Unity, you can use a licensed version of Management Center for Cisco Security Agents to create, customize, deploy, and manage Cisco Security

Agents that are compatible with the desired third-party software. For more information, see the “Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents” section on page 13.

Requirements and Supported Software—Cisco Unity Bridge Server

See the applicable section:

- [Software Requirements—Cisco Unity Bridge Server, page 6](#)
- [Supported Optional Software—Cisco Unity Bridge Server, page 6](#)

Software Requirements—Cisco Unity Bridge Server

- Cisco Unity Bridge version 3.1(1) or later running on the Bridge server.
- Microsoft Windows Server 2003 or Windows 2000 Server in English running on the Bridge 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 Bridge Server

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

- McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 and later.
- 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 Bridge server

The support policy for optional software on the Cisco Unity Bridge server is available in *Cisco Unity Bridge 3.1 System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/requirements/31cubsysreq.html.

If you want to use third-party software (including modified Cisco Security Agent policies) that is not supported for use with Cisco Security Agent for Cisco Unity, you can use a licensed version of Management Center for Cisco Security Agents to create, customize, deploy, and manage Cisco Security Agents that are compatible with the desired third-party software. For more information, see the “Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents” section on page 13.

Determining the Software Version

The version of Cisco Security Agent for Cisco Unity and the version of the policy with which the agent was created 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 to both Cisco Security Agent for Cisco Unity and to the policy with which the agent was created.
-

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 *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity software and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.
- For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Cisco Unity Connection software and is available at http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.
- For Cisco Unity Bridge documentation on Cisco.com, see http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- For information on Cisco Security Agent version 5.2.0, build 272, with which Cisco Security Agent for Cisco Unity version 3.1(6) was compiled, see the readme file http://www.cisco.com/web/software/280775020/23291/CSA_5.2.0.272_readme.txt.



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

New and Changed Requirements and Support—Release 3.1(6)

There are no new or changed requirements or support in this release; see the “[Resolved Caveats—Release 3.1\(6\)](#)” section on page 13. Refer to the release notes of the applicable version for information about new and changed requirements and 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.

New and Changed Functionality—Release 3.1(6)

There is no new or changed functionality in this release; see the “[Resolved Caveats—Release 3.1\(6\)](#)” section on page 13. Refer to the release notes of the applicable version for information about new and changed functionality in 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.

Installation and Upgrade Information

- [Downloading Cisco Security Agent for Cisco Unity 3.1\(6\)](#), page 8
- [Installing Cisco Security Agent for Cisco Unity 3.1\(6\)](#), page 9
- [Upgrading to Cisco Security Agent for Cisco Unity 3.1\(6\)](#), page 10
- [Uninstalling Cisco Security Agent for Cisco Unity](#), page 10

Downloading Cisco Security Agent for Cisco Unity 3.1(6)

Cisco Security Agent for Cisco Unity is available on Cisco.com in the following downloads:

- As a standalone download, as documented in this section. The .export file used by Management Center for Cisco Security Agents is also available in this location; see the “[Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents](#)” section on page 13.
- As an optional component in the Cisco Unity Server Updates wizard, along with the latest recommended Microsoft updates. Shortly after a new version of the agent is released, it is added to the Server Updates wizard. To determine whether the latest version of the agent is available in the Server Updates wizard, refer to *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/updates/wizard/cuupwz.html.

To Download the Cisco Security Agent for Cisco Unity Installation Application

- Step 1** On a computer with a high-speed Internet connection, go to the Cisco Unified Communications Applications Downloads page at <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240>.



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

- Step 2** Expand **Unified Communications Applications > Voice Mail and Unified Messaging > Cisco Unity**, and click **Cisco Security Agent for Cisco Unity**.
- Step 3** Under Latest Releases, click the link for the latest version, and confirm that the computer you are using has sufficient hard-disk space for the downloaded file.
- Step 4** Follow the on-screen prompts to complete the download. Make note of the MD5 value.
- Step 5** For the downloaded file, use a checksum generator to confirm that the MD5 checksum matches the checksum that is listed on Cisco.com. If the values do not match, the downloaded file is damaged.



Caution Do not attempt to use a damaged file to install software or the results will be unpredictable. If the MD5 values do not match, download the file again until the value for the downloaded file matches the value listed on Cisco.com.

Free checksum tools are available on the Internet, for example, the Microsoft File Checksum Integrity Verifier utility. This utility is described in Microsoft Knowledge Base article 841290, *Availability and Description of the File Checksum Integrity Verifier Utility*. The article also includes a link for downloading the utility.

- Step 6** Copy the downloaded installation application to a removable storage device or to a network location that is accessible from the Cisco Unity server.

Installing Cisco Security Agent for Cisco Unity 3.1(6)



- Note**
- If you are upgrading Cisco Security Agent for Cisco Unity to version 3.1(6), see the “[Upgrading to Cisco Security Agent for Cisco Unity 3.1\(6\)](#)” section on page 10 instead.
 - If you downloaded the Server Updates wizard, install the Cisco Security Agent for Cisco Unity software by using the procedure in *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/updates/wizard/cuupwz.html instead.

We recommend that you install Cisco Security Agent for Cisco Unity after regular business hours because the installation process will affect system performance. In addition, when the installation completes, you must restart the 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 3.1(6)

- 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** Browse to the location where you saved the downloaded Cisco Security Agent for Cisco Unity installation application, and run the application.

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



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 installation.

Step 5 When the installation completes, follow the on-screen prompts to restart the computer.

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

Upgrading to Cisco Security Agent for Cisco Unity 3.1(6)

Do the following tasks in the order listed to upgrade to Cisco Security Agent for Cisco Unity version 3.1(6). The tasks refer to sections in these release notes.

1. Download the software. See the [“Downloading Cisco Security Agent for Cisco Unity 3.1\(6\)”](#) section on page 8.
2. Uninstall the previous version. See the [“Uninstalling Cisco Security Agent for Cisco Unity”](#) section on page 10.
3. Install version 3.1(6). See the [“Installing Cisco Security Agent for Cisco Unity 3.1\(6\)”](#) section on page 9. When the installation is complete, the Cisco Security Agent service is enabled automatically.

Uninstalling Cisco Security Agent for Cisco Unity

To Uninstall Cisco Security Agent for Cisco Unity

Step 1 On the Windows Start menu, click **Programs > Cisco Security Agent > Uninstall Cisco Security Agent**.

Step 2 Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unity.

Step 3 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](#), page 11
- [Custom SQL Server Backups Must Be Written to a SQLBackups Directory \(Cisco Unity Only\)](#), page 12

- [Locations in Which Cisco Security Agent Logs Events](#), page 12
- [Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents](#), page 13
- [Web Browsing from a Server on Which Cisco Security Agent for Cisco Unity Is Installed](#), page 13

Cisco Security Agent Service Must Be Disabled for Specific Tasks

Stop and disable the Cisco Security Agent service in the following situations, or Cisco Security Agent for Cisco Unity may interrupt or block selected actions:

- 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.

The following two procedures provide instructions for disabling and re-enabling the service.

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.

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.

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	<p>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.</p> <p>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.)</p>
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 .

Managing Security Policies for Cisco Security Agent for Cisco Unity by Using Management Center for Cisco Security Agents

To add, delete, or view policies included in Cisco Security Agent for Cisco Unity, run Management Center for Cisco Security Agents, and import the file CiscoUnity-CSA-5.2.0.272-3.1.6.export. The file is available in the same location as Cisco Security Agent for Cisco Unity. For download instructions, see the “[Downloading Cisco Security Agent for Cisco Unity 3.1\(6\)](#)” section on page 8.

For more information on Management Center for Cisco Security Agents, refer to the Cisco Security Agent page on Cisco.com at <http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>.

Web Browsing from a Server on Which Cisco Security Agent for Cisco Unity Is Installed



Caution

Do not use a server on which Cisco Security Agent for Cisco Unity is installed 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 any Severity 1, 2, 3, and 4 caveats in this release.

You can find the latest caveat information for Cisco Security Agent for Cisco Unity 3.1(6)—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/go/bugs>.



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 3.1(6) 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 Caveats—Release 3.1(6)

There are no open caveats for Cisco Security Agent for Cisco Unity Release 3.1(6).

Resolved Caveats—Release 3.1(6)

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.)



Note

Table 1 lists only the resolved caveats that are specific to Cisco Security Agent for Cisco Unity. For a separate list of caveats that were resolved in Cisco Security Agent version 5.2.0, build 272, with which Cisco Security Agent for Cisco Unity version 3.1(6) was compiled, see the readme file at http://www.cisco.com/web/software/280775020/23291/CSA_5.2.0.272_readme.txt.

Table 1 Cisco Security Agent for Cisco Unity Release 3.1(6) Resolved Caveats

Caveat Number	Severity	Component	Description
CSCsr47291	4	voicecsa	CSA 5.2 causes SNMP and RSKdataservice to crash
CSCsm33672	4	voicecsa	CSA - Uninstalling enables Windows Firewall

Troubleshooting Information

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

- [Blue-Screen Condition \(Cisco Unity Only\), page 14](#)
- [MAPI Network Error \(Cisco Unity Only\), page 14](#)
- [Unexplained Problems, or Errors from Cisco Security Agent, page 15](#)
- [Second Attempt to Install Software Fails Without a Warning, page 16](#)

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.

Unexplained Problems, 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 applications 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 Unexplained Problems, 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 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, send diagnostic information to Cisco TAC:
- a. On the Windows Start menu, click **Programs > Cisco Security Agent > Cisco Security Agent Diagnostics**.
Cisco Security Agent Diagnostics gathers diagnostic information on Windows configuration and on Cisco Security Agent for Cisco Unity. Gathering this data may take a while. The resulting csa-diagnostics.zip file is saved in the system temp directory.
 - b. Contact Cisco TAC and send them the csa-diagnostics.zip file.
-

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 12.
-

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0809R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

