



Release Notes for Cisco Security Agent for Cisco Unified MeetingPlace Release 6.0(7)

Published April 3, 2008

These release notes provide download, installation, and upgrade instructions, and information on new and changed requirements, support and functionality, and caveats for Cisco Security Agent for Cisco Unified MeetingPlace Release 6.0(7).

Cisco Security Agent for Cisco Unified MeetingPlace is supported for use with the following Cisco Unified MeetingPlace components:

- Cisco Unified MeetingPlace Web Conferencing
- Cisco Unified MeetingPlace Gateway Systems Integrity Manager
- Cisco Unified MeetingPlace H.323/SIP Gateway
- Cisco Unified MeetingPlace Directory Services
- Cisco Unified MeetingPlace SMTP E-Mail Gateway
- Cisco Unified MeetingPlace for Lotus Notes
- Cisco Unified MeetingPlace for Office Communicator
- Cisco Unified MeetingPlace for Outlook
- Cisco Unified MeetingPlace Video Integration

Cisco Security Agent for Cisco Unified MeetingPlace software is available on the Cisco Unified MeetingPlace Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/meetingplace-3d>.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [Requirements and Supported Software, page 2](#)
- [Related Documentation, page 3](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Installation and Upgrade Information, page 4](#)
- [Important Notes on Using Cisco Security Agent for Cisco Unified MeetingPlace, page 7](#)
- [Caveats, page 8](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 9](#)

Introduction

Cisco Security Agent for Cisco Unified MeetingPlace is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with Cisco Unified MeetingPlace 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 Unified MeetingPlace 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 Microsoft 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 6.0(7) of the standalone Cisco Security Agent for Cisco Unified MeetingPlace is compiled with Cisco Security Agent version 5.0.0, build 205.



Caution

Do not view Cisco Security Agent for Cisco Unified MeetingPlace as providing complete security for Cisco Unified MeetingPlace 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 Unified MeetingPlace provides enhanced defense for many different Cisco Unified MeetingPlace 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*.

Requirements and Supported Software

See the applicable section, depending on the product:

- [Software Requirements, page 3](#)
- [Determining the Software Version, page 3](#)

Software Requirements

- One or more of the following supported software versions:

Cisco Unified MeetingPlace Directory Services	5.4(104)
Cisco Unified MeetingPlace for Lotus Notes	6.0(15.0)
Cisco Unified MeetingPlace for Office Communicator	6.0(11.0)
Cisco Unified MeetingPlace for Outlook	6.0(14.0)
Cisco Unified MeetingPlace H.323/SIP Gateway	5.3(1.8)
Cisco Unified MeetingPlace SMTP E-Mail Gateway	5.4(108)
Cisco Unified MeetingPlace Video Integration	5.4(107.0)
Cisco Unified MeetingPlace Web Conferencing	6.0(171.0)

- Microsoft Windows Server 2003 in English. Other language versions are not supported.

Determining the Software Version

The version of Cisco Security Agent for Cisco Unified MeetingPlace 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 Unified MeetingPlace 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 Unified MeetingPlace 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

The complete documentation set for Cisco Unified MeetingPlace Release 6.x is now available in wiki format at http://docwiki.cisco.com/index.php/Cisco_Unified_MeetingPlace,_Release_6.x. Cisco community members with CCO passwords can contribute expertise to articles and exchange ideas on the Discussion page associated with each article. For more information, click the **About DocWiki** link at the bottom of any page on the wiki.

For descriptions and URLs of traditional Cisco Unified MeetingPlace documentation on Cisco.com, refer to the *Documentation Guide for Cisco Unified MeetingPlace*. The document is shipped with Cisco Unified MeetingPlace and is available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_documentation_roadmaps_list.html.

Installation and Upgrade Information

- [Downloading Cisco Security Agent for Cisco Unified MeetingPlace 6.0\(7\)](#), page 4
- [Installing Cisco Security Agent for Cisco Unified MeetingPlace 6.0\(7\)](#), page 5
- [Installation and Upgrade Notes](#), page 6
- [Uninstalling Cisco Security Agent for Cisco Unified MeetingPlace](#), page 7

Downloading Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7)

**Note**

If Cisco Unified MeetingPlace Web Conferencing Release 6.0(171.0) is installed on the server, the Web Conferencing installer places a copy of the Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7) installation executable in the C:\Program Files\Cisco Systems\MPWeb directory. The file name is CiscoUnifiedMeetingPlaceCSA-K9.exe.

To Download Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7)

-
- 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 Unified MeetingPlace Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/meetingplace-3d>.

**Note**

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

- Step 3** Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unified MeetingPlace, you need to fill out a brief questionnaire. Follow the on-screen prompts.
- Step 4** Click **CiscoMeetingPlaceWebConfCSA607-K9.exe**.
- Step 5** Follow the on-screen prompts to complete the download.
- Step 6** If you plan to install Cisco Security Agent for Cisco Unified MeetingPlace from a compact disc, burn the CD.
-

Installing Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7)

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



Caution

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

To Install Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7)

- 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 Unified MeetingPlace. 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:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, double-click the name of the first virus-scanning service.
 - On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - Click **Stop** to stop the service immediately.
 - Click **OK** to close the Properties dialog box.
 - Repeat Step **b** through Step **e** for each of the remaining virus-scanning services.
 - When the services have been disabled, close the Services MMC.
- Step 6** If Cisco Unified MeetingPlace Web Conferencing is not installed on the server (for example, you are installing Cisco Security Agent for Cisco Unified MeetingPlace on a standalone H.323/SIP Gateway server), perform the following sub-steps to add a key to the registry to allow the installer to proceed:
- On the Windows Start menu, click **Run**. Enter **regedit** and click **OK**.
 - Expand the key HKEY_LOCAL_MACHINE\Software\Latitude.
 - On the Edit menu, click **New > Key**.
 - Name the new key **MeetingPlace WebPublisher**.
 - Click the new MeetingPlace WebPublisher key, then click **Edit > New > Key**.
 - Name the new key **General**.
 - Click the new General key, then click **Edit > New > String Value**.
 - Name the new string value **Version**.
 - Right-click **Version** and click **Modify**.
 - For Value Data, enter **6.0.0.0** and click **OK**.

- k. Close the registry editor.
- Step 7** In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Unified MeetingPlace file, and double-click **CiscoMeetingPlaceWebConfCSA607-K9.exe**.
- Step 8** Follow the on-screen prompts.
- Step 9** When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.
Cisco Security Agent for Cisco Unified MeetingPlace begins to work as soon as you restart the server. You do not need to configure the application.
- Step 10** 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.
-

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 Unified MeetingPlace 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 7.)

This section contains two procedures:

- [To Stop and Disable the Cisco Security Agent Service, page 6](#)
- [To Re-enable and Start the Cisco Security Agent Service, page 7](#)

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 Unified MeetingPlace

To Uninstall Cisco Security Agent for Cisco Security Agent for Cisco Unified MeetingPlace

- Step 1** Stop the Cisco Security Agent service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, double-click **Cisco Security Agent**.
 - On the General tab, click **Stop** to stop the service immediately.
 - 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 Unified MeetingPlace.
- Step 4** Click **Yes** again to restart the server.
-

Important Notes on Using Cisco Security Agent for Cisco Unified MeetingPlace

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

- [Cisco Security Agent Service Must Be Disabled for Specific Tasks, page 7](#)
- [Locations in Which Cisco Security Agent Logs Events, page 8](#)

Cisco Security Agent Service Must Be Disabled for Specific Tasks

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

- Before you install any software on a server on which Cisco Security Agent for Cisco Unified MeetingPlace is installed.
- Before you upgrade any software on a server on which Cisco Security Agent for Cisco Unified MeetingPlace 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 Unified MeetingPlace 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.

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 6.

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 .

Caveats

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

You can find the latest caveat information for Cisco Security Agent for Cisco Unified MeetingPlace 6.0(7)—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 Unified MeetingPlace 6.0(7) only. Release notes for all versions of Cisco Security Agent for Cisco Unified MeetingPlace are available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

Open Caveats—Release 6.0(7)

Click the 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 Unified MeetingPlace Release 6.0(7) Open Caveats

Caveat Number	Severity	Component	Description
CSCsj03819	2	csa	CSA denies client access to Home page on ports 80, 8080
CSCsj01008	2	csa-windows	CSA with Windows Integrated authentication produce 500 server error
CSCsj01017	2	csa-windows	CSA with WIA - database errors after services restart

Resolved Caveats—Release 6.0(7)

There are no resolved caveats for Cisco Security Agent for Cisco Unified MeetingPlace Release 6.0(7).

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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.