Custom Search:

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 below. This information is for Cisco Security Agent for Cisco Unified MeetingPlace Release 6.1.

Contents

Introduction

Cisco Security Agent for Cisco Unified MeetingPlace is supported for use with certain Cisco Unified MeetingPlace components. (See the list at Requirements and Supported Software.)

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.

Note that the version 6.1.8.1 of the standalone Cisco Security Agent for Cisco Unified MeetingPlace which you will download from the link provided below (see Downloading Cisco Security Agent for Cisco Unified MeetingPlace 6.1) is compiled with Cisco Security Agent version 5.2.0, build 263. What that means is that the internal build number Cisco Security Agent uses and shows when you open its Help/About section is: V5.2.0.263.

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

- Microsoft Windows Server 2003 in English. Other language versions are not supported.
- One or more of the following supported software versions:

Cisco Unified MeetingPlace Directory Services	6.1.1.0
Cisco Unified MeetingPlace for Lotus Notes	6.1.7.0
Cisco Unified MeetingPlace for Office Communicator	6.1.1.0
Cisco Unified MeetingPlace for Outlook	6.1.16.0
Cisco Unified MeetingPlace H.323/SIP Gateway	6.0.5.10
Cisco Unified MeetingPlace SMTP E-Mail Gateway	6.1.1.0
Cisco Unified MeetingPlace Video Integration	6.0.5.6
Cisco Unified MeetingPlace Web Conferencing	6.1.8.1

Installation and Upgrade Information

Downloading Cisco Security Agent for Cisco Unified MeetingPlace 6.1

Note: If Cisco Unified MeetingPlace Web Conferencing Release 6.1 is installed on the server, the Web Conferencing installer places a copy of the Cisco Security Agent for Cisco Unified MeetingPlace 6.1 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 6.1

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.
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/cisco/software/release.html?mdfid=281164943&release=6.1%288.1%29&relind=AVAILA
   Note: To access the software download page, you must be logged on to Cisco.com as a registered user.
3. Because of export controls on strong encryption, before you download Cisco Security Agent for Cisco Unified MeetingPlace you need to accept the Cisco EULA. Follow the on-screen prompts.
4. Click **CiscoUnifiedMeetingPlaceCSA-K9-6181.exe** to get additional information on the download.
5. Click the download button and follow the on-screen prompts to complete the download.
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 6.1

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.

Note Install Cisco Security Agent for Cisco Unified MeetingPlace *after* you have installed other software on the server.

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 6.1

1. Log on to the server by using an account that is a member of the Administrators group or the Local Administrators group.
2. Confirm that the server has at least 20 MB of hard-disk space available for the download file and the installed files.
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.
4. If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.
5. If antivirus software is installed on the server, disable and stop the scanning services:
    1. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
    2. In the right pane, double-click the name of the first virus-scanning service.
    3. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
    4. Click **Stop** to stop the service immediately.
    5. Click **OK** to close the Properties dialog box.
    6. Repeat Step 2 through Step 5 for each of the remaining virus-scanning services.
    7. When the services have been disabled, close the Services MMC.
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:
    1. On the Windows Start menu, click **Run**. Enter **regedit** and click **OK**.
    2. Expand the key HKEY_LOCAL_MACHINE\Software\Latitude.
    3. On the Edit menu, click **New > Key**.
    4. Name the new key **MeetingPlace WebPublisher**.
    5. Click the new MeetingPlace WebPublisher key, then click **Edit > New > Key**.
    6. Name the new key **General**.
    7. Click the new General key, then click **Edit > New > String Value**.
    8. Name the new string value **Version**.
    9. Right-click **Version** and click **Modify**.
    10. For Value Data, enter **6.0.0.0** and click **OK**.
    11. Close the registry editor.
7. In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Unified MeetingPlace file, and double-click **CiscoUnifiedMeetingPlaceCSA-K9-6181.exe**.
8. Follow the on-screen prompts.
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.

1. If antivirus software is installed on the server, re-enable and start the virus-scanning services:
    1. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
    2. In the right pane, double-click the name of the first scanning service.
    3. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
    4. Click **Start** to start the service.
    5. Click **OK** to close the Properties dialog box.
    6. Repeat Step b through Step e for each of the remaining virus-scanning services.
    7. 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.)

This section contains two procedures:

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

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

1. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
2. In the right pane, double-click **Cisco Security Agent**.
3. On the General tab, click **Stop** to stop the service immediately.
4. In the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
5. Click **OK** to close the Cisco Security Agent Properties dialog box.
6. When the service has been disabled, close the Services MMC.

To Re-enable and Start the Cisco Security Agent Service

1. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
2. In the right pane, double-click **Cisco Security Agent**.
3. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
4. Click **Start** to start the service.
5. Click **OK** to close the Cisco Security Agent Properties dialog box.
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

1. Stop the Cisco Security Agent service:
    1. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
    2. In the right pane, double-click **Cisco Security Agent**.
    3. On the General tab, click **Stop** to stop the service immediately.
    4. Click **OK** to close the Cisco Security Agent Properties dialog box.
2. On the Windows Start menu, click **Programs > Cisco Systems > Uninstall Cisco Security Agent**.
3. Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unified MeetingPlace.
4. Click **Yes** again to restart the server.
5. After the server has restarted, logon as the Administrator.
6. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
7. From the Services Control Panel (MMC), verify that the Windows Firewall service is stopped and Disabled

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

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.

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**.