



APPENDIX **B**

Cisco Security Agent: Standalone Agent Overview

This appendix describes the standalone version of Cisco Security Agent that is sometimes installed on a Security Manager server.



Note

- General user documentation for Cisco Security Agent is on Cisco.com at: <http://www.cisco.com/en/US/products/sw/secursw/index.html>. However, the standalone agent on your server is customized for Security Manager. Because you *cannot* configure the customized, standalone agent and because Management Center for Cisco Security Agents is *not* installed, some information in the documentation for Management Center for Cisco Security Agents does not apply.
- To understand and work around problems that you might have with the standalone agent, see [Troubleshooting the Standalone Security Agent, page A-12](#).

This appendix contains the following major sections:

- [The Basics, page B-1](#)
- [Understanding and Managing Security Level Settings, page B-2](#)
- [Responding to Query Challenges, page B-2](#)
- [Uninstalling the Standalone Agent, page B-3](#)

The Basics

If your target server is not protected by the full, commercial version of Cisco Security Agent when you start to install Security Manager, Security Manager installs a customized, standalone version of Cisco Security Agent, with predefined policies that you cannot change. See [Cisco Security Agent, page 1-5](#).

Once installed, the standalone agent controls system operations with policies that allow or deny specific system actions. The agent checks whether an action is allowed or denied before any system resources are accessed and acted upon. The agent never interferes with your daily operations unless it detects what it considers to be a forbidden or unexpected system operation. Nonetheless, its rules are meant to protect your server from rootkits or similarly malicious software and are therefore very strict.

The standalone agent combines Security Manager-specific policies with baseline policies for Windows. To learn about the baseline policies for Windows, log in to your Cisco.com account, then go to <http://www.cisco.com/cgi-bin/Software/Tablebuild/dofstp.pl?ftpfile=cisco/crypto/3DES/cw2000/csa/fcs-csamc-4.5.1.616-CSA-Policy-Descriptions.zip&app=Tablebuild&status=showC2A>.

**Note**

If you think that Cisco Security Agent has blocked a valid operation, you can contact Cisco TAC. See [Obtaining Documentation and Submitting a Service Request](#), page xiv.

Agent Log Files

Three log files for the standalone agent are stored in the C:\Program Files\Cisco Systems\CSAgent\log subdirectory:

CSAgent-Install.log	installation log file
csalog.txt	general log file
securitylog.txt	security events log file

Understanding and Managing Security Level Settings

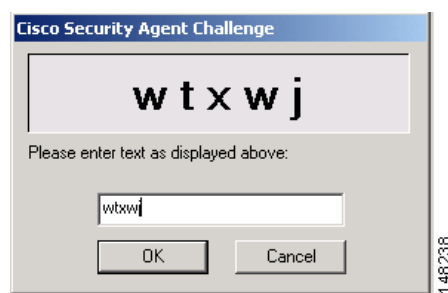
You can right-click the agent icon in the server system tray to change the security level setting at any time. The security level setting determines whether the agent imposes *high*, *medium*, or *low*-security restrictions on your server, or if it imposes no restrictions. The default is *medium*. Every level that you might select provides a distinct balance between security and convenience.

If you set the agent security level to *high*, it prevents your server from accepting inbound connections on any UDP or TCP ports except the specific ports that Security Manager and Common Services use. In addition, if the level is *high* and if the agent detects an untrusted rootkit, all connections (inbound and outbound) are blocked.

Responding to Query Challenges

When you right-click the agent icon and select **Security Level > Off** to disable your standalone agent, it displays a kind of challenge-response prompt ([Figure B-1](#)) that is commonly called a CAPTCHA (which stands for “Completely Automated Public Turing Test to Tell Computers and Humans Apart”).

Figure B-1 Challenge-Response Prompt



This method confirms that malicious software is not responsible for the request to disable your agent. To learn more, see [Using Management Center for Cisco Security Agents 5.2](#).

Uninstalling the Standalone Agent



Caution

You can uninstall the standalone agent, which removes all restrictions that the agent imposes, but your server will be significantly more vulnerable and exposed to attack than it is when the agent is installed. We recommend that you do *not* uninstall Cisco Security Agent.

As a temporary alternative, you can right-click the agent icon in your server system tray, then select a lower security level setting or select the option that temporarily disables the standalone agent.

Another alternative is to reset the standalone agent, which clears its rootkit detection status. To reset the agent, select **Start > Programs > Cisco Systems > Cisco Security Agent > Reset Cisco Security Agent**.

To uninstall the standalone agent (even though we recommend that you do *not* uninstall it), select **Start > Programs > Cisco Security Agent > Uninstall Cisco Security Agent**.

You must reboot.

Related Topics

[Cleaning Up an Unclean Agent, page B-3](#)

Cleaning Up an Unclean Agent

You might find that while performing an upgrade to Security Manager, the Cisco Security Agent remains active, even after you attempt to uninstall it.

Typically, if you cannot uninstall Cisco Security Agent before installing Security Manager, do the following steps:

Stop CSA service. If service is stopped, follow the steps for a typical cleanup. If service is not stopped, follow the steps for an atypical cleanup.

Typical Cleanup

- Step 1** Remove Cisco Security Agent from **Add/Remove** programs.
- Step 2** Delete the Cisco Security Agent from **Start > All Programs**.
- Step 3** Manually remove the CSAgent folder from C:\Program Files\Cisco Systems.
- Step 4** Search the registry and delete all entries for the strings “CSAgent” and “Cisco Security Agent.” To access the registry, select **Start > Run**. Enter **regedit** in the Open field, then click **Open**.
- Step 5** Reboot the machine.

If you try to remove the CSagent from Add/Remove Programs, and an error states the CSagent cannot be removed, you should first delete the CSagent entries in regedit before removing Cisco Security Agent from Add/Remove programs. See [Atypical Cleanup, page B-4](#).

Atypical Cleanup

-
- Step 1** Search the registry and delete all entries for the strings “CSAgent” and “Cisco Security Agent.” To access the registry, select **Start > Run**. Enter **regedit** in the Open field, then click **Open**.
- Step 2** Delete the Cisco Security Agent from **Start > All Programs**.
- Step 3** Remove Cisco Security Agent from **Add/Remove** programs.
- Step 4** Manually remove the CSagent folder from C:\Program Files\Cisco Systems.
- Step 5** Reboot the machine.
-

Related Topics

[Manually Removing the CSagent Version 5.2, page B-4](#)

Manually Removing the CSagent Version 5.2

If you cannot uninstall the CSagent with Add/Remove programs, or if the Agent uninstall failed, do the following to remove the Agent manually:

-
- Step 1** Boot up in SAFEMODE with networking for Windows machines (usually F8).



Note If you are removing the agent from a system without IIS or Apache, go to [Step 4](#).

- Step 2** Run the following from a CMD shell in the `..\csagent\bin`
- **For IIS**
`csa_datafilter -u iis`
 - **For Apache 1.3**
`csa_datafilter -u apache13 <.conf file with full path name> <modules dir. path>`
 - **For Apache 2.0**
`csa_datafilter -u apache20 <.conf file with full path name> <modules dir. path>`

- Step 3** If the above scripts do not work, remove the filters manually as follows:

For Apache 1_3

- a. Go to where Apache is installed (normally Program Files\apache).
- b. Open `apache\conf\httpd.conf` using notepad.
- c. Search for "csafilter".
- d. Delete the the two lines that begin with:
`"loadmodule csafilter. . ."`
`"addmodule mod_csafilter . . ."`

- e. Go to `apache\modules` and delete the following:
`mod_csafilter*.so`

For Apache 2

Follow the steps noted for Apache 1_3, with the exception that no reference is made to "addmodule mod_csafilter. . ."

For IIS

- a. Right-click **My Computer**, then select **Manage**.
- b. Go to **Services and Applications**.
- c. Right-click **Internet Information Services**, then select **Properties**.
- d. Under Master Properties, select **www service**.
- e. Edit and click the **ISAPI Filters** tab.
- f. Highlight the csafilter, then select **Remove**.
- g. Click **OK**.

Step 4 Net stop CSAgent in case some CSA agent services were started.

Step 5 Make sure the CSA agent icon (red flag) does not appear at the lower right corner of your monitor.



Note If the Agent icon is shown, exit out, right-click the red flag, then click **Exit Agent Panel**.

Step 6 Delete the Program Files\Cisco (Systems)\CSAgent folder.

Step 7 Delete the following directory:

Program Files\InstallShield Installation Information\{DE49974667B9-11D4-97CE-0050DA10E5AE}

Step 8 Delete the following driver files, which, depending on your operating system, might be located at Windows (or WINNT)\system32\drivers\:

- csacentr.sys
- csafile.sys
- csanet.sys
- csareg.sys
- csatdi.sys

Step 9 Delete all references to csagent in the Start Menu\Programs directory.

Step 10 Delete WINDOWS\system32\csauser.dll, which, depending on your operating system, might be located at WINNT\system32\.



Note Do not delete the entire key; remove only CSAUSER.DLL. Any other DLLs that are referenced in the AppInit_DLLs registry key are required by other programs and deleting them can cause system instability.

If you cannot delete this file, you must modify the registry key that loads this DLL, then reboot before you can delete it. To do this:

- a. Open the registry editor by selecting **Start > Run > regedit**.
- b. Go to **HKLM > SOFTWARE > Microsoft > Windows NT > CurrentVersion > Windows**.
- c. Modify the AppInit_DLLs registry key and change the reference from csauer.dll to xyz.



Note It is possible that even after modifying the reference to xyz and rebooting the server, the csauer.dll file is still not deleted. If this occurs, continue to the next step.

- d. Reboot.



Note After removing csauer.dll from the AppInit_DLLs registry key, you must reboot before Windows allows you to delete the csauer.dll file.

Step 11 Delete WINNT or WINDOWS\system32\csafilter.dll, csa_uninstall.bat, csarule.dll (if they exist).

Step 12 Delete the reference to CSA in **Start > Programs > Startup**.

Step 13 Delete the following registry keys:

- HKLM > system > controlset001 > control > session manager > knowndlls > csauer.dll
- HKLM > system > controlset002 > control > session manager > knowndlls > csauer.dll
- HKLM > system > controlset003 > control > session manager > knowndlls > csauer.dll (WinNT)
- HKLM > System > Currentcontrolset > Services > csacenter, csafilter, csahook
- HKEY_Local_Machine > Software > Cisco > CSAgent
- HKEY_Local_Machine > Software > Cisco > CSAgentinstalled
- HKEY_Local_Machine > Software > Microsoft > windows > currentversion > uninstall > {DE499746-67B9-11D4-97CE-0050DA10E5AE}

Step 14 **W2K, WINXP, W2K3**

- a. Remove references to any CSA* resource in the Windows Device Manager. (Go to **Start > Control Panel > System > Hardware > Device Manager**.) Make sure you select "show hidden devices" (**View > Show hidden devices**) and expand the non-plug and play devices section.
- b. Right click on each csa* resource and uninstall it.



Note Do not reboot until all the "Cisco Security Agent*" resources are uninstalled.

- c. Reboot.



Note You must reboot for the changes to take effect.

Step 15 **For WINNT**

- a. Remove references to any "Cisco Security Agent*" resource in the Windows Device Manager.
- b. Right-click on each "Cisco Security Agent*" resource and uninstall it.



Note Do not reboot until all the "Cisco Security Agent*" resources are uninstalled.

- c. Reboot.



Note You must reboot for the changes to take effect.

- Step 16** Reboot the server and verify that all CSA resources are deleted in Windows Device Manager. (See [Step 14](#).)
- Step 17** Delete WINNT or WINDOWS\system32\csauser.dll after you reboot.
- Step 18** Search the registry and delete all entries for the strings "CSAgent" and "Cisco Security Agent." To access the registry, select **Start > Run**. Enter **regedit** in the Open field, then click **Open**.



Note Some entries cannot be deleted.

- Step 19** Verify that CSAgent is not listed in **Control Panel > Add/Remove Programs**.
-

■ **Cleaning Up an Unclean Agent**