APPENDIX B

Bundled Cisco Security Agent: Overview

Cisco Security Agent provides host-based intrusion prevention. Regarding Security Manager, there are two versions of Cisco Security Agent—external and bundled:

- External Cisco Security Agent—Cisco Security Agent that is not installed as part of the Cisco Security Manager installation.
- Bundled Cisco Security Agent—Cisco Security Agent that is installed as part of the Cisco Security Manager installation. Bundled Cisco Security Agent is sometimes referred to as a "customized, standalone agent" because it is customized for Security Manager and because Management Center for Cisco Security Agents is not installed; thus, it is standalone.

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

- General user documentation for Cisco Security Agent is on Cisco.com at: http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html. However, the bundled agent on your server is customized for Security Manager. Because you *cannot* configure the bundled 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 Bundled Cisco Security Agent, page A-15.

This appendix contains the following major sections:

The Basics

If your target server is not protected by external Cisco Security Agent when you start to install Security Manager, Security Manager under certain conditions installs bundled Cisco Security Agent, with predefined policies that you cannot change. See Cisco Security Agent, page 1-3.

Caution Cisco Security Manager may not work as expected if external Cisco Security Agent (Cisco Security Agent that is not installed as part of the Cisco Security Manager installation) is installed on the server machine.

After installation, bundled Cisco Security 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.

Bundled Cisco Security 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/doftp.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 xii.

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.

Uninstalling Bundled Cisco Security Agent

You can uninstall bundled Cisco Security Agent, in the process removing 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 do not recommend that you 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 bundled Cisco Security Agent, clearing its rootkit detection status. To reset the agent, select **Start > Programs > Cisco Systems > Cisco Security Agent > Reset Cisco Security Agent**.

To uninstall bundled Cisco Security Agent, select **Start > Programs > Cisco Security Agent > Uninstall Cisco Security Agent**. Uninstallation in this way requires a system restart.

Cleaning Up an Unclean Agent

You might find that while upgrading Security Manager, Cisco Security Agent remains active, even after you try to uninstall it.

If you cannot uninstall Cisco Security Agent, try to stop the Cisco Security Agent service:

- If you can stop the Cisco Security Agent service, follow the Procedure for Typical Cleanup, page B-3.
- If you can not stop the Cisco Security Agent service, follow the Procedure for Atypical Cleanup, page B-3.

Procedure for Typical Cleanup

If you cannot uninstall Cisco Security Agent, but you can stop the Cisco Security Agent service, follow these steps to uninstall Cisco Security Agent using a typical cleanup:

Step 1 Remove Cisco Security Agent from **Add/Remove** programs.

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 Procedure for Atypical Cleanup, page B-3.

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 Restart the server.

Procedure for Atypical Cleanup

If you cannot uninstall Cisco Security Agent, and you can not stop the Cisco Security Agent service, follow these steps to uninstall Cisco Security Agent using an a typical 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 Restart the server.

Manually Removing the CSAgent Version 5.2.0.282

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 pennant) does not appear in the system tray.

Note If the Agent icon is shown, exit, right-click the red pennant, 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, follow these steps:

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 csauser.dll to *xyz*.

Note It is possible that even after modifying the reference to *xyz* and rebooting the server, the csauser.dll file is still not deleted. If this occurs, skip the following substep and proceed with the next step.

d. Restart.

Note After removing csauser.dll from the AppInit_DLLs registry key, you must reboot before Windows allows you to delete the csauser.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 Cisco Security Agent in **Start > Programs > Startup**.

Step 13 Delete the following registry keys:

- HKLM > system > controlset001 > control > session manager > knowndlls > csauser.dll
- HKLM > system > controlset002 > control > session manager > knowndlls > csauser.dll

- HKLM > system > controlset003 > control > session manager > knowndlls > csauser.dll (WinNT)
- HKLM > System > Currentcontrolset > Services > csacenter, csafile, csanet, csareg, csaTDI, csagent, 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 Cisco Security Agent* 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 each Cisco Security Agent* resource and uninstall it.

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

c. Restart. You must restart 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 each "Cisco Security Agent*" resource and uninstall it.

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

c. Restart. You must restart 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**.

Some entries cannot be deleted.

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