



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/ps5057/tsd_products_support_series_home.html. However, the standalone agent on your server is customized for Security Manager. Because you can *not* 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-11](#).

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 xv.

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

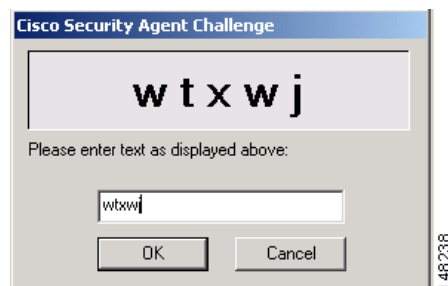
You can right-click the agent icon in the server system tray to change the security level setting at any time. The security level setting determines whether the agent imposes *high*, *medium*, or *low*-security restrictions on your server, or if it imposes no restrictions. The default is *medium*. Every 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 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.

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.

■ Uninstalling the Standalone Agent