APPENDIX **A**

Cisco Security Agent Installation and Overview

Overview

This chapter describes the Cisco Security Agent and provides information on the agent user interface. It also includes installation information for Windows, Linux, and Solaris agents. (This information, with additional details, also appears in a similarly titled Appendix A in the User Guide.)

Once the agent is installed, there is no configuration necessary on the part of the end user in order to run the agent software. Optionally, as the administrator, you can ask users to enter individualized contact information into the fields provided. If required, the agent user interface makes it easy for the user to enter this data and send it to CSA MC.

This section contains the following topics.

- Downloading and Installing, page A-2
- The Cisco Security Agent User Interface, page A-4
- Installing the Solaris Agent, page A-6
- Installing the Linux Agent, page A-8

Downloading and Installing

Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution. But you may also point users to a URL for the CSA MC system. This URL will allow them to see all kits that are available. That URL is:

```
https://<system name>/csamc51/kits
```

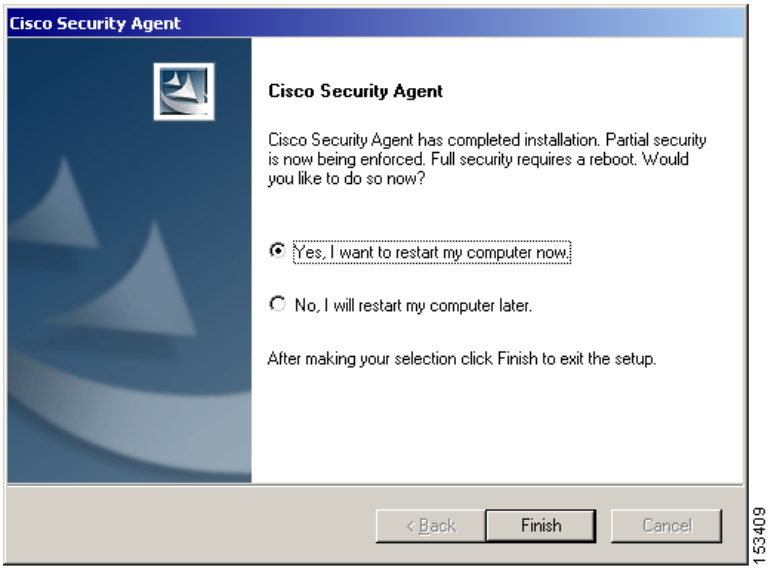
If you are pointing users to the “kits” URL and you have multiple agent kits listed here, be sure to tell users which kits to download.

Note Note that the Registration Control feature also applies to the <system name>/csamc51/kits URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering, it also prevents you from viewing the agent kits URL.

Note Cisco Security Agent systems must be able to communicate with the Management Center for Cisco Security Agents over HTTPS.

Once users install agents on their systems, they can optionally perform a reboot (if Force reboot is not selected). See Figure A-1. Whether a system is rebooted or not, the agent service starts immediately and the system is protected. (Note that Windows NT4 systems must be rebooted after an agent installation.)

Figure A-1 Optional Agent Reboot



If a system is not rebooted following the agent installation, the following functionality is not immediately available. (This functionality becomes available the next time the system is rebooted.)

Windows agents

- Network Shield rules are not applied until the system is rebooted.
- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Data access control rules are not applied until the web server service is restarted.

Solaris and Linux agents, when no reboot occurs after install, the following caveats exist

- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Buffer overflow protection is only enforced for new processes.
- File access control rules only apply to newly opened files.

- Data access control rules are not applied until the web server service is restarted.

After installation, the agent automatically and transparently registers with CSA MC. You can see which hosts have successfully registered by clicking the **Hosts** link available from the **Systems** category in the menu bar. This displays the hosts list view. All registered host system names appear here.

The Cisco Security Agent User Interface

Note The Cisco Security Agent user interface does not run on Solaris systems.

Note If the **Agent UI control rule** is not present (available on Windows and Linux only) for the system group, no agent UI appears on the end user system.

To open the Cisco Security Agent user interface on Windows and Linux systems, users can double-click on the flag icon in their system trays. The user interface opens on their desktop.

As the administrator, you decide which agent UI options to provide to the end user. These options are controlled by the Agent UI control rule. Available options are as follows:

- **Allow user to reset agent UI default settings**—Selecting this checkbox in the Agent UI control rule causes the end user to have a product reset option available from the Start>Programs>Cisco Security Agent menu. Selecting the "Reset Cisco Security Agent" option puts all agent settings back to their original states and clears almost all other user-configured settings. This does not clear configured Firewall Settings or File Protection settings. But if these features are enabled, they are disabled as this is the default factory setting. The information entered into the edit boxes for these features is not lost.
- **Allow user interaction**—Selecting this checkbox in the Agent UI control rule causes the end user to have a visible and accessible agent UI, including a red flag in the system tray.

- **Allow user access to agent configuration and contact information**—Selecting this checkbox in the Agent UI control rule provides Status, Messages, and Contact Information features, including the ability to manually poll the MC. It also provides the User Query Responses window.
- **Allow user to modify agent security settings**—Selecting this checkbox in the Agent UI control rule provides System Security and Untrusted Applications features.
- **Allow user to modify agent personal firewall settings**—Selecting this checkbox in the Agent UI control rule provides Local Firewall Settings and File Protection features.

The options available to the user in the agent UI depend upon the features selected in the Agent UI control rule governing the agent in question. All possible agent features are described in Appendix A of the User Guide.

Uninstall Windows Cisco Security Agent

To uninstall the Cisco Security Agent, do the following:

From the **Start** menu, go to **Programs>Cisco Security Agent>Uninstall Cisco Security Agent**. Reboot the system when the uninstall is finished.

Note You can also uninstall the agent from the Start>Settings>Control Panel>Add/Remove Programs dialog.

Installing the Solaris Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Solaris systems.

Note See the similarly titled Appendix A in the User Guide for information on a Solaris agent utility which allows you to manually poll to CSA MC and perform other tasks.

When you download the Cisco Security Agent kit from CSA MC, do the following to unpack and install it. (Note that you can put the downloaded tar file in any temp directory. Do not put it in the opt directory, for example, as you may then experience problems with the installation.)

Step 1 You must be super user on the system to install the agent package.

```
$ su
```

Step 2 Untar the agent kit.

```
# tar xf
CSA-Test_Mode_Server_V5.1.0.265-sol-setup-f734064be5a448b88e2a2786
7059113c.tar
```

Step 3 Install the agent package.(Use the command listed below when you install. This command forces the installation to use a package administration file to check the system for the required OS software agent dependencies. If the required dependencies are not present, such as the "SUNWlibCx" library, the install aborts.)

```
# pkgadd -a CSCOcsa/reloc/cfg/admin -d .

[Output:]
The following packages are available:
  1 CSCOcsa CSAagent
          (sun4u) 5.1.0.15
```

Step 4 Select the correct package or press enter to unpack all current packages.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
[Output:]
Processing package instance <CSCOcsa> from </space/user>
```

The install now displays the Cisco copyright and prompts you to continue the installation.

Step 5 Answer yes (y) to continue the installation.

```
This package contains scripts which will be executed with
super-user permission during the process of installing this
package.
Do you want to continue with the installation of <CSCOcsa>
[y,n,?] y
[Output:]
Installing CSAagent as <CSCOcsa>
```

The installation continues to copy and install files. When the install is complete, the following is displayed:

```
[Output:]
The agent installed cleanly, but has not yet been started.
The command:  /etc/init.d/ciscosec start
will start the agent.  The agent will also start
automatically upon reboot. A reboot is recommended to
ensure complete system protection.
The following packages are available:
  1 CSCOcsa CSAagent
       (sun4u) 5.1.0.15
```

Step 6 Quit (q) when installation is finished.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: q
```

Step 7 Optionally, reboot the system by entering the following.

```
# shutdown -y -i6 -g0
```

Caution If a system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)

The agent installs into the following directory:

```
/opt/CSCOcsa
```

Some files are put into additional directories such as `/kernel/strmod/sparcv9`, `usr/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.

Caution If you are upgrading the Solaris agent and you encounter the following error, "There is already an instance of the package and you cannot install due to administrator rules", you must edit the file `/var/sadm/install/admin/default`. Change `"instance=unique"` to `"instance=overwrite"` and then proceed with the upgrade.

Uninstall Solaris Agent

To uninstall the Cisco Security Agent, enter the following command:

```
# pkgrm CSCOcsa
```

Note If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless this rule is disabled. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC/VMS system are not changed to restrict this access.) See **Agent self protection** in the User Guide for details on this rule type.

A shipped UNIX policy allows secured management applications to stop the agent service. For example, after having logged in by selecting Command Line Login in the options menu of the login screen, all login applications are considered secure management applications. You can now run the `pkgrm` command to uninstall the agent.

Installing the Linux Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Linux systems.

When you download the Cisco Security Agent kit from CSA MC, do the following to unpack and install it.

Step 1 Move the tar file downloaded from CSA MC to a temporary directory, e.g.

```
$ mv
CSA-Server_V5.1.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar /tmp
```

Step 2 Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V5.1.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar
```

Step 3 cd to CSCOcsa directory where the rpm package is located.

```
$ cd /tmp/CSCOcsa
```

Step 4 Run script install_rpm.sh as root.

```
# sh ./install_rpm.sh
```

The package will be installed to `/opt/CSCOcsa`, with some files being put into directories such as `/lib/modules/CSCOcsa`, `/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.

Note CSAagent rpm packages are not relocatable.

Caution If a system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)

Note Linux Agent UI: For gnome desktop environments, the install script will only modify the default session config file for launching the agent UI automatically every time a user starts a gnome desktop session. But if a user already has their own session file (~/.gnome2/session), the default session file (/usr/share/gnome/default.session) will not be effective. Therefore, the agent UI will not automatically start when the user logs in. In such a case, the user must add the agent UI (/opt/CSCOcsa/bin/ciscosecui) manually (using "gnome-session-properties" utility) to make the agent UI auto-start.

Caution On Linux systems, if you upgrade the kernel version or boot a different kernel version than the initial version where the agent was installed, you must uninstall and reinstall the agent.

Uninstall Linux Agent

To uninstall the Cisco Security Agent, do the following.

Step 1 You must know the version number of the currently installed agent. Keep in mind that upgrades may have been installed since the first installation. When you know the version, run the following, using the correct version number.

```
# rpm -qf /opt/CSCOcsa/bin/ciscosecd
CSAagent-5.1-218
```

Step 2 Remove that rpm with rpm -ev, e.g.

```
# rpm -ev CSAagent-5.1-218
```

Caution If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless this rule is disabled. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC system are not changed to restrict this access.) See **Agent self protection** in the User Guide for details on this rule type.

You can uninstall the linux agent regardless of policies if you login using single user mode.