



# APPENDIX **A**

## Cisco Security Agent Overview

---

### Overview

This chapter describes the agent and provides information on the agent user interface. 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 provide end users with an advanced UI that allows them to control their security settings and to use other added features.

If you have configured Query User rules, users should know how to respond to query pop-up boxes. This information and additional advanced UI configuration information is included in the Help provided with the agent user interface. You may want to refer end users to this agent help.

This section contains the following topics.

- [Downloading and Installing, page A-2](#)
- [The Agent User Interface, page A-8](#)
- [Turn Agent Security Off, page A-20](#)
- [Installing Software Updates on Agents, page A-21](#)
- [Common Windows Cisco Security Agent Error Codes, page A-21](#)
- [Installing the Solaris Agent, page A-22](#)
- [UNIX Agent csactl Utility, page A-25](#)

- [Installing the Linux Agent, page A-27](#)

## 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 CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:

```
https://<system name>/csamc52/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.

End users must have administrator privileges on their systems to install the agent. Systems to which agents are installed must meet the following requirements:

Table A-1 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher <b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	<ul style="list-style-type: none"> <li>• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions)</li> <li>• Windows XP (Professional, Tablet PC, or Home Edition) with Service Pack 0, 1, or 2</li> <li>• Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4</li> <li>• Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a</li> <li>• All Windows, Internet Explorer 4.0 or higher required.</li> </ul> <b>Note</b> Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows XP and Windows 2000 (Terminal Services are not supported on Windows NT.)  Supported language versions are as follows: <ul style="list-style-type: none"> <li>• For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported.</li> <li>• For Windows NT, US English is the only supported language version.</li> </ul>
Memory	128 minimum—all supported Windows platforms

System Component	Requirement
Hard Drive Space	50 MB or higher <b>Note</b> This included program and data.
Network	Ethernet or Dial up <b>Note</b> Maximum of 64 IP addresses supported on a system.

**Note**

The Cisco Security Agent uses approximately 20 MB of memory. This applies to agents running on all supported Microsoft and UNIX platforms.

**Caution**

When upgrading or changing operating systems, uninstall the agent first. When the new operating system is in place, you can install a new agent kit. Because the agent installation examines the operating system at install time and copies components accordingly, existing agent components may not be compatible with operating system changes.

To run the Cisco Security Agent on your Solaris server systems, the requirements are as follows:

**Table A-2 Agent Requirements (Solaris)**

<b>System Component</b>	<b>Requirement</b>
Processor	UltraSPARC 400 MHz or higher  <b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	Solaris 9, 64 bit, patch version 111711-11 or higher, and 111712-11 or higher installed.  Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)  <b>Note</b> If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the pkgadd -d . SUNWlibCx command.
Memory	256 MB minimum
Hard Drive Space	50 MB or higher  <b>Note</b> This includes program and data.
Network	Ethernet  <b>Note</b> Maximum of 64 IP addresses supported on a system.

To run the Cisco Security Agent on your Linux systems, the requirements are as follows:

**Table A-3 Agent Requirements (Linux)**

System Component	Requirement
Processor	500 MHz or faster x86 processor <b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	RedHat Enterprise Linux 4.0 WS, ES, or AS RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	50 MB or higher <b>Note</b> This includes program and data.
Network	Ethernet <b>Note</b> Maximum of 64 IP addresses supported on a system.



**Note**

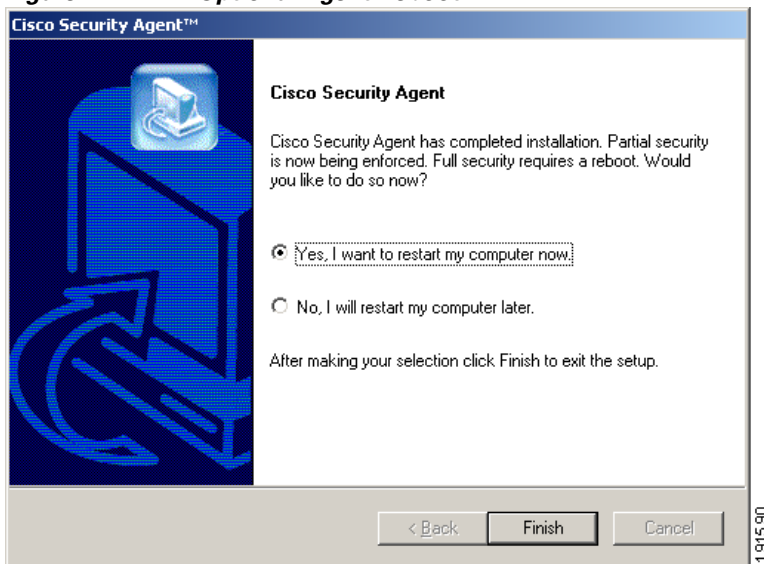
Agent systems must be able to communicate with CSA MC over HTTPS.



**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.

Once users install agents on their systems, they can optionally perform a reboot (if Automatic reboot is not selected at kit creation time). See [Figure A-1](#). Whether a system is rebooted or not, the agent service starts immediately and the system is protected.

**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.

At this time, 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. Agents are now ready to receive policies.

## The Agent User Interface



### Note

---

The Cisco Security Agent user interface does not run on Solaris systems. The Solaris agent has a utility (csactl) to provide some of the capabilities that the Windows and Linux agents provide in their user interface. See [UNIX Agent csactl Utility, page A-25](#) for details. The Cisco Security Agent user interface appearance and functionality is the same on all Windows and Linux platforms.

---

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. See [Agent UI Control, page 6-7](#). 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 when a reset occurs.
- **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. (If you select this checkbox, you are providing the end user with controls that you have limited access to. Firewall queries and other information will not log the CSA MC event log.)

To open the agent user interface, users can double-click on the agent icon in their system trays. The user interface opens on their desktop. The options available 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 here.

### Status

- The host name of the machine on which this agent is installed.
- The name of the CSA MC with which this agent is registered.
- The date and time the agent registered with CSA MC.
- The date and time when the agent last polled in to CSA MC (data is not downloaded each time the agent polls).
- The date and time the agent last downloaded data from CSA MC.
- Lets users know if there is a software version update available for their agent.
- If users have the Cisco Trust Agent installed and are using Network Admission Control, the Network Admission Control posture result for the agent is displayed on the UI. For example, it may display the status as Healthy, Quarantine, Infected, etc.
- When the end user clicks the **Poll** button, it forces the agent to poll the management center immediately rather than waiting for the configured time interval to trigger a poll. This way, the agent receives any rule changes right away.
- **Reset Cisco Security Agent**

This setting is available from the Start>Programs>Cisco Security Agent>Reset Cisco Security Agent menu on Windows systems and the System Menu>Cisco Security Agent menu on Linux systems where the agent is installed. 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

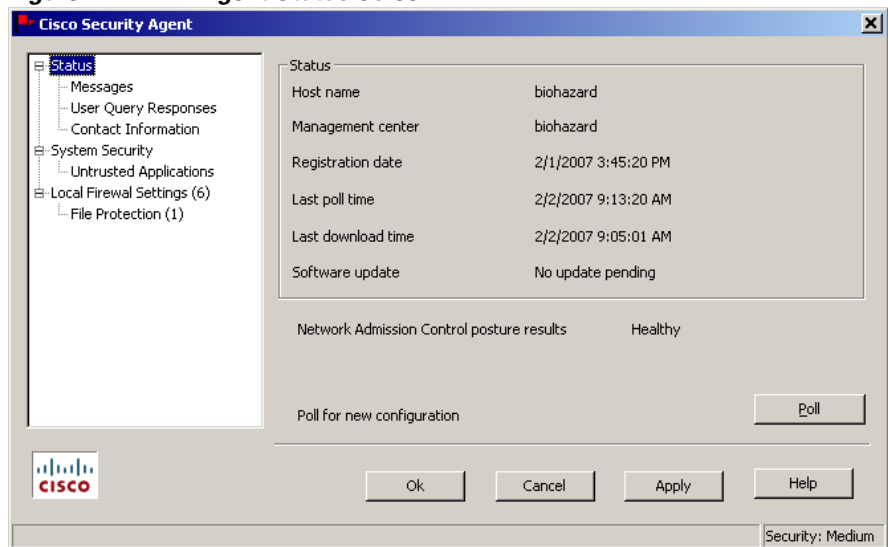
File Protection settings. But if these features are enabled, they are disabled as this is the default factory setting. The information entered into the edit boxes for these features is not lost.

- **Local Cisco Security Agent Diagnostics (collecting troubleshooting data)**

This utility is available from the Start>Programs>Cisco Security Agent>Cisco Security Agent Diagnostics menu on systems where the agent is installed. The end user can manually select "Cisco Security Agent Diagnostics" which causes the agent to gather self-describing diagnostic information on the system and on the agent itself (e.g. information pertaining to any configured system states). Since this same data can be collected remotely from the MC (see [Host Status, page 3-29](#)), you should only ask users to manually gather this data if for some reason remote diagnostics is not working. Note that it may take some time to collect this data.

When the collection is complete, a "csa-diagnostics.zip" file has been created. By default, this file is placed in the system temp directory. Users can then send this file to you.

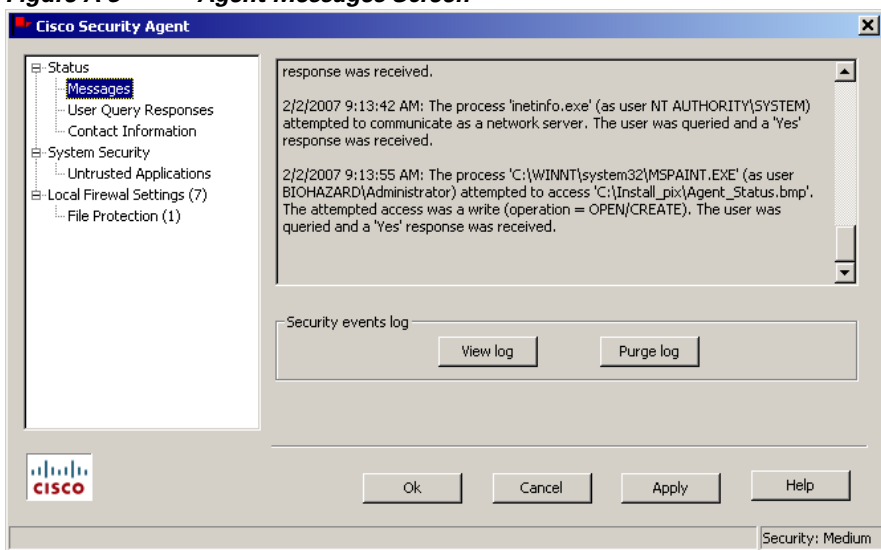
**Figure A-2 Agent Status Screen**



## Messages

When an agent denies a system action, a message informing the user of this event is placed in the Messages field. The user can click Messages in the left pane to view these events. Also note that the user can click the View log button to launch a text file containing all security events that have occurred on the system. This text file presents more detailed information on system events that have been logged by the agent. Click the Purge Log button to clear the text log file (if it begins to grow too large and takes up too much disk space). Note that the Purge Log file feature does not clear the messages viewable in the Messages field. It clears the log text file.

**Figure A-3 Agent Messages Screen**



### User Query Responses

When users respond to queries, the agent can remember their responses permanently or temporarily. This way, if the same query is triggered again, the action is allowed, denied, or terminated based on what was answered previously with no pop-up query box appearing again either permanently or for some period of time. In order to reduce the number queries users must respond to, it is generally advantageous, when possible, to permanently remember query responses.

It is the Don't ask again checkbox available from the Query Settings page in the MC that controls whether the end user has the ability to have a query response remembered permanently. As the administrator, you decide whether or not users have the option to choose Don't ask again. If user queries do not include a Don't ask again option and responses are only cached temporarily (for approximately an hour) users can click the Clear button in the agent Query User Responses window to delete all temporarily cached responses.

**Note**

---

For a Query setting, the response to the query is relevant to the question, not to the resource. For example, if a File access control rule queries the user for a response and that identical query is also configured for a Network access control rule, the user is not queried again when the Network access control rule triggers. (The query response from the previous File access control rule is automatically taken.)

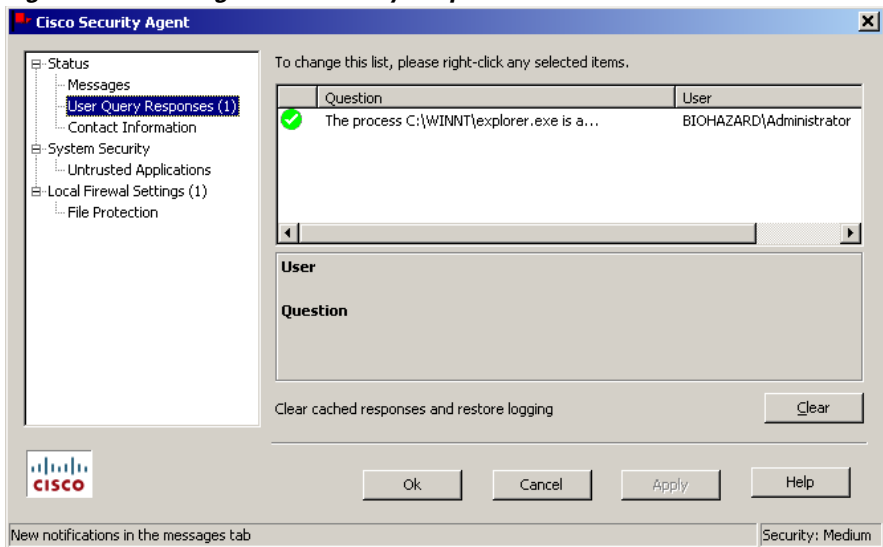
---

To clear permanent responses listed in the agent Query User Responses window edit field, users right-click on a selected response in the edit field and select **Remove**. Permanent responses are remembered across reboots. Temporarily cached responses are not remembered across reboots.

Note that query response is tied to the user who responded. On multi-user machines, multiple users may be asked the same question.

Note that users can sort Query User Responses in the edit field by right-clicking within in the edit field and selecting one of many **Sort** options.

**Figure A-4 Agent User Query Responses Screen**



191586

## Contact Information

This window allows users to enter their contact information including name, telephone number, location, and email address.

## System Security

This window provides users with a security slide bar. The Low, Medium, and High security levels allow users to select an administratively defined security policy. Each setting maps to a specified system state configured on the central management center. If you have not defined different levels of security states for agents, when users move the slider between security levels, it will not alter their agent security. Note that in all cases, whether you have states defined for all security levels or not, if you permit end users to turn off agent security, when the slider is moved to the Off setting, it will disable all agent security.

Here are some examples of how you might define various security states to correspond to specific security levels:

- Configure a system state and a corresponding policy that applies when the agent security level is set to High. This security setting may cause the agent to detect a wide range of both known attacks and potential attack behavior. With high security enabled, these actions could be automatically denied when they are detected rather than giving the user the option of allowing them via a query user pop-up box (as might be available in lower settings).
- Configure a system state and a corresponding policy that applies when the agent security level is set to Medium. A Medium security setting may cause the agent to detect a wide range of attacks similar to those detected at the high setting. But this level might cause the user to be presented with more query pop-up boxes to ensure that the action taking place is intended and not a type of attack.
- Configure a system state and a corresponding policy that applies when the agent security level is set to low. A Low security setting may cause the agent to detect the more commonly known attacks that are easily distinguished from normal system behavior. In most cases, the user could be queried as to whether the detected action should be allowed or not.

## Network Lock

Users can select the Network Lock checkbox from the System Security window. When the Network Lock checkbox is enabled, the agent will not allow any new network connections until the lock is disabled. Alternatively,

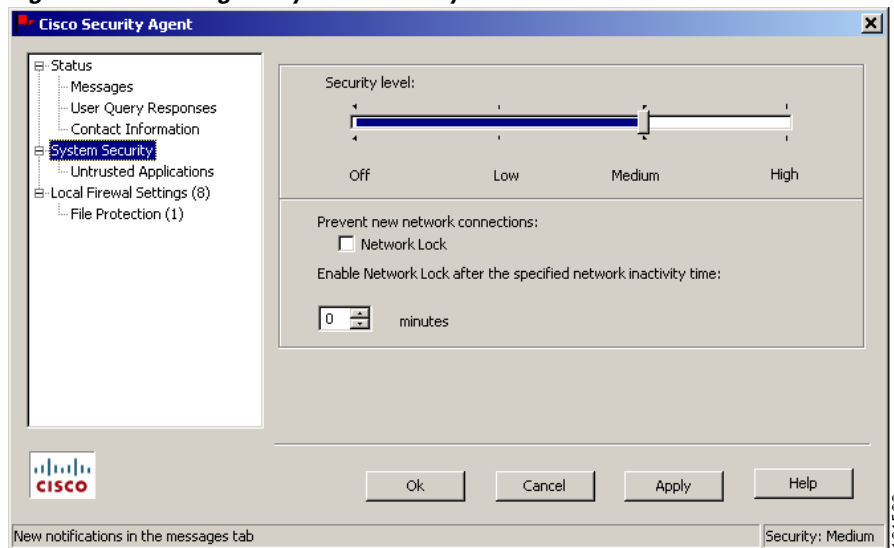
users can set a time frame of 0-60 minutes of network access inactivity before the agent automatically enforces a network lock on the system. When that time frame is reached, the Network Lock checkbox is automatically selected by the agent itself. Users must unselect the checkbox to turn it off again. When a network lock is enforced on the system, existing network connections are not lost, but no new connections (in or out) are allowed.

If the Network Lock is enabled when users reboot the system, Network Lock is no longer turned on after the reboot. (All other agent settings, except temporary query response caching, remain constant across reboots.)

**Note**

A **Resume** button may appear in this agent window. See [Installation Applications Policy, page 7-4](#) for information on the Resume button.

**Figure A-5 Agent System Security Screen**



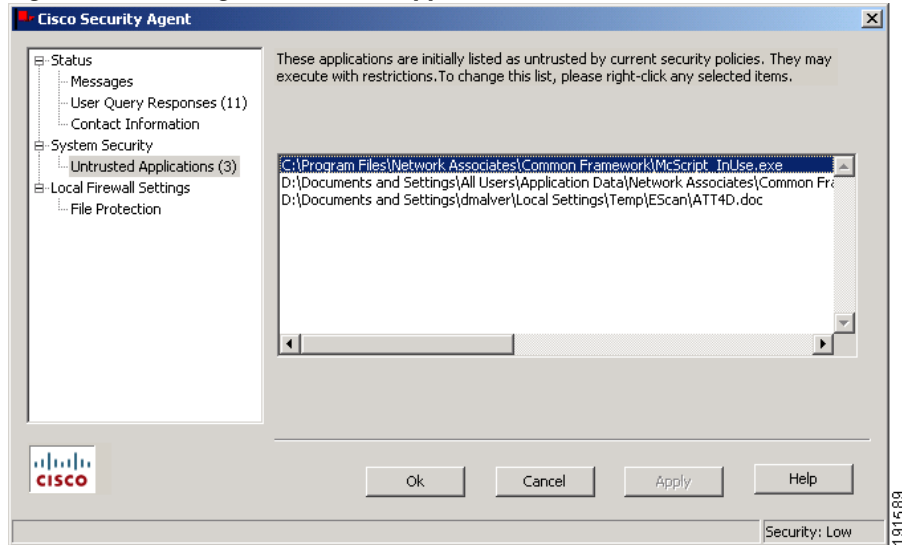
### Untrusted Applications

Applications that have read downloaded content from the network are generally considered to be more vulnerable than other application types. The central management center and the agent keep track of applications and file types that read downloaded content and place this information in the Untrusted Applications edit box. Applications and files listed there can

continue to operate under restrictions. Therefore, being listed as an untrusted application is a result of management center definitions and agent actions (query responses, for example). But the consequences of being labeled an untrusted application are defined by the management center. The management center imposes the appropriate restrictions. For example, untrusted applications cannot write to registry keys that are typically targeted by viruses and it cannot write to system executables.

If users want to remove a file or program from the list of untrusted applications, from the Untrusted Applications window, right-click on the selected entry in the edit box and select **Mark As Trusted**. This removes the application from the untrusted list, making it trusted.

**Figure A-6** Agent Untrusted Applications Screen



## Local Firewall Settings

You can enable these firewall settings on the agent UI to allow end users to control which applications have security permissions on their systems and what those permissions are. This feature allows local control but the centrally defined policy assigned by you must also allow for it. Settings defined here must pass both local and central permissions in order to work. Firewall setting permissions are assigned locally when end users are queried as to whether or not the application in question can access the network. These permissions can

also be assigned during a learning mode period. Also note, that this feature is intended for interactive workstations as opposed to servers which should only be managed by a central policy. If this feature is present, users must select the Enable checkbox to turn on firewall settings.

Users can see what permissions have been assigned to specific applications based on the graphic that appears beside the application name in the edit box. If there is no graphic present for an application, that network permission type has not yet been assigned. If users want to change the assigned permissions of a given application, they can select it in the edit box and press the Delete key.



---

**Note** If a host belongs to a group operating in Test Mode, local firewall settings are ignored.

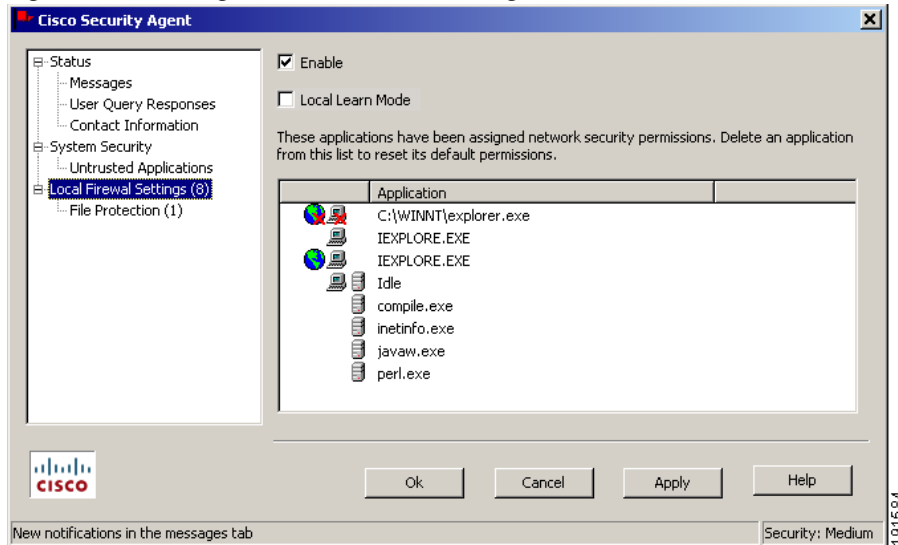
---

### Local Learn Mode

Users can enable local learn mode for the firewall settings feature. While in local learn mode, the agent is noting which applications run on the system and what those applications are allowed to do locally on that host. Running the agent in local learn mode for a certain amount of time allows it to learn the system's normal operating behavior and then provide security accordingly once learning mode is disabled. While in local learn mode, the agent notes what applications are used to access the network and assigns those permissions automatically.

When the agent is taken out of local learn mode, it will allow only those applications it previously noted to run in the manner in which they were used during the learning period. If the agent notices a new action that it has not learned taking place on the system, the agent queries the user, asking if it is okay for the application in question to access the resource in question. Once users reply to the query, the agent remembers the response and the next time the application is used, the same action is allowed or denied based on the initial response and users are not queried again.

Figure A-7 Agent Local Firewall Settings Screen

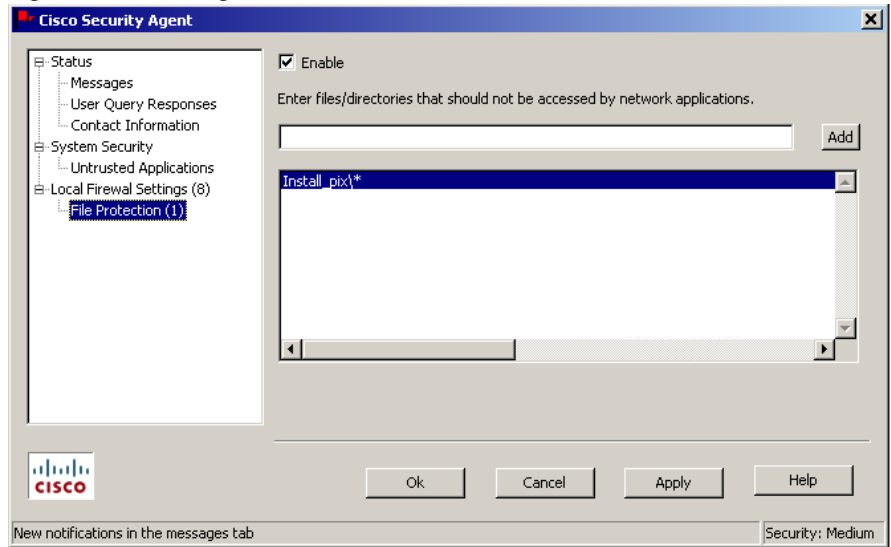


## File Protection

Through some simple configuration, the agent can protect specified local files and directories on systems from all network access. This is useful if there is sensitive personal information stored on user systems. Entering the name of the file or directory that users want protected cuts off all network access to that resource.

Users must select the Enable checkbox to turn on File Protection. From the File Protection window, users can enter the file or directory name in the top edit field and click the Add button. This file or directory is now protected from all network access. (Note that if a network application attempts to access a protected file, users are queried. In some instances, users may want to allow this access.) To remove file protection, select the file name or directory name in the edit field and press the Delete key.

In order for the agent to determine if an entry is a file or a directory, users must use a specific syntax. That syntax is explained to end users in the Cisco Security Agent online help.

**Figure A-8** Agent File Protection Screen**Note**

When a rule is triggered on an agent system and a message appears in the Messages tab, the flag icon in the system tray waves.

# Turn Agent Security Off

Provided there is not an Agent service control rule or Agent UI control rule (See [Agent Service Control, page 6-3](#) and [Agent UI Control, page 6-7](#) for rule details) that denies this action, all users can stop the security the agent provides on a Windows or Linux host by accessing the agent UI and clicking on the flag in the menu bar. If users move the sidebar (if present) to the Off setting, agent security enforcement stops.

**Note**

---

If there is no agent UI on a system (no user interaction), the ability to turn off agent security is not available to non-administrative users.

---

Provided there is not an Agent service control rule that denies this action, Windows administrators can run the following commands from a command prompt window on the agent host system to stop and start the agent service:

```
net stop csagent
net start csagent
```

Provided there is not an Agent service control rule that denies this action, administrators can stop and start the agent service on a UNIX (Solaris and Linux) host by running the following commands from a command prompt window on the agent host system:

```
/etc/init.d/ciscosec stop
/etc/init.d/ciscosec start
```

**Caution**

---

Stopping agent security and/or stopping the agent service on any system disables all rules on that system. Starting the agent service and resuming security reinstates all rules.

---

# Installing Software Updates on Agents

Cisco occasionally provides software updates for Cisco Security Agents. You configure CSA MC to distribute the appropriate software updates to specified agents across the network. When agents poll in to check for new rules, if there is an update available for the agent in question, it transparently receives the update at that time. The update installs without any interaction from the end user. See [Modify Groups With Hosts That Meet a Search Criteria, page 3-47](#) for CSA MC configuration details

**Note**

---

Use the `csactl` utility (see [page A-25](#)) on Solaris systems to check for updates and install them.

---

In some cases, you may require agent systems to be rebooted after installing an update. Users are prompted that the system will reboot within 5 minutes if this is necessary. Note that configuration changes are not applied until the system is rebooted.

Agent systems contain online help explaining how software updates work. You may want to refer users to it.

## 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.

# Common Windows Cisco Security Agent Error Codes

The following are the most commonly seen error codes for Windows agent installations.

2029 - OKENA\_STATUS\_DB\_ERROR. This message usually indicates that the database is down or busy.

2030 - OKENA\_STATUS\_LICENSE\_REACHED\_LIMIT.

2031 - OKENA\_STATUS\_REGISTRATION\_NOT\_ALLOWED. This indicates that the CSA MC registration control is actively denying agent registration.

2035 - OKENA\_STATUS\_INVALID\_LICENSE. This indicates that the license is corrupt or expired.

2037 - OKENA\_STATUS\_REGISTRATION\_BACKOFF. This indicates that an agent with the same IP address has already registered with CSA MC in the past hour.

## 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. When you download the 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_V5.2.0.265-sol-setup-f734064be5a448b88
e2a27867059113c.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) 5.2.0.15
```

**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
Installing CSAagent as <CSCOcsa>
```

**Step 6** The installation continues to copy and install files. When the install is complete, the following is displayed:

```
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) 5.2.0.15
```

**Step 7** Quit (q) when installation is finished.

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

**Step 8** Optionally, reboot the system by entering the following.

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



### Caution

If a Solaris 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 agent, enter the following command:

```
# pkgrm CSCOcsa
```

**Note**

---

If an agent is running a policy which contains an Agent service control 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 Service Control, page 6-3](#) for details on this rule type.

---

# UNIX Agent csactl Utility

Because the Solaris Cisco Security Agent has no user interface, a utility is provided which allows you to check the Solaris agent status, poll in to CSA MC and re-enable logging. The command you enter to perform these functions is **csactl**.



## Note

Note that this utility has also been made available for Linux systems. Because Linux does provide an agent UI, using the csactl utility on Linux is optional.

Enter the csactl command as follows:

```
# /opt/CSCOcsa/bin/csactl <command>
```

Available commands are:

poll	Triggers an immediate poll of the management server. (Also lets you know if there is a software update available.)
resetlog	Resets the logging holdback -- allows all log messages.
status	Displays a small amount of status information. (Also lets you know if there is a software update available.)
swupdate	Updates agent software.
info <text>	This is a mechanism for directly sending custom (informational) textual events to CSA MC. Once the message reaches the CSA MC, it can be viewed or a notification can be sent to an administrator.
warning <text>	This is a mechanism for directly sending custom (warning) textual events to CSA MC. Once the message reaches CSA MC, it can be viewed or a notification can be sent to an administrator.

alert <text>	This is a mechanism for directly sending custom (alert) textual events to CSA MC. Once the message reaches CSA MC, it can be viewed or a notification can be sent to an administrator.
about	Displays agent software version number.

The commands listed above are only available to root.

For example, poll in to CSA MC by entering the following:

```
# /opt/CSCOcsa/bin/csactl poll
Poll of management center succeeded
```

For example, check the status of the agent by entering the following:

```
# /opt/CSCOcsa/bin/csactl status
Status:
Management center: stormcenter
Registration time: 2006-11-20 15:19:16
Host id: {FG9DA858-6131-46E9-18BD-EE32BA2D0676}
Last download time: 2006-11-20 15:19:23
Last poll time: 2006-11-20 15:20:42
Software update: newer version is available
```

For example, to perform a software update:

```
# /opt/CSCOcsa/bin/csactl swupdate
```



**Note**

You must reboot the system after performing a software update.

For example, re-enable logging if duplicate messages are being throttled:

```
# /opt/CSCOcsa/bin/csactl resetlog
Reset Log throttle sent to kernel
```

# 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_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar /tmp
```

**Step 2** Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V5.2.0.218-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 Linux 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.)

---

## 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-5.2-218
```

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

```
# rpm -ev CSAagent-5.2-218
```



---

**Caution**

If an agent is running a policy which contains an Agent service control 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 Service Control, page 6-3](#) for details on this rule type.

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

---