



CHAPTER 3

Configuring Groups and Managing Hosts

Overview

The system hosts across your network, including mobile systems in the field, must download Cisco Security Agent software and register with Management Center for Cisco Security Agents to receive the security policies configured for them. When you are ready to apply policies to the hosts running agents, having those hosts placed into common groups streamlines the process of assigning policies to several hosts at once. To place hosts into groups, you must first analyze the security needs of each host system and map out a security plan. Hosts with similar requirements can then be grouped together.

Management Center for Cisco Security Agents ships with several pre-configured groups you can use. If the included groups do not suit your needs, use the instructions in this chapter to configure new groups or to edit existing ones.

This section contains the following topics.

- [Grouping Hosts Together, page 3-2](#)
- [Mandatory Group Enrollment, page 3-3](#)
- [Configuring Groups, page 3-4](#)
- [Managing Agent Kits, page 3-10](#)
- [Creating Agent Kits, page 3-10](#)
- [Agent Reboot vs. No Reboot, page 3-21](#)
- [Agent Registration, page 3-23](#)

- [Scripted Agent Installs and Uninstalls](#), page 3-23
- [Registration Control](#), page 3-22
- [Managing Hosts Using CSA MC](#), page 3-24
- [Viewing General Host Statuses with CSA MC](#), page 3-24
- [Viewing All Hosts Managed by CSA MC](#), page 3-25
- [Viewing Host Details](#), page 3-25
- [Host Detail View](#), page 3-27
- [Searching for Hosts](#), page 3-35
- [Deleting Moved and Migrated Hosts: Overview](#), page 3-38
- [Changing Host Memberships in Groups](#), page 3-42
- [Changing Host Memberships in Groups](#), page 3-42
- [Modify Groups With Hosts That Meet a Search Criteria](#), page 3-47
- [Host Managing Tasks](#), page 3-51
- [Configuring Scheduled Software Updates](#), page 3-56
- [Software Updates in a Distributed Configuration](#), page 3-60

Grouping Hosts Together

Host groups reduce the administrative burden of managing a large number of agents. All hosts across your network, including mobile systems in the field, must exist as registered host entries in the Management Center for Cisco Security Agents for policy configurations to be assigned to them.

Grouping individual host systems together provides the following advantages:

- It lets you consistently apply the same set of policies across multiple host systems.
- It lets you apply Alert mechanisms and Event Set parameters based on group configurations.
- It lets you use Test Mode to try out policies on groups of hosts before you actively enforce those policies.

You can group hosts together based on any criteria that best fits your enterprise. For example:

- Group hosts according to system function, such as web servers. Then you would create a policy that corresponds specifically to the needs of your web servers and distribute it to that group.
- Group hosts according to business groups, such as finance, operations, and marketing. Distribute policies based on each business group's individual needs.
- Group hosts according to geographical or topological location. For example, group hosts based on their subnet designation for reporting purposes.
- Group hosts according to their importance to your organization. Place mission-critical systems into a common group to apply critical alert level configurations to them.

**Note**

Hosts may belong to multiple groups and automatically receive policies that are attached to every group to which they belong. You can add or remove hosts from a group at any time. However, the policy configuration of a host that is moved to another group will not take effect until you generate your rule programs and distribute them.

Mandatory Group Enrollment

CSA MC provides three auto-enrollment architectural groups <All Windows>, <All Solaris>, <All Linux> that are mandatory for all hosts of a given OS architecture. For example, all Windows hosts are automatically enrolled in the <All Windows> (in addition to any other groups you have specified) when they register with CSA MC. Hosts cannot be removed from these mandatory groups.

By providing group auto-enrollment for hosts, any policies you attach to these groups also become mandatory by association. You might want to use these mandatory groups to apply policies that prevent some critical service from being inadvertently banned. For example, you could attach policies to prevent DNS or DHCP from being disabled by an overly restrictive rule.

Configuring Groups

Host groups reduce the administrative burden of managing a large number of agents. Grouping hosts together also lets you apply the same policy to a number of hosts. A group is the only element required to build agent kits.

You do not configure hosts with CSA MC as you do other CSA MC elements. When hosts across your network download and install agent kits, they automatically and transparently register with CSA MC. Hosts inherit membership to the groups that were associated with the agent kit they installed. Successfully registered hosts appear in a linked list when you select Hosts from the Systems category in the menu bar. At registration time, hosts are also automatically put into their assigned group. You can change host groupings at any time.

**Note**

Management Center for Cisco Security Agents ships with preconfigured groups (in addition to the mandatory groups) you can use if they meet your initial needs. If you use a preconfigured group, you do not have to create your own group as detailed in the following pages.

To configure a group, do the following.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down list that appears. The list of existing Groups is displayed. Management Center for Cisco Security Agents ships with several pre-configured groups.
- Step 2** Click the **New** button to create a new group entry. (This group is empty until hosts install agents and register.)

**Note**

If you have "All" designated as the operating system type for your administrator session, you are prompted to select whether this is a Windows, Solaris, or Linux group. See [Configuring Role-Based Administration, page 2-5](#) for details. (You cannot combine hosts of differing OS architectures in the same group.)

- Step 3** In the available group fields, enter the following information:
- **Name**—This is a unique name for this group of hosts. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, hyphens, and

underscores. You should adopt a naming convention that lets you quickly recognize groups in the CSA MC group list view.

- **Description**—This description appears in the list view to help you identify this particular group. Expand the **+Detailed** field to enter a longer description.

**Tip**

You can use the Tab key to navigate between edit fields.

Figure 3-1 Group Configuration Page

The screenshot shows the Management Center for Cisco Security Agents V5.2 interface. The browser address bar shows `https://biohazard/csam:52/webadmin`. The page title is "Management Center for Cisco Security Agents V5.2". The navigation menu includes "Events", "Systems", "Configuration", "Analysis", "Maintenance", "Reports", "Search", and "Help". The current page is "Systems > Groups > Servers - IIS Web Servers".

Quick links:

- [Modify host membership](#)
- [Modify policy associations](#)
- [View related events](#)
- [Explain rules](#)

Name: Servers - IIS Web Servers **Version:** 5.2 r119

Description: Systems running Microsoft IIS web server

Target architecture: Windows

Polling interval (hh:mm:ss): 01:00:00 Send polling hint

Rule overrides:

- Test mode
- Learn mode

Log overrides:

- Log deny actions
- Verbose logging mode
- Filter user info from events

Application Deployment Investigation enabled: No [\[Enable\]](#)

Attached Policies:

Policy Name	Version	Description	Rule Modules
<input checked="" type="checkbox"/> Web Server - Microsoft IIS - Windows	5.2 r119	Application enforcement policy for IIS web server software.	2 modules

Combined Policy Rules:

View [All](#) rules

Enforce rules: 32 (click the header links to sort)

ID	Type	Status	Action	Log	Description	Rule Module
353	Data access control	Enabled			IIS and Apache Web Servers, Common Windows file exploits	Common Web Server Security Module [V5.2 r119]
88	Application control	Enabled			IIS Web Server Dynamic Applications, invoke IIS Web Server in Isolation Mode	Microsoft IIS Web Server [V5.2 r119]

Buttons: Save, Delete, No rule changes pending, Generate rules

Logged in as: admin

Step 4 You can change the default **Polling interval** to any value between 10 seconds and 24 hours (formatted as hh:mm:ss). This controls how often agents in this group poll into CSA MC for policy updates. Shortening the polling time can be useful when you are trying out new policies. Otherwise, the default value is recommended. (If you have the same hosts in multiple groups, the group containing the shortest polling interval setting takes precedence for the hosts in question.)



Note If you change a group's polling interval, that new interval time will not take effect until the host polls in again for new rules. Therefore, it may take as long as the previous polling interval setting before hosts begin polling in using the new setting.

Step 5 Optionally, enable the **Send polling hint** capability. Normally, if you make changes to a policy, schedule a software update, or make any other change to a host's configuration, the host does not receive that change until it next polls into the MC. But if you have the Send polling hint checkbox selected, certain changes that occur on the MC will cause a "non-reliable" signed UDP message to be sent to the appropriate hosts. This message tells hosts to poll into the MC earlier than their next scheduled polling interval. The UDP message would be sent if a policy change occurs, if a global correlation event causes a file to be added to the global quarantine list, and if you select to retrieve status information from a particular host. (This feature only works if no NAT or PAT exists between CSA MC and the agent.)

Step 6 Optionally, enable one or more **Rule overrides** for the group. You can select the **Test mode** checkbox for this group.



Caution In Test Mode, the Cisco Security Agent will not deny any action even if an associated policy says it should be denied. Instead, the agent will allow the action but log an event (if logging is selected for the rule). This helps you to understand the impact of deploying a policy on a host before enforcing it. For further information, see [Using Test Mode, page 5-7](#).

Step 7 Optionally, enable **Learn mode** to localize policies on the agent and to prevent the flurry of query pop-ups that can appear to a user when the agent is first installed. Learn mode works in a specific manner, in combination with deployed query user rules. These queries are automatically answered and remembered persistent for the learning mode period. More information is provided in [Using Learn Mode, page 5-11](#).



Note Using the Hosts Managing Tasks page, you can configure “timed” Learn Mode and “timed” Test Mode. Basically, you can configure a task that causes hosts to move in and out of selected groups at timed intervals. This way, you can have all new hosts move out of a Learn Mode group or a Test Mode group after a set time. Refer to [Host Managing Tasks, page 3-51](#) for configuration information.

- Step 8** Optionally, enable one or more **Log overrides**. Enable **Verbose logging mode** to change the event log timer to log all reoccurring events rather than suppressing duplicates. See [Chapter 10, “Event Logging and Alerts”](#) for more information on the event log.
- Step 9** Optionally, enable **Log all deny actions** to turn on logging for all deny rules running on hosts within the group regardless of the individual rule settings for the policy attached to the group. You may wish to use this feature to turn on all deny logging for diagnostic purposes.
- Step 10** Optionally, you can select the **Filter user info from events** checkbox for this group. Due to privacy issues, you may not want this username information displayed in events or in the additional information screen available from the event Details link.
- Step 11** Optionally, for Windows groups, you can select to enable Application Deployment and Analysis. This analysis functionality works with CSA MC and the agent, serving as a data collection tool for administrators deploying policies across systems and networks. See [Chapter 13, “Using Cisco Security Agent Analysis”](#) for detailed information. If this feature is enabled, you can access analysis reports from a link on this page.
- Step 12** When all required information is entered, click the **Save** button to enter and save your group in the CSA MC database.

Once you attach (associate) policies to specific groups, the configuration view for the group displays a table listing all the rules, in order of precedence, that are applied to that group. From this table, you can navigate to those rules and policies.

Resetting Cisco Security Agents

The MC lets you centrally reset agent settings back to their original states and clears all user-configured settings. You may want to do this in order to clear cached user query responses or to reset system states.

To remotely reset *all* hosts in a group to the system default settings, click the **Reset Cisco Security Agents** link in the Quick Links section of the Group page.

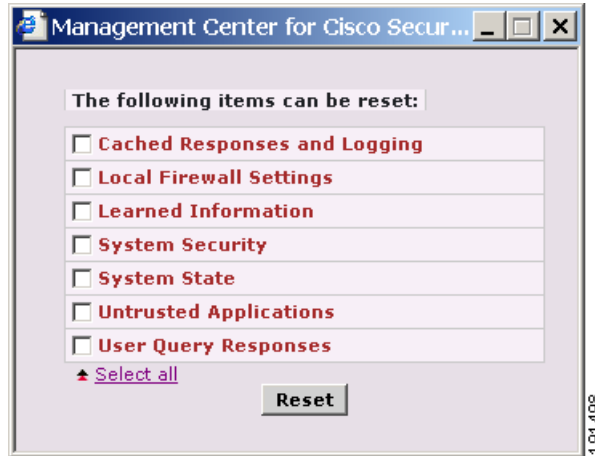
**Note**

This functionality is also available from the individual Host page, letting you reset one host at a time. See [The Agent User Interface, page A-8](#) for more information on the agent reset option (also available locally on the agent system).

When you click the **Reset Cisco Security Agents** link, a pop-up window appears displaying various checkboxes that let you reset various specific agents settings or to reset all settings. You can reset the following agent settings:

- **Cached Responses and Logging** - This clears the temporarily cached query user responses. These are query responses that are stored locally for approximately one hour.
- **Local Firewall Settings** - This clears any local firewall network permissions or file protections that the end user has configured.
- **Learned Information** - This clears the learned, persistent query responses on the agent system. It also clears other learned information such as running applications and unusual system calls. This also causes the automatic 72 learning period to start again. See [Using Learn Mode, page 5-11](#).
- **System Security** - This resets the Security level slide bar to its original deployment setting (Medium). This also clears the Network Lock if it is selected.
- **System State** - This resets the agent System State back to its original deployment state. This is useful if the end user system has been quarantined or been placed in a network lockdown state by the agent due to a rootkit detection or by some other means. The reset will be received by the agent regardless of a quarantine or network restriction being imposed.
- **Untrusted Applications** - This clears the Untrusted Applications list that is automatically kept by the agent.
- **User Query Responses** - This clears *all* the persistent query responses on the agent system.

Figure 3-2 Reset Cisco Security Agent Options



191498

Managing Agent Kits

The Management Center for Cisco Security Agent allows for the creation and maintenance of custom agent installation kits that greatly reduce the administrative burden of deploying the agent on new systems.

Agent kits must have group associations for deployment. Groups are a collection of policies and are associated with a number of Hosts. When hosts download agent kits, the kits place the host in the corresponding groups and enforce the associated policies of each group.

CSA MC also ships with preconfigured agent kits you can use if they meet your initial needs. There are kits for generic desktops, generic servers, and CSA MCs (CiscoWorks VMS).

Creating Agent Kits

At the time of creation of the agent kit, it must be associated with one or more groups. The particular agent kit a host installs determines with what group(s) the host is associated. You can create as many kits as necessary to distribute your policies to targeted hosts.

After a kit is installed on a host, the agent running on that host registers itself with CSA MC. CSA MC then automatically places the host in the groups that were associated with the installed kit.

**Note**

CSA MC ships with preconfigured agent kits you can use if they meet your initial needs. There are prebuilt kits for desktops, servers, and many more. These kits place hosts in the corresponding groups and enforce the associated policies of each group. (If you use a preconfigured agent kit, you do not have to build your own kit as detailed in the following pages.)

**Note**

If you intend to distribute Cisco Trust Agent (CTA) in an agent kit, make sure that you have copied the correct CTA installer files to CSA MC before you begin this procedure. See *Installing the Management Center for Cisco Security Agent* manual for the procedure to copy CTA installer files.

To create agent kits, do the following.

Step 1 Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. Existing agent kits are displayed.

Step 2 Click the **New** button to create a new agent kit.

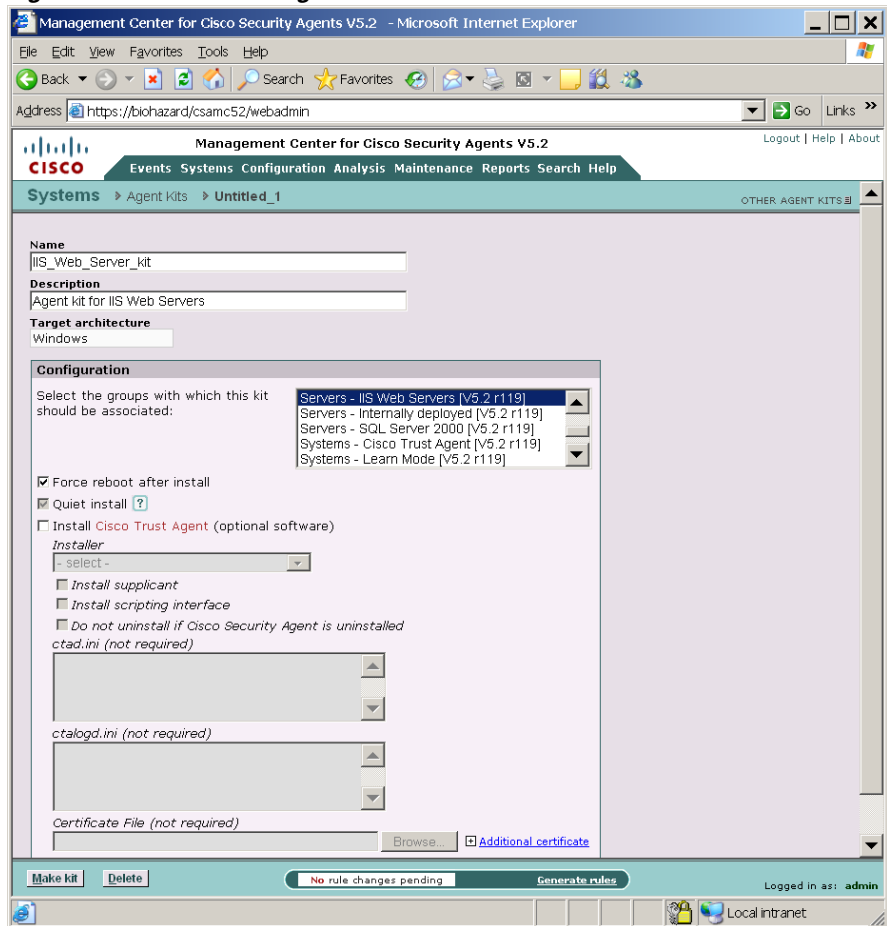
**Note**

If you have "All" designated as the operating system type for your administrator session, you are prompted to select whether this is a Windows, Linux, or Solaris kit. See [Configuring Role-Based Administration, page 2-5](#) for details. (You cannot select a Solaris group for an agent kit that you have configured for Windows systems.)

Step 3 In the agent kit configuration view (see [Figure 3-3](#)), enter a **Name** for this kit. This must be a unique name. Agent kit names cannot have spaces. Generally, it's a good idea to adopt a naming convention that lets you and the systems that will be downloading the kit, recognize it easily.

Step 4 (Optional) Enter a description in the Description field. The description appears in the agent kit list view to help you identify this particular kit.

Figure 3-3 Create Agent Kit



- Step 5** From the available list box, select the group or groups of host systems that will download and install this kit. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press and hold the **Shift** key when you click on an item to select multiple successive items.
- Step 6** You have the option of forcing systems to reboot after the agent installation completes (Windows and Linux only). If you select the **Force reboot after install** checkbox, when the install finishes, a message appears to the end user warning that the system will automatically reboot in 5 minutes. This reboot cannot be

stopped by the end user. Keep in mind, if you are selecting to force a reboot, the installation must also be "Quiet". See the next step for more details. Refer to [Agent Reboot vs. No Reboot, page 3-21](#) for information on what security is not enforced if a system is not rebooted after an agent installation.



Note Solaris agent kit installations do not have the option to reboot automatically when complete. If you wish to reboot a Solaris system after installing an agent, you must do so manually.



Note In some cases, you may not want a system to reboot after the installation completes. If a reboot does not occur after the agent installation, partial security is enforced immediately. Full security is enforced after the first reboot. See [Agent Install Complete Prompt for Automatic Reboot, page 3-20](#) for details. (Note that Windows NT4 systems must be rebooted after an agent installation.)

Step 7 Select whether or not to have agents install "quietly" on end-user systems (Windows and Linux only). A **Quiet install** requires users to download the self-extracting executable as does the "noisy" install. The difference is, no prompts appear and the user is not required to enter any information or select any options. A noisy install prompts the user for installation options, such as selecting the installation directory, in addition to the reboot prompt.

These possible checkbox options would be combined for the following effects once the Windows or Linux agent installation has completed:

Force reboot checkbox=enabled Quiet install checkbox=enabled	The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes.
Force reboot checkbox=disabled Quiet install checkbox=enabled	The install proceeds and ends quietly with no prompts. Full functionality occurs the next time the user happens to reboot.
Force reboot checkbox=disabled Quiet install checkbox=disabled	The install prompts the user for directory path installation and ends by displaying a prompt indicating that an update has occurred and the end user can reboot the system at their convenience for full functionality.

Step 8 (Optional) Install the Cisco Trust Agent by selecting the checkbox next to **Install Cisco Trust Agent**. (Instructions for copying the CTA installation files are in the *Installing Management Center for Cisco Security Agents* PDF manual.) The area below the checkbox expands to show several fields. These fields are not explained in this manual. *You must refer to your CTA documentation for CTA product information.*

**Note**

If no CTA installation files have been copied to the CSA MC system, the Cisco Trust Agent checkbox is “grayed out” on the Agent kit page. This checkbox is only active and available when CTA installation files have been detected on the MC system.

**Note**

Distribution of CTA through agent kits is only supported for Windows versions of CTA.

These fields allow you to specify the following settings:

- **CTA Installer.** From the drop-down menu, specify which Cisco Trust Agent installer to use. (You must copy the latest CTA installer files, provided by the CTA product group, to CSA MC first. See the installation guide for information.) Note that the only CTA kits available for installation with CSA 5.2 include the following syntax: `ctasilent*.exe` or `cta*.msi`. All valid CTA kit installations are silent.

If you select a CTA installer that includes the “supplicant”, the **Install Supplicant** checkbox becomes available. If you are installing the supplicant, you can optionally browse to **Network, Policy, and Credential Configuration** .xml files to install with CTA. (Note that each file may be a maximum of 128KB in size.)

- **Install scripting interface.** The CTA Scripting Interface is only available for NAC Phase 2 networks.
- **Do not uninstall if Cisco Security Agent is uninstalled.** Check this box if you want CTA to remain installed even if CSA is uninstalled.
- **ctad.ini/Initialization data.** The text you enter in this data field is used to create the `ctad.ini` file for CTA. Note that this field accepts a maximum of 10kbs of data.

- **ctalogd.ini/Log data.** The text you enter in this data field is used to create the ctalogd.ini file for CTA. Note that this field accepts a maximum of 10kbs of data.

**Note**

If you do not enter your own text into the ctad.ini or ctalogd.ini fields, CTA installs using the default ctad.ini and ctalogd.ini files and their default settings.

- **Certificate file.** Browse to one more Cisco Secure ACS server certificates to be installed along with CTA. (Click the **Additional file** link to add more files for the number of certificates you want include.)

**Note**

Although the certificate file is not required to install CTA, it is required for CTA to operate.

**Note**

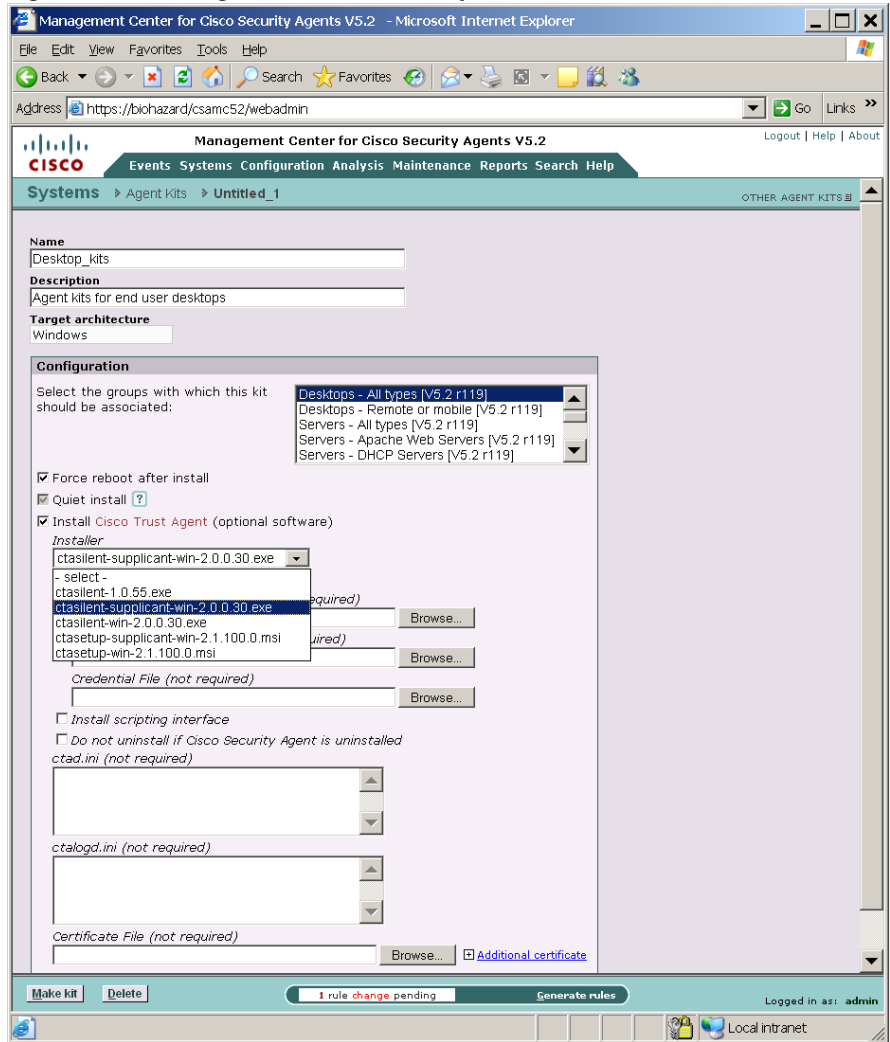
Refer to Cisco Trust Agent Administrator Guide for a complete description of how these settings impact your CTA installation. For NAC and CTA plugin details, see [Cisco Security Agent Posture Plug-in for CTA, page 12-22](#).

**Note**

If you are installing the Cisco Trust Agent, you must apply the CTA policy (pre-configured and shipped with CSA MC) to the applicable groups for CTA to operate.

Be aware that CTA may not be supported on all OS types that support the Cisco Security Agent. Before installing the Cisco Trust Agent, please refer to your CTA documentation for supported operating system information.

Figure 3-4 Agent Kit CTA Install Options



Step 9 Click the **Make Kit** button.

Once you click the Make Kit button, CSA MC produces a kit for distribution. It displays a URL for this particular kit (see [Figure 3-5](#)). You may distribute this URL, via email for example, to the host systems the kit is designated for. 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>/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.

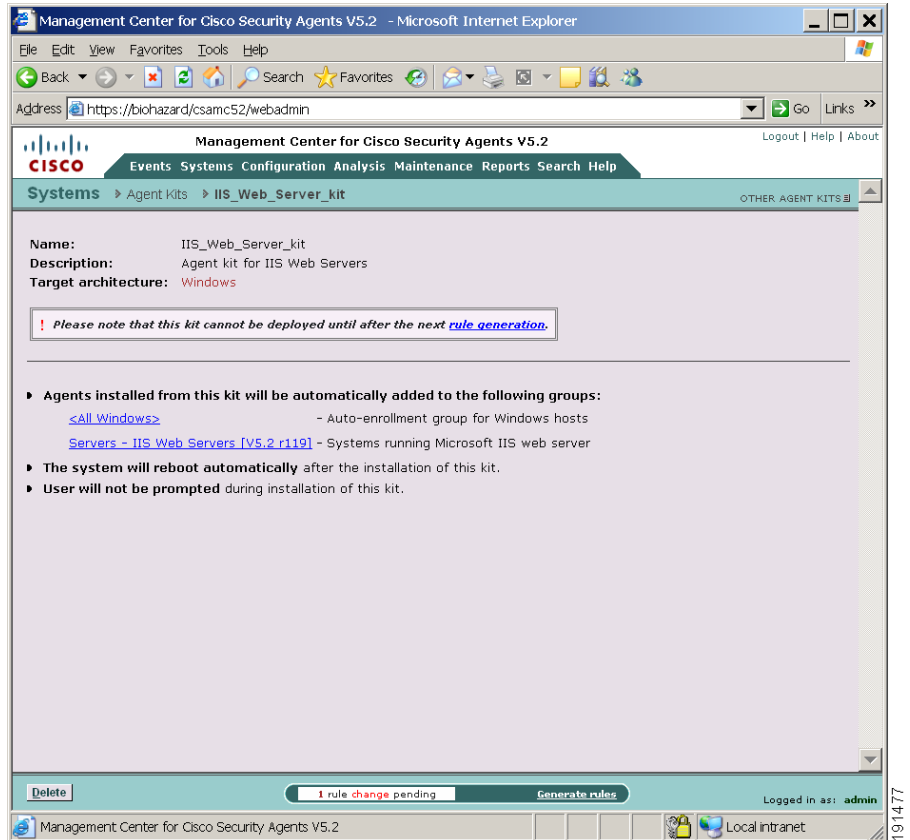


Note Note that the Registration Control feature also applies to the < system name>/csamc52/kits URL. If the Registration Control feature (see [Registration Control, page 3-22](#) for details on the feature) prevents your IP address from registering, it also prevents you from viewing this “kits” URL.



Note You must generate rules after agent kits are created. See [Agent Kit Status, page 3-19](#) for details on when a kit is ready for download.

Figure 3-5 Agent Kit Download URL

**Note**

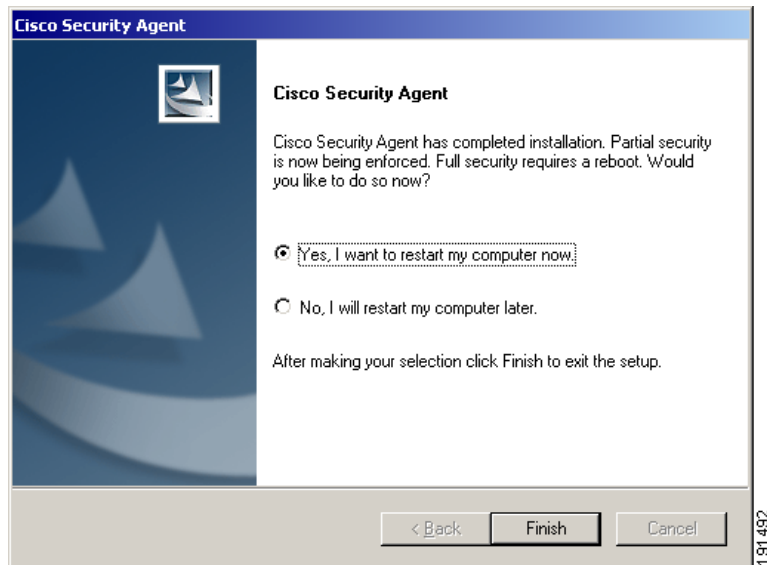
If you installed Management Center for Cisco Security Agents to the default directory, all agent kits are placed in the `%Program Files%\Cisco Systems\CSAMC\CSAMC52\bin\webserver\htdocs\deploy_kits` directory.

Agent Kit Status

When you create an agent kit, it is given one of three status levels based on how far into the configuration you've progressed. Those status levels are as follows:

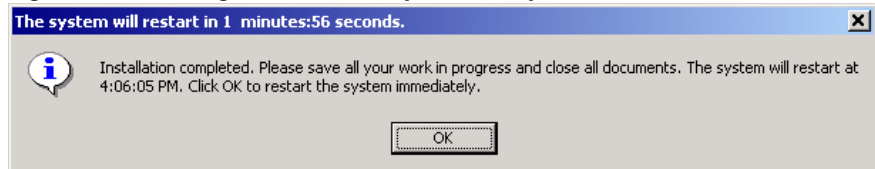
- **Ready:** This means the agent kit is ready for download to host systems.
- **Needs rule generation:** This means that all agent kit configuration parameters are complete, but you must generate rules before the kit can be downloaded.
- **Incomplete:** This means that you have not configured all the necessary parameters for this agent kit. You must complete the configuration and then generate rules before the kit can be downloaded.
- **Undeployable:** This status will only occur if you have ungenerated kits on the MC and then you upgrade the MC to a newer version. Agent kits that were created but never generated and have an old version number can never be deployed and should be deleted.

Figure 3-6 Agent Install Complete Prompt for Optional Not-Automatic Reboot



191492

Figure 3-7 Agent Install Complete Prompt for Automatic Reboot



191479

Agent Reboot vs. No Reboot

If a system is not rebooted following the Cisco Security 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.



Caution

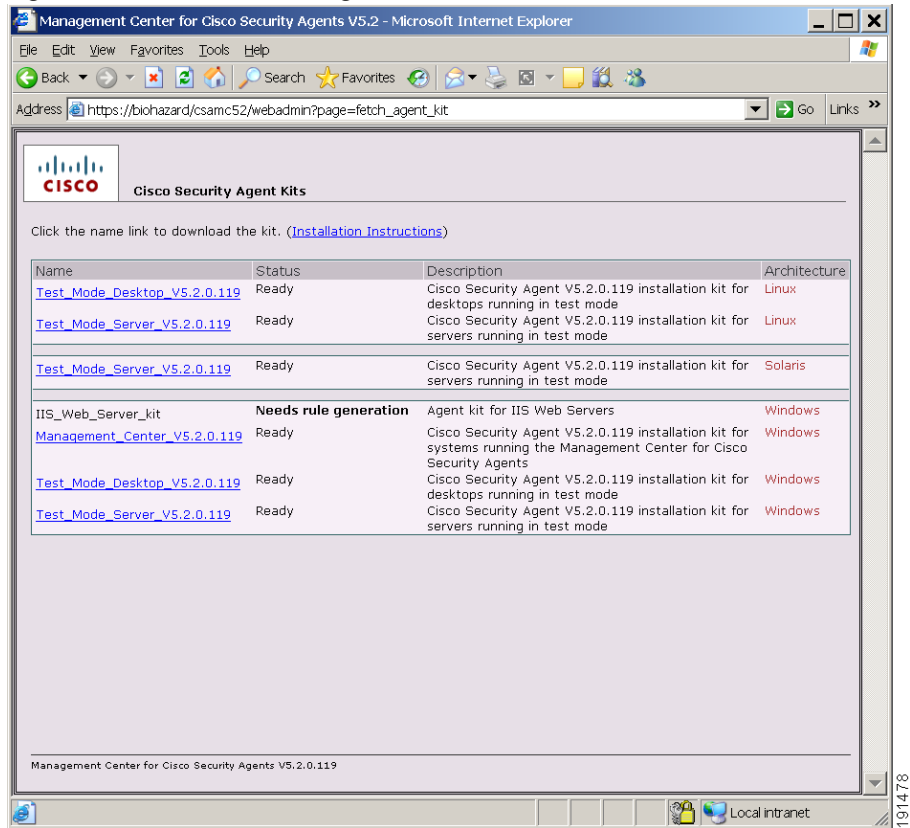
Windows NT systems must be rebooted after the agent installation completes. Windows NT systems will not receive a reboot optional prompt at the end of an agent installation (even if that option is part of the agent kit installation).



Note

The reboot information here only applies to new agent installations. It does not apply to software updates. Please refer to [Table 3-1 on page 3-58](#) for software update reboot details.

Figure 3-8 Download Agent Kits



Registration Control

This feature is accessible from the Systems item in the menu bar. Enter a range of addresses in the registration control page to restrict agent hosts attempting to successfully register with CSA MC. Only those hosts with addresses entered here can register with CSA MC.

The default entry here is <all> (0.0.0.0-255.255.255.255) which applies no address registration restrictions. An example entry of restricted registration addresses is as follows. (Only those addresses within the range listed can register. This range is inclusive):

192.168.10.0-192.168.10.255

172.16.20.0-172.16.20.255

Agent Registration

When an agent kit is ready for distribution, you can notify end users to download and install the kit from the URL produced by CSA MC when the kit is made. Once the kit installation is complete, each individual host's agent automatically and transparently registers with CSA MC.



Note

Each kit is created for particular groups based on the policies that will be attached to those groups. Policies are described in [Chapter 4, “Building Policies”](#).

Scripted Agent Installs and Uninstalls

You can use scripts to silently install and uninstall Windows Cisco Security Agents on end user systems. (Scripted agent installs and uninstalls are not supported on Linux and Solaris systems.)

- Scripted install: The agent kit is a self-extracting executable placed in the following directory on the server: %Program Files%\Cisco Systems\CSAMC\CSAMC52\bin\webserver\htdocs\deploy_kits. (Retrieve the kit from this directory or download it from the server.) You can then use a script to copy and silently install agent kits on systems. Note that you must select the **Quiet install** checkbox when you build the kit if you are planning to install it via a script.
- Scripted uninstall: The agent installation places a bat file in the system32 directory. Administrators may use a script to remotely and silently uninstall the agent by invoking the CSA_uninstall.bat file in the system32 directory. You must also pass a parameter to the file for the agent to uninstall silently regardless of whether the original agent kit was a Quiet install. Enter the following: CSA_uninstall.bat 3

**Note**

Before silently uninstalling the agent via a script, you must disable any agent service control rules that deny or query administrators before stopping the agent service.

Whether or not an end user system is going to have a visible agent UI or a hidden one (see [Agent UI Control, page 6-7](#)), the end user (or administrator) must download and install the agent kit on the system. The initial installation of an agent kit cannot be done automatically (unless you have written your own script to do so, see [Scripted Agent Installs and Uninstalls, page 3-23](#)).

Managing Hosts Using CSA MC

A host is any system that has installed an agent kit from CSA MC and has registered with CSA MC. The host may be a desktop or server and may be of any supported operating system type.

Once the host has registered with CSA MC, it can receive policy updates, it can be added to or removed from groups, and its status can be monitored by CSA MC.

Viewing General Host Statuses with CSA MC

Follow this procedure to view the general status of all hosts managed by CSA MC:

-
- Step 1** Move your mouse over **Events** in the menu bar and click **Status Summary** in the drop-down list.
 - Step 2** If it is not already expanded, click the plus box next to **Network Status**.
 - Step 3** There are several Network Status categories listed in the status summary page. Next to each category is a number indicating how many hosts have been placed in each of the status categories. Click the link for the number of hosts in the category to see the host list view for that category.

Viewing All Hosts Managed by CSA MC

To view all the hosts that are managed by CSA MC, follow this procedure:

-
- Step 1** Move your mouse over **Systems** in the menu bar and click **Hosts** in the drop-down menu.
- Step 2** (Optional) Sort the host list by operating system.
- Step 3** From the Architecture drop-down list box, select one of the following host statuses:

- **Active** : A host is active if it polls into the management server at regular intervals and has not missed three polling intervals. When you select this viewing option, a "Yes" for Active or a "No" for Not Active appears in the column.

Note that a "Not active host" is a host that has missed three polling intervals or has not polled into the server for at least one hour.

- **Protected**: When you select this viewing option, a "Yes" for Protected or a "No" for Not Protected appears in the column. A system is not protected if it does not belong to a group or if it belongs to a group that has no policies attached.
- **Latest software**: When you select this viewing option, a "Yes" for Latest Software or a "No" for Not Latest Software appears in the column. If an agent is not running the latest software, you will want to deploy a software update.
- **Test Mode**: When you select this viewing option, a "Yes" for running in Test Mode or a "No" for Not Running in Test Mode appears in the column.
- **Last Poll**: When you select this viewing option, the time and date of the most recent poll for the host is displayed.

Viewing Host Details

To view detailed information about one host, follow this procedure:

-
- Step 1** Move your mouse over **Systems** in the menu bar and click **Hosts** in the drop-down menu.
- Step 2** (Optional) Sort the host list by operating system.

Step 3 Click the link to a host to view detailed information about that host on the Host Detail page (see [Figure 3-9](#)).

From the Host Detail Page you have access to these tasks and information:

- [Quick Links Tasks](#)
- [Host Name and Description](#)
- [Host Identification](#)
- [Host Status](#)
- [Host Settings](#)
- [Group Membership and Policy Inheritance Table](#)
- [Combined Policy Rules Table](#)

Figure 3-9 Host Detail View

The screenshot displays the Management Center for Cisco Security Agents V5.2 interface in a Microsoft Internet Explorer browser. The address bar shows the URL <https://biohazard/csamc52/webadmin>. The page title is "Management Center for Cisco Security Agents V5.2". The navigation menu includes "Events", "Systems", "Configuration", "Analysis", "Maintenance", "Reports", "Search", and "Help". The breadcrumb trail is "Systems > Hosts > biohazard".

Quick links

- [Modify group membership](#)
- [View related events](#)
- [Explain rules](#)
- [Reset Cisco Security Agent](#)

Name
biohazard

Description
WindowsNT 5.2.3790 Service Pack 1 R2 [tS] (English) [x86 fam 15 model 2 step 4]x2 1023MB Tag: G7VBX11 (at cisco systems)

Contact information

Status

Host Identification

Product information: Cisco Security Agent Version 5.2.0.119
Last known IP address: 172.01.10.02 [[History #](#)]
Host ID: 109
UID: {63DC346F-3E34-444F-8EBC-87D1940B4D2C}
Registration time: 11/28/2006 9:33:21 AM
Operating system: Windows 2003 [WindowsNT 5.2.3790 SP 1 R2 Server with Terminal Services;English]
Cisco Trust Agent active: No

Host Status

Events issued in past 24 hours: [17](#)
Software version: Agent is running the latest software
Policy version: Up-to-date
Time since last poll: 0h 3m 35s
Security level: Medium
Insecure boot detected (state condition): No [[History #](#)]
Unprotected access detected (state condition): No
Untrusted rootkit detected (state condition): No
BIOS supported boot detection: No
Time since last Application Deployment data upload: -
[Detailed status and diagnostics](#)

Host Settings

Polling interval: 0h 10m 0s
Send polling hint: On
Test mode: Off
Learn mode: Off
Verbose logging mode: Off
Log deny actions: Off
Filter user info from events: Off
Application Deployment Investigation enabled: No [[Enable #](#)]

Group Membership and Policy Inheritance

Group Name	Version	Description	Policies
Move to Recycle Bin			

1 rule change pending [Generate rules](#) Logged in as: admin

Local intranet

Quick Links Tasks

- Click the **Modify group membership** link in the Quick Links box on the host detail page (see [Figure 3-9](#)) to add or remove this host from a group. See the

procedure, [Modifying the Group Membership of a Single Host, page 3-42](#), for the complete procedure.

- Click **View Related Events** to view an event log showing only the events for the host you are looking at.
- CSA MC provides an explanation, in paragraph form, of the policies attached to each host. Clicking the **Explain rules** link takes you to this paragraph explanation.
- Click the **Reset Cisco Security Agent** link to reset certain values that may have been configured or selected by the end user. See [Resetting Cisco Security Agents, page 3-8](#) for details.

Host Name and Description

- **Name and Description:** These fields are populated with information received from the agent system when it registers. This is the name that identifies this host system on the network. This name does *not* have to be unique. CSA MC assigns each registering host a unique ID number by which the database identifies it.
- **Contact Information:** Click this link to view any contact information provided to the agent by the user. The available fields for the user are: first name, last name, email, telephone, and location. This user is not required to provide this information, however, if an agent is generating alerts, having this contact information readily available could expedite troubleshooting measures.

Host Identification

- **Product Information**—This is the Cisco Security Agent version for this particular machine.
- **Last known IP address**—This is the IP address of the host. If DHCP addressing is used, this is the last known address of the host.
- **Host ID**—CSA MC assigns each registering host a unique ID number by which the database identifies it.
- **UID**—This is a globally unique ID for your agent. It is obtained from the agent kit. Different kits present different IDs. Every host that installs a particular kit will have the same registration ID. Once registered, however, each host receives a unique global ID.

- Registration time—This is the time that the agent registered with CSA MC.
- Operating System—This is the operating system installed on this particular machine. If the operating system is unsupported, this information appears here in red text.
- Cisco Trust Agent status—This displays whether optional CTA software is Installed, Not installed, Active, or Inactive on the system. This also displays the status of the CTA software version. If this field displays Not active, either CTA is not installed or NAC is not configured to check CSA attributes. If CSA attributes are not being queried by the NAC infrastructure, the status is Not active. (Note that if CTA software is active, this field also displays the current CTA posture status.)

Host Status

- Events issued in the past 24 hours—This is the number of events (rule triggers) that have occurred on the host system in the given time frame.
- Software Version—This is the version of Cisco Security Agent software the system is running. If there is a software update available for this host, this field provides that information. If an update for a host is scheduled but not yet installed, this field provides that information as well.
- Policy version—This field reads "Up-to-date" or "Not up-to-date", indicating whether the agent has the latest policy configuration from CSA MC.
- Time since last poll—This is the interval since the host system's last polling request.
- Security level—This indicates the current level displayed by the Security Level bar in the agent UI.
- Untrusted rootkit detected (state condition)—This indicates that the host has been in this named state. The only way to clear this state is to reset the state on the host. See [System State Sets, page 5-13](#).
- Insecure boot detected (state condition)—This indicates that the host has been in this named state. The only way to clear this state is to reset the state on the host. See [System State Sets, page 5-13](#).
- BIOS supported boot detection—This indicates if the host system BIOS is compatible with BIOS dependent boot detection features. See [Kernel Protection, page 6-50](#).

- Time since last Application Deployment data upload—If application deployment data collection is enabled on the end user system, this indicates the time of the most recent upload of analysis logging data.
- Detailed status and diagnostics—Click this link to view status information for the host in question. The Host Diagnostics window (see [Figure 3-10](#)) that is opened by this link uploads information from the agent. NOTE that you may have to click the **Diagnose** button to retrieve the most recent host information. This causes the agent to poll in with status data. You can use this information to diagnose agent issues and to view the current states and policies running on the agent system.

Clicking the **Diagnose** button also remotely triggers a program on the agent to gather additional self-describing diagnostic information on the system and on the agent itself. When the collection is complete, a "csa-diagnostics.zip" file is created and automatically uploaded to the MC. This zip file can be accessed from the Host Diagnostics window. The **Uploads** section of this window displays how many diagnostic zip files have been uploaded (see [Figure 3-11](#)). The MC can store a maximum of 3 diagnostic files per host. Click on the <#> **Uploads** link on the Host Diagnostics pop-up window to access the individual .zip files (see [Figure 3-12](#)).

**Note**

The MC can store a total of 100 diagnostic files for all hosts.

Figure 3-10 Host Diagnostics Pop-up Window - Data

The screenshot displays a web-based diagnostic window titled "Management Center for Cisco Security Agents V5.2 - Host Diagnostic - Microsoft Internet Explorer". The window shows the following information:

- Host:** biohazard
- Received:** 11/28/2006 3:06:55 PM
- Uploads:** Upload requested. Please wait a few minutes after next poll for upload to appear.
- Data:**
 - CTA Posture: Unknown
 - Disk space available: 0.2 GB of 4.9 GB (4%)
 - Security: Medium
 - Domain: (blank)
 - Folder: Desktop: C:\Documents and Settings\Administrator.BIOHAZARD\Desktop**
 - Folder: Desktop: C:\Documents and Settings>All Users.WINDOWS\Desktop**
 - Folder: Desktop: C:\Documents and Settings\Default User.WINDOWS\Desktop**
 - Folder: Documents: C:\Documents and Settings\Administrator.BIOHAZARD\My Documents**
 - Folder: Documents: C:\Documents and Settings\Default User.WINDOWS\My Documents**
 - Folder: ProgramFiles: C:\Program Files**
 - Folder: ProgramFiles: C:\Program Files\Common Files**
 - Folder: StartMenu: C:\Documents and Settings\Administrator.BIOHAZARD\Start Menu**
 - Folder: StartMenu: C:\Documents and Settings>All Users.WINDOWS\Start Menu**
 - Folder: StartMenu: C:\Documents and Settings\Default User.WINDOWS\Start Menu**
 - Folder: Startup: C:\Documents and Settings\Administrator.BIOHAZARD\Start Menu\Programs\Startup**
 - Folder: Startup: C:\Documents and Settings>All Users.WINDOWS\Start Menu\Programs\Startup**
- Diagnose:** Auto-refresh every 30 seconds
- Host Diagnostic (refreshing in 6 seconds)
- Local intranet

The window also includes a "History" tab and a "Diagnose" button. A vertical scrollbar is visible on the right side of the data section.

191484

Figure 3-11 Host Diagnostics Pop-up Window - <#> Uploads

Management Center for Cisco Security Agents V5.2 - Host Diagnostic - Microsoft Internet Explorer

Diagnostic History Host: biohazard

Received: 11/28/2006 3:06:55 PM

Uploads: 3 uploads

Data:

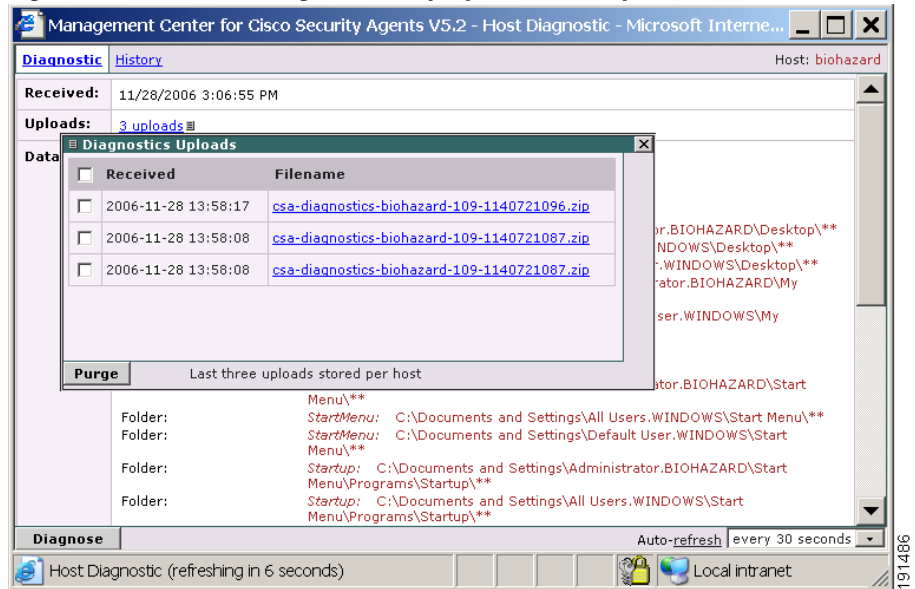
CTA Posture:	Unknown
Disk space available:	0.2 GB of 4.9 GB (4%)
Security:	Medium
Domain:	
Folder:	Desktop: C:\Documents and Settings\Administrator.BIOHAZARD\Desktop**
Folder:	Desktop: C:\Documents and Settings\All Users.WINDOWS\Desktop**
Folder:	Desktop: C:\Documents and Settings\Default User.WINDOWS\Desktop**
Folder:	Documents: C:\Documents and Settings\Administrator.BIOHAZARD\My Documents**
Folder:	Documents: C:\Documents and Settings\Default User.WINDOWS\My Documents**
Folder:	ProgramFiles: C:\Program Files**
Folder:	ProgramFiles: C:\Program Files\Common Files**
Folder:	StartMenu: C:\Documents and Settings\Administrator.BIOHAZARD\Start Menu**
Folder:	StartMenu: C:\Documents and Settings\All Users.WINDOWS\Start Menu**
Folder:	StartMenu: C:\Documents and Settings\Default User.WINDOWS\Start Menu**
Folder:	Startup: C:\Documents and Settings\Administrator.BIOHAZARD\Start Menu\Programs\Startup**
Folder:	Startup: C:\Documents and Settings\All Users.WINDOWS\Start Menu\Programs\Startup**

Diagnose Auto-refresh every 30 seconds

Host Diagnostic (refreshing in 6 seconds) Local intranet

191485

Figure 3-12 Host Diagnostics Pop-up Window - Uploads Window

**Note**

Host diagnostics are available locally to the Windows end user 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.

Host diagnostics are available locally to the UNIX and Linux end user by executing the `./diag` shell script from the `/opt/CSCOCsa/bin` directory. This creates a `csa-diagnostic.gz` file in the `/tmp` directory.

Host **History** information is also available from the Host Diagnostics pop-up window. The feature itself (the collection of host history data) is enabled and disabled from the Status Summary page. Clicking the **History** link at the top of the Host Diagnostics pop-up window takes to a page that provides the following types of information: host registration, test mode setting changes, learn mode setting changes, IP address changes, CTA posture changes, CSA version changes, host active/inactive status changes.

When you enable Host history collection, a two week history of the previously listed host status changes is maintained for every host registered with the MC.

You may want to use these various types of agent diagnosis information in conjunction with the **Reset Cisco Security Agent** option available from the host **Quick Links** section. This way, you can reset the values that you are viewing in the host diagnosis window through a combination of polling and clicking between windows.

**Note**

The same Reset Cisco Security Agent functionality is also available on the Groups page (see [Resetting Cisco Security Agents, page 3-8](#) for a description of the available reset options). To centrally reset *all* hosts in a group to the system default settings, use the reset functionality from the Group page. (Note that this reset option is also available locally on the agent system.)

Host Settings

- Polling interval (seconds)—The value shown here indicates the time interval in which this system polls in to the management server. This feature is configurable through the Groups page.
- Send polling hint—This field indicates if the polling hint capability is turned on for the group in which this host is a member. See [Configuring Groups, page 3-4](#) for details on this setting. This field will display “On (unavailable)” if NAT or PAT exists between CSA MC and the agent - preventing the hint message from being received.
- Test Mode—If this host is part of a group operating in "test mode," that information is displayed here. See Test Mode for further information.
- Verbose logging mode—This field can read as either OFF or ON, indicating whether this feature is enabled for this host. This feature is configurable through the Groups page.
- Log deny actions—This field indicates if the Log <all> deny actions capability is turned on for the group in which this host is a member. See [Configuring Groups, page 3-4](#) for details on this setting.

- Filter user info from events—This field indicates if the Filter user from events capability is turned on for the group in which this host is a member. See [Configuring Groups, page 3-4](#) for details on this setting.
- Application Deployment investigation enabled—This appears if application deployment data collection capability, available from the Analysis menu bar item, is enabled on the end user system. If this feature is enabled, you can access analysis reports from a link on this page. If this feature is not enabled, you can enable it from a link here. (You may have to create a new group in order to enable this feature. You can also do that task from a link that appears here.) See [Chapter 13, “Using Cisco Security Agent Analysis”](#) for detailed information on this feature.

Group Membership and Policy Inheritance Table

The group membership and policy inheritance table provides you with a list of hyperlinks to all the groups the host is a member of, the policies attached to those groups, and the rule modules attached to those policies. From these links you can jump to any of the listed security components to learn more about them.

Combined Policy Rules Table

This table provides you with a list of all the rules that affect the host. These combined lists are often quite long for any host. You can filter and sort the rules to get a better understanding of how the rules work.

Searching for Hosts

-
- Step 1** Move the mouse over **Search** in the menu bar and select **Hosts** from the drop-down menu that appears.
 - Step 2** In the search field, enter a string to search for. The search will find hostnames containing this string.
 - Step 3** Refine your search by selecting one additional radio button from the Host Search Criteria Box. The buttons are explained below:

- **Active hosts with the “the latest” or “an old” configuration.** The search finds hosts that poll into the management server at regular intervals and have not missed three polling intervals. The search will find a host with either the “the latest” policy updates or “an old” policy.
- **Active hosts with “software update pending” or “old software.”** This search finds hosts that poll into the management server at regular intervals and have not missed three polling intervals. It will find hosts with Cisco Security Agent software updates pending or hosts with old software.
- **Active hosts with "Disabled, Low, Medium, High" Cisco Security Agent level.** This finds host with the select level set in the agent UI System Security page slide bar.
- **Hosts not actively polling (status unknown).** This search finds hosts that have not polled into the management server in at least one hour or that have missed three polling intervals in a row.
- **Hosts that have not polled for (a specified number) of days.**
- **Unprotected hosts.** This search finds hosts that do not belong to any group or hosts that belong to groups which have no policies attached.
- **Hosts with unsupported platforms.** An unsupported platform is an operating system not listed in the System Requirements section of the “Installing Management Center for Cisco Security Agents.” It is also an operating system running with a service pack not qualified for use with the agent.
- **Hosts using "desktop, server" licenses.** This search finds either all agents running under desktop system licenses or server system licenses.
- **Hosts with or without Cisco Trust Agent installed.** This search finds hosts on which optional Cisco Trust Agent software is or is not installed.
- **Hosts attached to group.** This search finds hosts attached to the one group you pick from the drop down box.
- **Hosts attached to group for <#> of days.** This search finds hosts attached to the one group you pick from the drop down box for the number of days you enter in the available edit field.
- **Hosts running in test mode.** Agents on hosts running in test mode do not deny any action or operation even if an associated policy says it should be denied. Instead, the agent allows the action and logs an event if a deny or query rule is triggered.

- **Hosts in state condition "Insecure boot detected, Untrusted rootkit detected"**. This search finds hosts that are in the system state condition selected. All the possible state conditions are not listed here. The state conditions listed here are persistent and can only be cleared using the Reset function. See [System State Sets, page 5-13](#) for details.
 - **Hosts with BIOS supported boot detection**. This search finds host systems running with a BIOS that supports the "Insecure boot detected" system state functionality. See [System State Sets, page 5-13](#) for details.
 - **Hosts currently using or that have used a particular IP address**.
 - **Hosts without Application Deployment Investigation data upload**. This search finds hosts where the Application Deployment Data collection capability is disabled on the end user system.
 - **All**. This is the default setting. All the hosts, containing the string searched for, will be found.
- Step 4** Use the **Display Hosts** drop-down list box to display only the hosts of a particular operating system or of all operating systems, if you make no other selection.
- Step 5** In the **Preferences** box, select any of the following check-boxes:
- **Show references box**. This box is checked by default. When you include this in your search criteria, you will be able to look up the group memberships of the hosts you found with the search.
 - **Search on description**. If you check the box for this preference, hostnames and description fields are both searched for the string you entered in the search field.
 - **Search all other fields**. Select this checkbox to search all database fields (including the description field) for the string value.
- Step 6** Specify how many search results will be displayed on a page in the **Results per page** field.
- Step 7** Click **Find**. If the search finds matches, the hosts are displayed in a list and the search criteria box is collapsed. If the search finds no matches, the message "No Results Found" is displayed under the search criteria.

Deleting Moved and Migrated Hosts: Overview

Once an agent installs on a host system and registers with CSA MC, that host is not immediately and automatically removed from the CSA MC hosts list if the agent is uninstalled from the system. The host remains in the host list on the MC until you manually purge it or until it becomes inactive (has not polled in for approximately 30 days). Once that 30 days of inactivity time frame has been reached, the Global Event Manager automatically removes the host in question from the visible hosts list.

You should be aware, that when the host is removed from the host list visible on the MC (removed either manually or automatically after 30 days), that host information is still cached by the MC. This cached host information is not visible on MC. This information is kept on hand by the MC in case the host in question does poll in again. If it does, its group membership is re-established.

Therefore, to completely removed a host from the MC, both visible and non-visible cached host information, you must manually purge this data from the Recycle Bin. You could also wait for another 30 days to pass. At that time, the MC purges all cached references to the host in the Recycle Bin. Additionally, you may want to purge the Recycle Bin if you expect a new agent to be installed on a system where an inactive or uninstalled agent once resided and you do not want the old host grouping to apply to the new host when it registers. Lastly, purging old, cached host information may improve CSA MC rule generation performance.

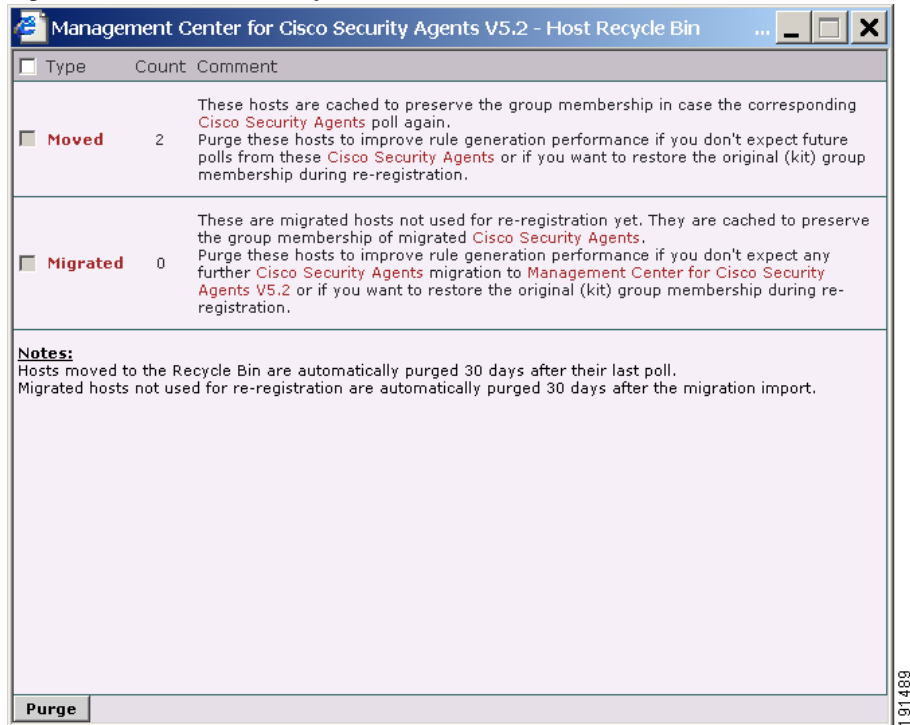
The Recycle Bin

The recycle bin window is available from the Hosts list page. To manually move hosts to the recycle bin, you must select the checkbox beside the host in question and click the **Move to Recycle Bin** button. This is how you remove an inactive or irrelevant host from the Hosts list. If you do not perform this task manually, as mentioned earlier, hosts that have been inactive for 30 days are automatically moved the recycle bin. When you click the **View Recycle Bin** button on the Host lists page, a pop-up window appears. A count of inactive hosts that have been moved either manually or automatically is displayed. You can select the checkbox beside the **Moved** category and click the **Purge** button available in this window to completely delete all host information on the “moved” hosts.

The other category of hosts shown in the recycle bin are **Migrated** hosts. If you’ve upgraded to the current version of CSA MC from a previous version of the product, you ran a migration script to move previous host/group information to the

new MC. Once the new MC has the host migration information, it waits for the migrated hosts to poll in and re-register. This occurs after the hosts have received a software update, installed that update, and began pointing to the new MC. Therefore, the “Count” in the migration category will be quite high after the migration first occurs. That number then decrements as the hosts receive software updates and register with the new MC. You are given the ability to purge hosts that may remain in the Migrated count long after all migrated host registration should have occurred. This lets you clean up old host data that may have migrated over but is not longer in use. Simply select the checkbox beside the Migrated category and click the Purge button to completely delete that migrated host information.

Figure 3-13 Hosts Recycle Bin



1 01 483

Moving Hosts to the Recollect Bin Using the Host List Page

Use this procedure to manually move hosts to the Recycle Bin and then permanently purge them.

- Step 1** Move your mouse over **Systems** in the menu bar and click **Hosts** in the drop-down menu.
- Step 2** (Optional) Sort the host list by operating system to find the correct host to remove.
- Step 3** (Optional) Sort the hosts using the hosts statuses in the Architecture drop-down list box to find the correct host to remove.
- Step 4** From the host list page there are two ways to remove hosts.

- Select the checkbox next to the hostname(s) you want to remove and then click **Move to Recycle Bin**. When prompted, make sure you are moving the correct host(s) and click **OK** to move the host(s) to the recycle bin.
- From the host list page, click the link to a host. Review the host details (see [Figure 3-9](#)) to make sure you are removing the correct host and then click **Move to Recycle Bin**. When prompted, make sure you are moving the correct host and click **OK** to move the host.

The Recycle Bin maintains a cache of moved hosts. Click the **View Recycle Bin** button on the Hosts list page to view the “count” of moved hosts. You must purge those hosts from the Recycle Bin page to completely remove all data on the hosts in question from the MC. See [The Recycle Bin, page 3-38](#) for details.

Moving Hosts to the Recycle Bin that Meet a Search Criteria

Use this procedure to manually move hosts to the Recycle Bin and then permanently purge them.

-
- Step 1** Use the procedure “[Searching for Hosts](#)” section on page 3-35 to find the hosts you want to move and purge.
 - Step 2** Click the checkboxes next to specific hosts to act on those hosts alone, or leave all the boxes unchecked to act on all the hosts found by the search.
 - Step 3** Click the **Operations** button at the bottom of the search results list page. (See [Figure 3-16](#).) The Host Operations Box opens. (See [Figure 3-17](#))
 - Step 4** In the **Available Operations** drop-down list box, select **Move to Recycle Bin**.
 - Step 5** In the Move to Recycle Bin drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
 - Step 6** Click **Execute**. This function moves hosts to the recycle bin.

When prompted, click **OK** to perform the operation or **Cancel** not to perform the operation.

The Recycle Bin maintains a cache of moved hosts. Click the **View Recycle Bin** button on the Hosts list page to view the “count” of moved hosts. You must purge those hosts from the Recycle Bin page to completely remove all data on the hosts in question from the MC. See [The Recycle Bin, page 3-38](#) for details.

Changing Host Memberships in Groups

When a host registers with CSA MC, it is automatically placed into the group(s) you designate for it. There is no need to add a host to a group initially. You only need to add hosts to groups when you are changing their group designation after they have registered.

Hosts may belong to multiple groups and receive policies that are attached to every group to which they belong. Removing hosts from a group removes the protection the hosts received from the various policies associated with that group.



Caution

You can add or remove hosts from a group at any time. If you do change host group assignments, the policy configuration of a host that has been moved to another group will not take effect until you generate your rule programs and distribute them.



Note

See [Viewing Host Details, page 3-25](#) for details on hosts.

There are several ways to change the host memberships in a group:

- [Modifying the Group Membership of a Single Host](#)
- [Modifying the Host Membership in a Single Group](#)
- [Bulk Transferring Hosts From One Group to Another](#)
- [Modify Groups With Hosts That Meet a Search Criteria](#)

Modifying the Group Membership of a Single Host

Use this procedure to add a host to, or remove a host from, various groups.

- Step 1** Move the mouse over **Systems** in the menu bar and select **Hosts** from the drop-down menu. This shows you the host list view; it is a list of all the hosts managed by CSA MC.
- Step 2** Click the link for the host whose group membership you want to modify.

- Step 3** Click **Modify group memberships** in the Quick Links box. This takes you to a swap box page containing a list of groups of which the host is **not** a member on the left and a list of groups of which the host **is** a member on the right.
- Step 4** Add or remove your host to groups:
- To add your host to a group, select a group in the left swap box and click the **Add** button. The group now appears in the right swap box with the other groups to which the host belongs.
 - To remove your host from a group, select a group in the right box and click the **Remove** button. The group now appears in the left swap box with the other groups to which the host does not belong.
- Step 5** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships. When a host polls in to CSA MC, it will receive the group membership changes along with updates to any rules it now follows.

**Note**

Note: You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

Modifying the Host Membership in a Single Group

Use this procedure to add or remove hosts from a single group.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears. This shows you the group list view; it is a list of all the groups managed by CSA MC.
- Step 2** From the group list view, click the link for the group to which you want to add or remove hosts. This brings you to that group's edit view.
- Step 3** From the edit view, click the **Modify host membership** link in the Quick Links box. This takes you to a swap box page containing a list of host systems that **are not** members of the group on the left and a list of hosts that **are** members of the group on the right.
- Step 4** Add or remove hosts to this group (see [Figure 3-14](#)):
- To add a host to this group, select the host in the left box and click the **Add** button. The host now appears in the right box with the list of all hosts attached to this group. The host is now a members of the group.
 - To remove hosts from this group, select the host in the right box and click the **Remove** button. The host now appears in the left box with the list of all hosts unattached to this group. The host is now not a member of this group.

In either case, to select multiple nonsuccessive items in a swap box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key while you click on the item in question. Click the **Select all** link beneath the swap box to select all items in the swap box. When you click the Add or Remove button, all selected items are added or removed.

- Step 5** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships. When a host polls in to CSA MC, it receives the group membership changes along with updates to any rules it now follows.

**Note**

You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

Bulk Transferring Hosts From One Group to Another

Use the bulk transfer feature to easily move or copy all hosts from one group into the Group you are currently viewing.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears. This shows you the group list view; it is a list of all the groups managed by CSA MC.
 - Step 2** From the group list view, click the link for the group to which you want to add or remove hosts. This brings you to that group's edit view.
 - Step 3** From the edit view, click the **Modify host membership** link in the Quick Links box. This takes you to a swap box page containing a list of host systems that **are not** members of the group on the left, and a list of hosts that **are** members of the group on the right.

The bulk transfer operations are at the bottom of this page. (See [Figure 3-14](#).)

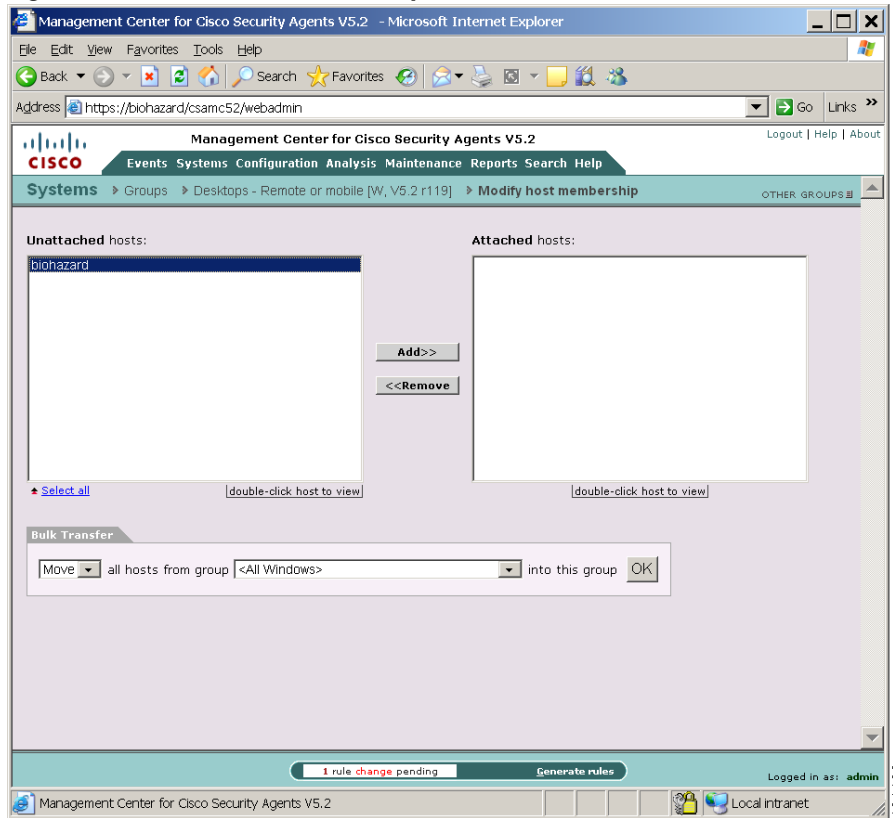
- Step 4** In the Bulk Transfer box, select **Move** or **Copy** in the first drop-down list box to move hosts or copy hosts, from the group you specify to the group whose membership you are modifying.
- Step 5** In the second drop-down list box, select the group whose members will be moved out of or copied to the group whose membership you are modifying.
- Step 6** Click **OK**. The hosts you moved or copied now appear in the right swab box with the list of hosts attached to this group. The hosts you moved or copied are now members of the group.
- Step 7** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships and when a host polls in to CSA MC, it receives the group membership changes along with updates to any rules it now follows.



Note Note: You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

When you next click the **Generate** button, policies associated with this group will no longer be applied to the removed hosts. (The host is not deleted from the database, it is just no longer part of the group.)

Figure 3-14 Add Hosts to Group



191490

Modify Groups With Hosts That Meet a Search Criteria

Use this method to find all the hosts that match a certain criteria and move them in and out of groups.

-
- Step 1** Use the procedure “[Searching for Hosts](#)” section on page 3-35 to find the hosts whose group memberships you want to change.
- Step 2** Click the checkboxes next to specific hosts to act on those hosts alone, or leave all the boxes unchecked to act on all the hosts found by the search.
- Step 3** Click the **Operations** button at the bottom of the search results list page. (See [Figure 3-16](#).) The Host Operations Box opens. (See [Figure 3-17](#))
- Step 4** In the Available Operations drop-down list box, select one of the following options:
- **Move to Recycle Bin.** This function allows you to move hosts to the Recycle bin for the purpose of deleting those hosts from the local database. In the Move to Recycle Bin drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
 - **Attach to group.** This function copies hosts from one group to another.
 - In the Attach (if applicable) drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
 - In the **to the following group** drop-down list box, select the group to which you want to add the hosts.
 - **Detach from group.** This function removes hosts from a group.
 - In the Detach (if applicable) drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
 - In the **from the following group** drop down list-box, select the group from which you want to remove the hosts.
- Step 5** Click **Execute**.
- Step 6** When prompted, click **OK** to perform the operation or **Cancel** not to perform the operation. You receive a message confirming the success or failure of the operation.

Figure 3-15 Hosts Search Page

The screenshot displays the 'Hosts Search Page' within the 'Management Center for Cisco Security Agents V5.2' web application. The browser window title is 'Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer'. The address bar shows the URL: `https://biohazard/csamc52/webadmin`. The application header includes the Cisco logo and navigation links: 'Events Systems Configuration Analysis Maintenance Reports Search Help'. The current page is 'Search > Hosts'.

The main content area features a search interface with a text input field and a 'Find' button. Below this is the 'Host Search Criteria' section, which contains several radio button options and dropdown menus for filtering hosts:

- Active hosts with [the latest] configuration
- Active hosts with [software update pending]
- Active hosts with [Disabled] Cisco Security Agent security level
- Hosts not actively polling (status unknown)
- Hosts that [have not polled for] [1] day
- Unprotected hosts
- Hosts running [unsupported platform - 0 hosts]
- Hosts using [desktop] licenses
- Hosts [with] [Cisco Trust Agent active and posture <Don't care>]
- Hosts attached to group [<All Linux>]
- Hosts attached to group [<All Linux>] for more than [7] days
- Hosts running in [test mode]
- Hosts in state condition [Insecure boot detected]
- Hosts with BIOS supported boot detection
- Hosts [currently using] at least one IP address [containing] []
- Hosts without Application Deployment Investigation data upload
- Hosts that have been reimaged
- All

At the bottom of the search criteria section, there is a 'Display' field set to 'All' hosts running [<Any>] version.

To the right of the search criteria is a 'Preferences' sidebar with the following options:

- Show references
- Search on description
- Search all other fields
- Results per page: [50]

The bottom status bar shows 'No rule changes pending', a 'Generate rules' button, and 'Logged in as: admin'. The system tray at the bottom right indicates 'Local intranet' and the time '19:14:73'.

Figure 3-16 Hosts List Page

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

Address: https://biohazard/csamc52/webadmin

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Search > Hosts

host105 Find

Host Search Criteria [change]
All hosts (Windows)

Displaying 1 - 50 of 65 results

1 2 Next

#	Name	Description	Reference list
1	host10540 [W]	Description for host 10540	Groups
2	host10541 [W]	Description for host 10541	Groups
3	host10542 [W]	Description for host 10542	Groups
4	host10543 [W]	Description for host 10543	Groups
5	host10544 [W]	Description for host 10544	Groups
6	host10545 [W]	Description for host 10545	Groups
7	host10546 [W]	Description for host 10546	Groups
8	host10547 [W]	Description for host 10547	Groups
9	host10548 [W]	Description for host 10548	Groups
10	host10549 [W]	Description for host 10549	Groups
11	host1055 [W]	Description for host 1055	Groups
12	host10550 [W]	Description for host 10550	Groups
13	host10551 [W]	Description for host 10551	Groups

Operations 5 rule changes pending Generate rules Logged in as: admin

Management Center for Cisco Security Agents V5.2 Local intranet

191491

Figure 3-17 Host Operations Box

191488

Host Managing Tasks

The configuration options on the Host Managing Tasks page let you add, move, and remove hosts from selected groups at set times so that the action occurs automatically. Using a configured, automatic, management task could be useful in various recommended scenarios. For example, you're conducting a pilot of the product and you want all newly registered hosts to remain in a group that has test mode (see [Using Test Mode, page 5-7](#)) enabled for certain period of time before those hosts move to a group that is not in test mode. Having this group movement occur automatically can reduce the administrative burden of having to manually do this. Especially, if it is your policy to have all new hosts start off in test mode.

This same scenario can be applied to using learn mode (see [Using Learn Mode, page 5-11](#)). Rather than having to remember to move hosts out of a group with learn mode enabled or having to remember to turn learn mode off, you can use a host managing task to do this automatically when scheduled.

Configure a host managing task to automatically add, move, or remove hosts as follows:

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Host Managing Tasks** from the drop-down list that appears. The list of existing tasks (if any) is displayed.
- Step 2** Click the **New** button to create a new task. The host managing tasks configuration page appears. See [Figure 3-18](#).
- Step 3** In the available fields, enter the following information:
- **Name**—This is a unique name for this task. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, hyphens, and underscores.
 - **Description**—This description appears in the list view to help you identify this particular task.
- Step 4** In the **Configuration** section of the page, select a combination of the following options:
- **Run this task every**
Select one or more days of the week to run this task. You can also specify a certain time to run the task. If you do not specify a time (note that it's a 24 hour clock), the default time is midnight.

- **Add** hosts from group <group name> to group <group name> if they have been part of the source group for more than <number> of days.

Use the **Add** checkbox option to put all hosts in an additional group without removing them from their current group. This addition to the selected group occurs only if the hosts have been part of the original group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Move** hosts from group <group name> to group <group name> if they have been part of the source group for more than <number> of days.

Use the **Move** checkbox option to migrate all hosts from the current specified group to another specified group. This moving of hosts from the selected group and the addition of those hosts to another group occurs only if the hosts have been part of the original group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Remove** hosts from group <group name> if they have been part of this group for more than <number> of days.

Use the **Remove** checkbox option to take all hosts from the current specified group out of that group. This removal of hosts from the selected group occurs only if the hosts have been part of that group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Regenerate** rule programs.

Agents do not receive most CSA MC configuration changes unless rules are generated after the changes are made. Therefore, if you configure a task to occur at a certain day and time and you want agents to pull the group configuration changes down when they occur, you must select this checkbox to generate rules as part of the task. If you do not select this checkbox, configuration changes that require a rule generation are only made on the MC and are not received by agents until a manual rule generation is performed.

Step 5 Click the **Save** button.

Click the **Execute now** button to immediately run the configured task.

Figure 3-18 Host Managing Tasks

The screenshot displays the Management Center for Cisco Security Agents V5.2 web interface. The browser address bar shows the URL `https://biohazard/csamc52/webadmin`. The page title is "Management Center for Cisco Security Agents V5.2". The navigation menu includes "Events", "Systems", "Configuration", "Analysis", "Maintenance", "Reports", and "Search Help". The current page is "Systems > Host Managing Tasks > Remove hosts from (Systems - Learn mode (W))".

The configuration page for the task "Remove hosts from (Systems - Learn mode (W))" is shown. The task version is 5.2 r119. The description is "Limit learning to 14 days". The task is enabled.

Configuration

Run this task every

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

At 01:00

Add hosts from group - select source group - to group - select destination group - if they have been part of the source group for more than 7 days.

Move hosts from group - select source group - to group - select destination group - if they have been part of the source group for more than 7 days.

Remove hosts from group Systems - Learn Mode [W, V5.2 r119] [learn] if they have been part of this group for more than 14 days. [Matching hosts: 0]

Regenerate rule programs.

Notes: A host is considered part of a group after it is added to the group and rules are generated and deployed to the host. If you wish an operation to proceed regardless of how long a host has been a member of the source group, use a value of 0 (zero).

Previous execution: N/A
Next execution: Tomorrow, at 01:00

Buttons: Save, Execute now, Delete. Status: 1 rule change pending. Generate rules. Logged in as: admin. Local intranet.

191487

Distributing Software Updates

Cisco provides software updates via its web site (www.cisco.com) for both CSA MC and the agent. You can download these updates, install them on CSA MC, and then distribute them to agent systems across your network as easily as you deploy new rule programs. When you download a self-extracting executable update and install it on the server system, the agent software update files get placed under **Available Software Updates** in CSA MC (accessible from **Systems>Software Updates** in the menu bar).

From the list of available updates that is created in the Available Software Updates page, you can make the appropriate updates available to agents through the Scheduled Software Updates page. Creating Scheduled Software Updates allows you to distribute updates to designated groups of agent systems. See [Configuring Scheduled Software Updates, page 3-56](#) for details.

**Note**

All “Quiet” Windows and Linux updates begin installing automatically during the designated installation window with no action occurring on the part of the end user.

From the Available Software Updates page, you can click on a particular update and view the following information (see [Figure 3-19](#)):

- Name of the software update, for example SP 5.2.0.102
- Description of the software update, for example Service Pack for agent on NT and Win2K, Windows XP, Windows 2003
- File, a link to the software update file itself on the server system
- Target system, a description of the system type for which the update is issued (agent and/or server)
- Version, this is the version of the software update
- Operating system, the operating system for which the update is issued
- Operating system version(s), the exact OS version numbers for which the update is issued

Figure 3-19 Available Software Updates Page

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface in Microsoft Internet Explorer. The browser address bar shows `https://biohazard/csamc52/webadmin`. The page title is "Management Center for Cisco Security Agents V5.2". The navigation menu includes "Events", "Systems", "Configuration", "Analysis", "Maintenance", "Reports", "Search", and "Help". The breadcrumb trail is "Systems > Software Updates > Available Software Updates > Update V5.2.0.119".

Name	Update V5.2.0.119
Description	Service pack for agent on Windows NT, Windows 2000, Windows XP and Windows 2003
Target systems	Cisco Security Agent (versions 5.2.0.1 - 5.2.0.118)
Version	5.2.0.119
Operating system	Windows 2000 , Windows 2003 , Windows NT , Windows XP
Operating system version(s)	Windows 2000 (5.0.4.2195 , 5.0.3.2195 , 5.0.2.2195 , 5.0.1.2195 , 5.0.0.2195) , Windows 2003 (5.2.1.3790 , 5.2.0.3790) , Windows NT (4.0.6.1381 , 4.0.5.1381) , Windows XP (5.0.1.2600 , 5.1.0.2600 , 5.1.1.2600 , 5.1.2.2600)

At the bottom of the page, there is a "Delete" button, a status bar indicating "1 rule change pending", and a "Generate rules" button. The user is logged in as "admin". The footer of the page shows "Management Center for Cisco Security Agents V5.2" and "Local Intranet".

191480

Configuring Scheduled Software Updates

Create Scheduled Software Updates to distribute an update or updates you have available in Available Software Updates to a selected group or groups.

To create Scheduled Software Update for distribution to agent systems, do the following.

-
- Step 1** From the menu bar **Systems** drop-down list, move the mouse over **Software Updates**. A cascading menu with further selections appears. Select **Scheduled Software Updates** (see [Figure 3-20](#)).
 - Step 2** Click the **New** button to create a new entry. This takes you to the update configuration page.
 - Step 3** Enter a **Name** for the update that makes it easily identifiable.
 - Step 4** Enter a **Description**. This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.
 - Step 5** Select the **Target operating system** for the update you're distributing (Solaris, Linux, or Windows). When you select an OS, the available updates and selectable groups change accordingly.
 - Step 6** From the **Software update** pulldown list, select the Solaris, Linux, or Windows update you want to distribute. Generally, it's called something like Update V5.2.0.102.
 - Step 7** **Enable update for hosts in selected groups** From the available list of groups, select one or more to distribute this update to.
 - Step 8** To select multiple items in a list box, hold down the Ctrl key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the Shift key to select multiple successive items.
 - Step 9** **Update time** Enter a time frame during which agent systems can receive and install updates. By default, the time frame is set to "any time" or for 24 hours. This way, users will update at any time you choose. If you put a time limit on the update, for example enter 10:00 to 11:00 (this would be AM), then after 11:00, if the user is not logged in during this hour window, the update would not be available again until the same time the next day.
 - Step 10** "Quiet install" updates begin installing automatically with no action occurring on the part of the end user. A reboot on the agent system is not required after a software update. Security continues to be enforced after an update, but if the

system is not rebooted, configuration changes and other changes are not applied. They are only applied on the next reboot. You can control what the end user sees during an update and whether a reboot is required after an update by using the following checkboxes.

- **Force reboot after install** (available for Windows and Linux): If you select this checkbox, when the update completes, a message appears to the end user warning that the system will automatically reboot in 5 minutes. This reboot cannot be stopped by the end user. Keep in mind, if you are selecting to force a reboot, the update must also be "Quiet". Therefore, regardless if the end user is present or not, if the machine is running and a quiet update with a forced reboot is received, both the install and the automatic reboot take place within the time frame specified in the update. (Generally, you will only want to use a quiet install with a forced reboot for an unattended server so that the update is installed and the system is rebooted without a user having to be present at the server.)
- **Quiet install** (available for Windows and Linux): If you select this checkbox, when the update completes, no prompt is displayed to the user. Therefore, since the update begins without prompting the user, this quiet install update occurs as a completely transparent process. The user does not know that a software update has occurred. Configuration changes provided in the update will take effect when the system is next rebooted.
- **Noisy install** (implied by no checkbox selection): If you do not select the Quiet install checkbox, and the end user has an agent UI, the end user is prompted that an update is available. The user can start the update at that time or postpone it.

**Note**

Software update functionality and prompt options occur regardless of Agent UI configurations on the end user system. Therefore, if you have deployed agents with no UI, you can deploy "noisy" software updates that prompt the end user. These functions are independent of each other. So, if you want all agent functions to be invisible to the end user, you should configure your update accordingly. (Note that there is one exception to this statement. If the end user does not have an agent UI and you deploy a "noisy" update, the option to postpone the update will not appear. The update will behave as though it were "quiet.")

These possible checkbox options would be combined for the following effects once the software update has completed:

Table 3-1 Software Update Reboot/Install Options

Force reboot checkbox=enabled Quiet install checkbox=enabled	The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes. (This combination is recommended for unattended servers.)
Force reboot checkbox=disabled Quiet install checkbox=enabled	The install ends quietly with no prompts. Therefore, the update is completely transparent to the end user. The update takes effect the next time the user happens to reboot.
Force reboot checkbox=disabled Quiet install checkbox=disabled	The install prompts the user that an update is available. The user can update at that time or postpone the update. When the update occurs, the install ends by displaying a prompt indicating that an update has occurred and the end user can reboot the system at his/her convenience to apply the changes.

Step 11 If you are using the Cisco Trust Agent (CTA) in your enterprise, you can use this page to configure a CTA software update in combination with a CSA update or on its own. Refer to your CTA documentation for particular software update information.

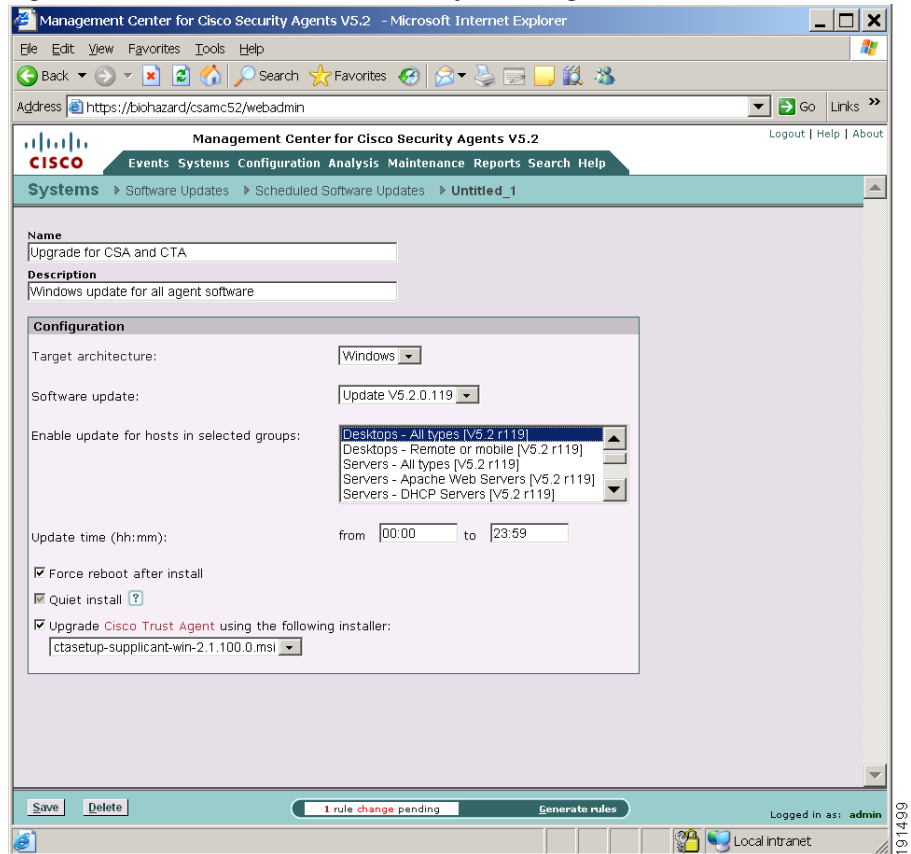
Step 12 Click the **Save** button.

You must Generate rules to deploy software updates to agents.

**Caution**

Once scheduled, Solaris software upgrades must be launched manually by accessing the **csactl** command line tool on the Solaris systems and typing in the software update command. When the update is complete, the system automatically reboots within 5 minutes. This reboot *cannot* be stopped. Therefore, once you launch the Solaris software update, you must understand that the system will reboot when the update completes.

Figure 3-20 Scheduled Software Updates Page



The next time agents poll in to CSA MC, they receive a prompt informing them that a software updated is available.

On Solaris agent systems, use the `csactl` utility to check for software updates and to install them. See [Appendix A, “Cisco Security Agent Overview”](#) for details.

Software Updates in a Distributed Configuration

There are two procedural items to note when installing a software update in a distributed installation environment with multiple MC's.

- In a distributed environment, you *must* install the software update on *all* MC's in your distributed configuration.
- In a distributed environment, when installing, upgrading, or uninstalling any MC in the distributed configuration, the service must be stopped on the other MCs. For example, in a configuration with 2 MCs, you *must* first *stop* the service on one MC before you install the software update on the other MC. Then restart the services.