



CHAPTER 4

Quick Start Configuration

Overview

This chapter provides the basic setup information you need to start using the Management Center for Cisco Security Agents to configure some preliminary groups and build agent kits. The goal of this chapter is to help you quickly configure and distribute Cisco Security Agent kits to hosts and have those hosts successfully register with CSA MC. Once this is accomplished you can configure some policies and distribute them to installed and registered Cisco Security Agents.

For detailed configuration information, you should refer to the User Guide.

This section contains the following topics.

- [Access Management Center for Cisco Security Agents, page 4-2](#)
- [Administrator Roles in CSA MC, page 4-3](#)
- [Administrator Authentication, page 4-3](#)
- [Cisco Security Agent Policies, page 4-4](#)
- [Configure a Group, page 4-5](#)
- [Build an Agent Kit, page 4-7](#)
- [The Cisco Security Agent, page 4-11](#)
- [View Registered Hosts, page 4-12](#)

- [Configure a Rule Module, page 4-13](#)
- [Configure a Policy, page 4-19](#)
- [Attach a Rule Module to a Policy, page 4-20](#)
- [Attach a Policy to a Group, page 4-20](#)
- [Generate Rule Programs, page 4-21](#)

Access Management Center for Cisco Security Agents

Local Access

- To access CSA MC locally on the system hosting CSA MC software, double-click the CSA MC desktop icon created during the installation.

Remote Access

- To access CSA MC from a remote location, launch a browser application and enter

```
http://<system hostname>.<domain>
```

For example, enter `http://stormcenter.cisco.com`

- Enter the administrator name and password created during the CSA MC installation.



Caution

If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Any newly deployed agents will not be able to register with the unlicensed CSA MC. Refer back to [Chapter 3, "Installing the Management Center for Cisco Security Agents"](#) for further licensing information.

Administrator Roles in CSA MC

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CSA MC installation automatically has configure privileges. When you create new administrators on the system, you can give them one of the following roles.

CSA MC Administrator Roles:

- **Configure**—This provides full read and write access to the CSA MC database.
- **Deploy**—This provides full read and partial write access to the CSA MC database. Administrators can manage hosts and groups, attach policies, create kits, schedule software updates, and perform all monitoring actions.
- **Monitor**—This provides administrators with read access to the entire CSA MC database. Administrators can also create reports, alerts, and event sets.

See the *Management Center for Cisco Security Agents User Guide* for Administrator configuration details.

Administrator Authentication

CSA MC allows administrators logging into the system to be authenticated either through the local configuration database or via LDAP authentication. If you intend to use LDAP authentication, LDAP server information must be entered in CSA MC. See the *Management Center for Cisco Security Agents User Guide* for Administrator LDAP authentication details.

Cisco Security Agent Policies

CSA MC default Cisco Security Agent kits, groups, policies, and configuration variables are designed to provide a high level of security coverage for desktops and servers. These default Cisco Security Agent kits, groups, policies, rule modules and configuration variables cannot anticipate all possible local security policy requirements specified by your organization's management, nor can they anticipate all local combinations of application usage patterns. Cisco recommends deploying agents using the default configurations and then monitoring for possible tuning to your environment.

If you are using shipped policies, you can also use shipped, pre-built agent kits. Therefore, if you're not creating your own configurations, you can simply refer to [Chapter 3](#) and [Chapter 10](#) in the User Guide for information on deploying kits to end users and viewing the event log.

**Note**

Each pre-configured rule module, policy, and group page has data in the expandable **+Detailed** description field explaining the item in question. Read the information in these fields to learn about the items described and to determine if the item in question meets your needs for usage.

As a jumping off point for creating your own configurations, the following sections in this manual take you through the step by step process of configuring some of the basic elements you need to initiate server/agent communications and to begin the distribution of your own policies.

Configure a Group

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 Cisco Security Agent kits. When hosts register with CSA MC, they are automatically put into their assigned group or groups. Once hosts are registered you can edit their grouping at any time.

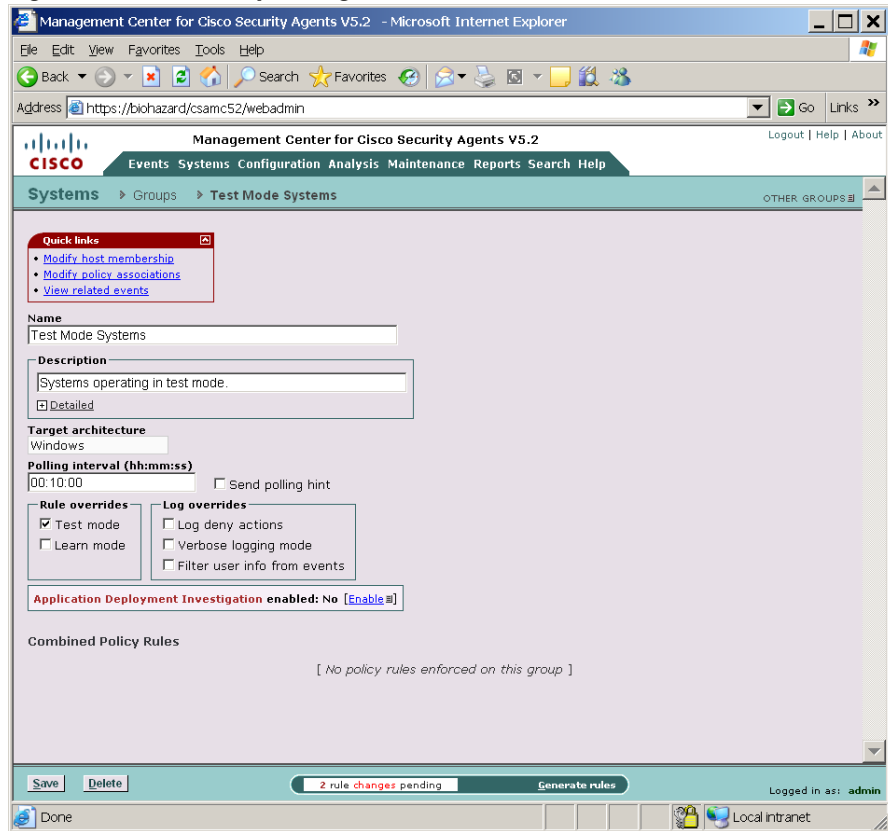
**Note**

Management Center for Cisco Security Agents ships with preconfigured 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 of CSA MC and select **Groups** from the drop-down menu that appears. The Groups list view appears.
- Step 2** Click the **New** button to create a new group entry. You are prompted to select whether this is a Windows, Linux, or Solaris group. For this example, click the Windows button. This takes you to the Group configuration page.
- Step 3** In the available group configuration 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, and underscores.
 - **Description**—This is an optional line of text that is displayed in the list view and helps you to identify this particular group.

Figure 4-1 Group Configuration View



Step 4 Cisco suggests that you select the **Test Mode** checkbox (available from the **Rule overrides** section) for this group. In Test Mode, the policy we will later apply to this group will not be active. In other words, the 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 letting you know the action would have been denied.

Using Test Mode helps you to understand the impact of deploying a policy on a host before enforcing it. If examining the logs shows you that the policy is working as intended on a group, you can then remove the Test Mode designation. For detailed information on **Polling intervals**, **Test Mode**, **Verbose Logging Mode**, **Log deny actions** and **Filter user from events** refer to the User Guide.

Step 5 Click the **Save** button to enter and save your group in the CSA MC database.

191447

Build an Agent Kit

**Note**

The Management Center for Cisco Security Agents ships with preconfigured agent kits you can use to download and install agents if they meet your initial needs (accessible from **System>Agent kits** in the menu bar). There are prebuilt kits for desktops, servers, and others. 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.)

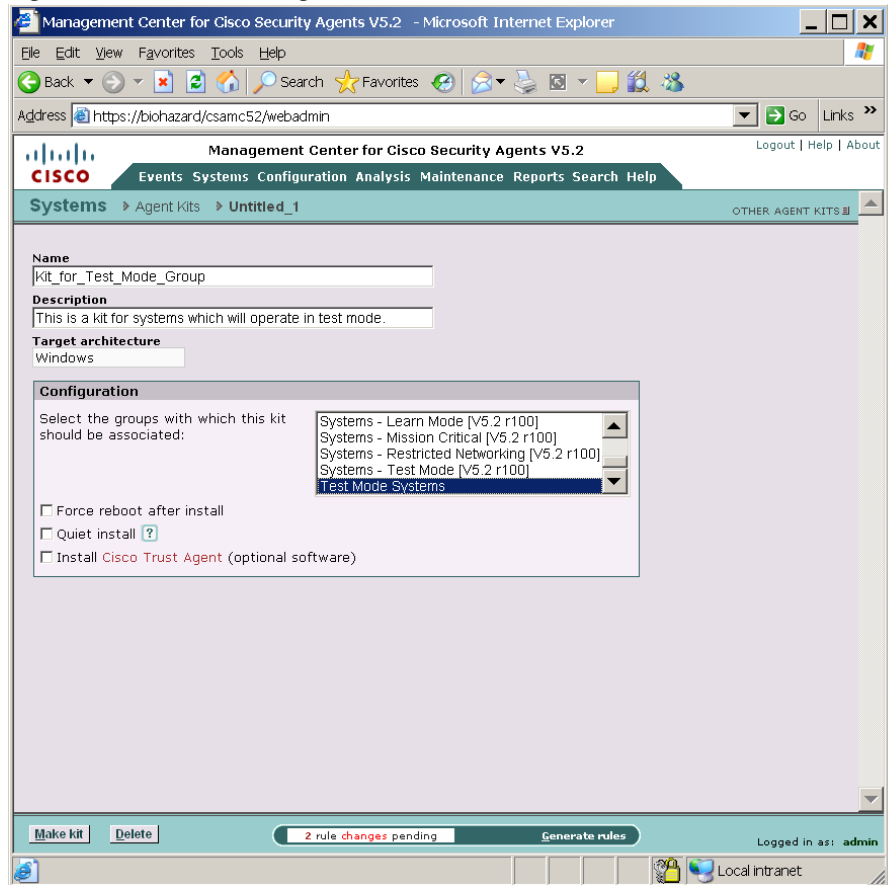
Once you have a group configured, you can build a Cisco Security Agent kit. Hosts on your network will download this kit and use it to install an agent on their system. A group designation is the only information this kit will initially contain for hosts that download and install it.

When an agent is installed on a host, the agent automatically and transparently registers itself with CSA MC. It now appears in the CSA MC database as part of the groups designated in the kit, and will enforce policies that are applied to those groups.

To create a Cisco Security Agent kit, 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. The agent kit list view displays the preconfigured agent kits.
 - Step 2** Click the **New** button to create a new agent kit. You are prompted to select whether this is a Windows, Linux, or Solaris agent kit. For this example, click the Windows button. This takes you to the Agent kit configuration page.
 - Step 3** In the configuration view (see [Figure 4-2](#)), enter a **Name** for the kit. This is a unique name (Agent kit names are an exception. Spaces are not valid name characters for agents kits as they are for other name fields).
 - Step 4** Enter a **Description**. This is an optional line of text that is displayed in the agent kit list view.
 - Step 5** From the available list box, select the groups you are associating with this kit. (The names of the groups you configured in the previous section should appear here.)
 - Step 6** You have the option of forcing systems to reboot after the agent installation completes. 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 User Guide for details.)
 - Step 7** Click the **Make Kit** button in the bottom frame. See [Figure 4-2](#).

Figure 4-2 Create Agent Kit



Once you click the Make Kit button and generate rules, CSA MC produces a kit for distribution (see Figure 4-3). You may distribute the kit download 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 `https://<system name>/csamc52/kits` URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering.

Figure 4-3 Agent Kit Created

The screenshot shows a web browser window titled "Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer". The address bar shows `https://biohazard/csamc52/webadmin`. The page content includes:

- Navigation menu: Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help.
- Breadcrumbs: Systems > Agent Kits > Kit_for_Test_Mode_Group.
- Message: "The agent kit was successfully created."
- Warning box: "Please note that this kit cannot be deployed until after the next rule generation."
- Details:
 - Name: Kit_for_Test_Mode_Group
 - Description: This is a kit for systems which will operate in test mode.
 - Target architecture: Windows
- Agents installed from this kit will be automatically added to the following groups:
 - <All Windows> - Auto-enrollment group for Windows hosts
 - Test Mode Systems - Systems operating in test mode.
- User will be prompted during installation of this kit.
- Footer: "3 rule changes pending", "Generate rules", "Logged in as: admin", "Local intranet".

191441

The Cisco Security Agent

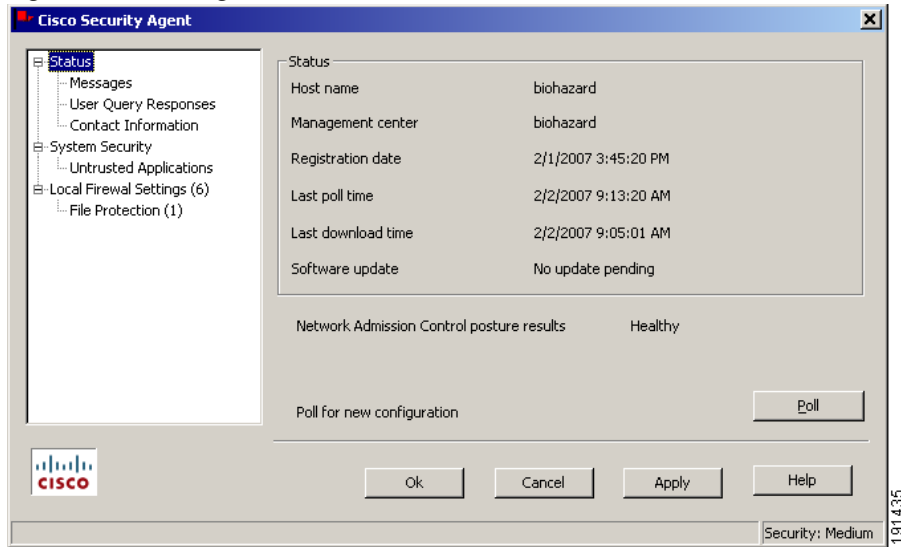
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on supported Windows, Linux, and Solaris platforms. (Note that on Solaris systems there is no agent user interface. See Appendix A in the User Guide for information on the Solaris agent utility.)

Once users successfully download and install Cisco Security Agents, they can optionally perform a reboot for full agent functionality.

When the system restarts, the agent service starts immediately and the flag icon appears in the system tray (if end user systems are configured to have an agent UI). At this time, the agent automatically and transparently registers with CSA MC. Agents are immediately enforcing rules.

To open the agent user interface, end users can double-click on the flag icon in their system tray. The user interface opens on their desktop.

Figure 4-4 Agent Status

**Note**

For detailed information on installing both the Windows and UNIX agents, refer to Appendix A in this manual or in the User Guide.

View Registered Hosts

From CSA MC, you can see which hosts have successfully registered by accessing **Hosts** from the **Systems** link in the menu bar. This takes you to the **Hosts list** page. On the right side of this page is a column that displays varying types of information on each host. Use the pulldown menu for this column to filter your host list based on the status in question.

To search for specific hosts based on more status data, use the **Search** option in CSA MC. Search for Hosts using available status information such as:

- Active hosts—A host is active if it polls into CSA MC at regular intervals.
- Not active hosts—A host is inactive if it has missed a certain number polling intervals or if it has not polled into the server for at least one hour.

You can also view registered hosts by accessing the Groups page. From the groups list view, click the link for the group you created in the previous sections. Now click the **Modify host membership** link. All hosts who installed the kit created using this group should appear here as part of the group. (You might want to click the Refresh button on your browser to ensure you are viewing updated information.)

Configure a Rule Module

This section provides brief instructions for configuring and distributing a policy to Cisco Security Agents. For a full discussion of rule modules and policies, you should refer to the User Guide. In the meantime, use the following instructions to distribute a fairly simple policy to the agents that are currently installed on end user systems.

When you configure a policy, you are combining rule modules under a common name. Those rule modules are then attached to a policy. That policy is attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts.

For this example, we will configure a rule module containing file access control rule that protects systems from a known email virus. In this example, a VBS file (badfile.vbs) is detected, correlated across systems, and quarantined by CSA MC. This quarantine list updates automatically (dynamically) as logged quarantined files are received. You can use a file access control rule to permanently quarantine a known virus as shown in this example.



Note

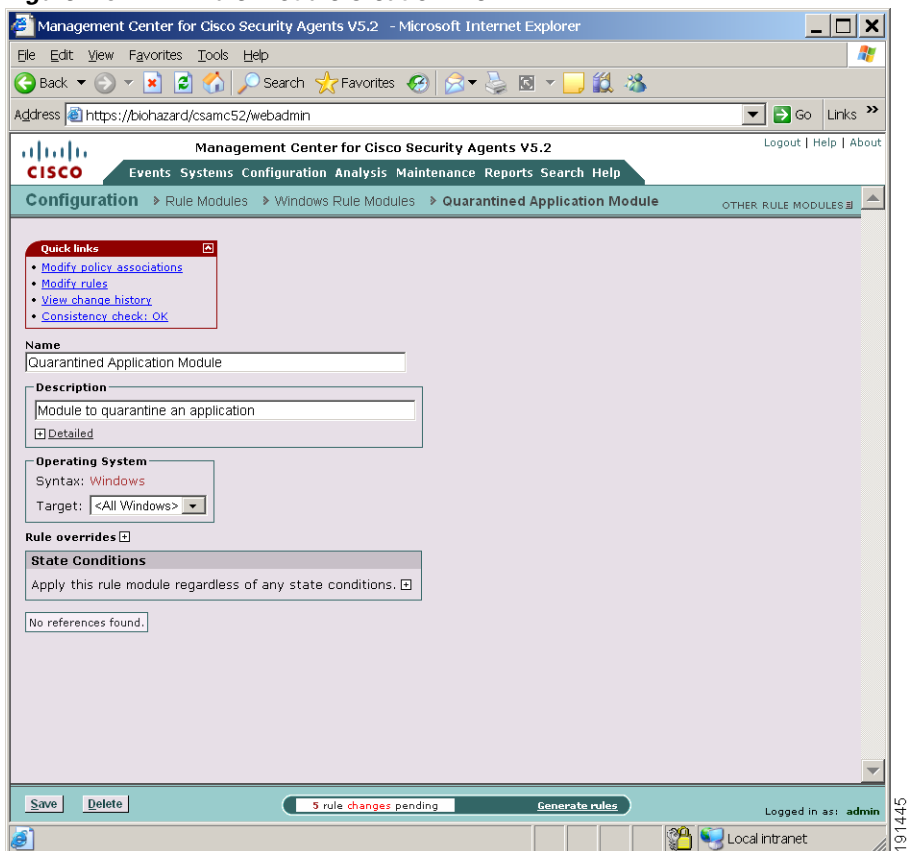
Cisco recommends that you do not edit the preconfigured policies shipped with the Management Center for Cisco Security Agents, but instead add new policies to groups for any changes you might want.

To configure this file quarantine rule module, do the following.

-
- Step 1** Move the mouse over **Configuration** in the menu bar and select **Rule Modules [Windows]** from the drop-down list that appears. The Windows Rule Module list view appears.
 - Step 2** Click the **New** button to create a new module. This takes you to the Rule Module configuration page. See [Figure 4-5](#).

- Step 3** In the configuration view, enter the **Name** *Quarantined Application Module*. Note that names are case insensitive, must start with an alphabetic character, can be up to 64 characters long. Spaces are also allowed in names.
- Step 4** Enter a **Description** of your module. We'll enter *Module to quarantine an application*.
- Step 5** Click the **Save** button. (We will not use State Sets in this example.)
Now we add our file access rule to this module.

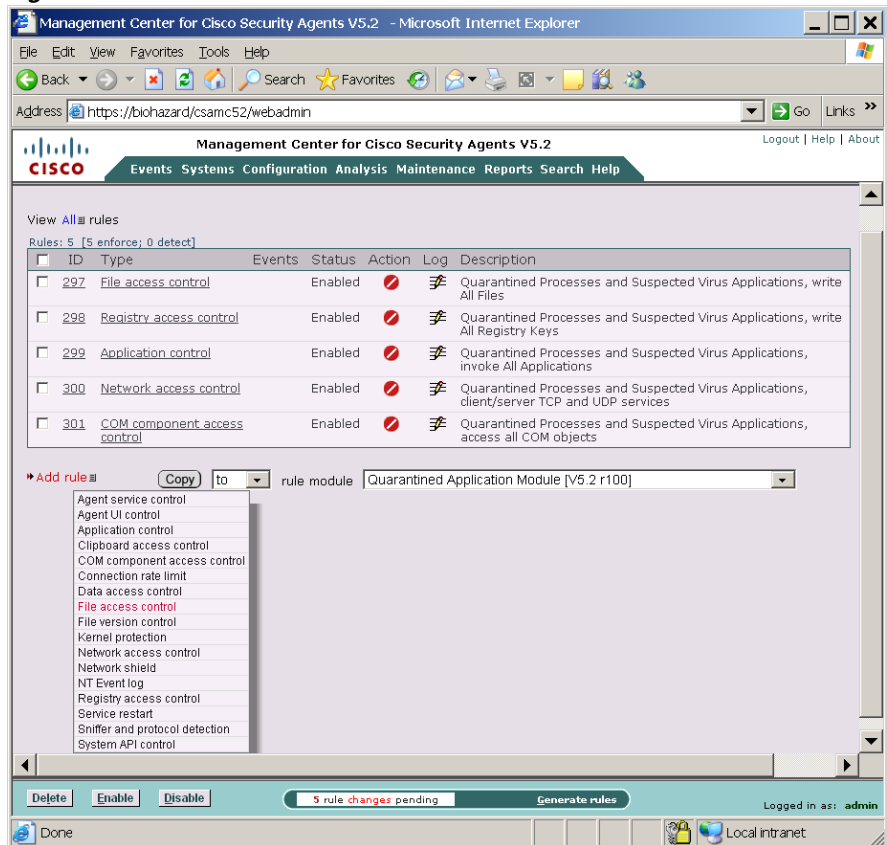
Figure 4-5 Rule Module Creation View



Create a File Access Control Rule

- Step 1** From the Rule Module configuration page (Figure 4-5), click the **Modify rules** link at the top of the page. You are now on the Rules page.
- Step 2** In the Rule page, click the **Add rule** link. A drop down list of available rule types appears.
- Step 3** Click the **File access control** rule from the drop down list (see Figure 4-6). This takes you to the configuration page for this rule.

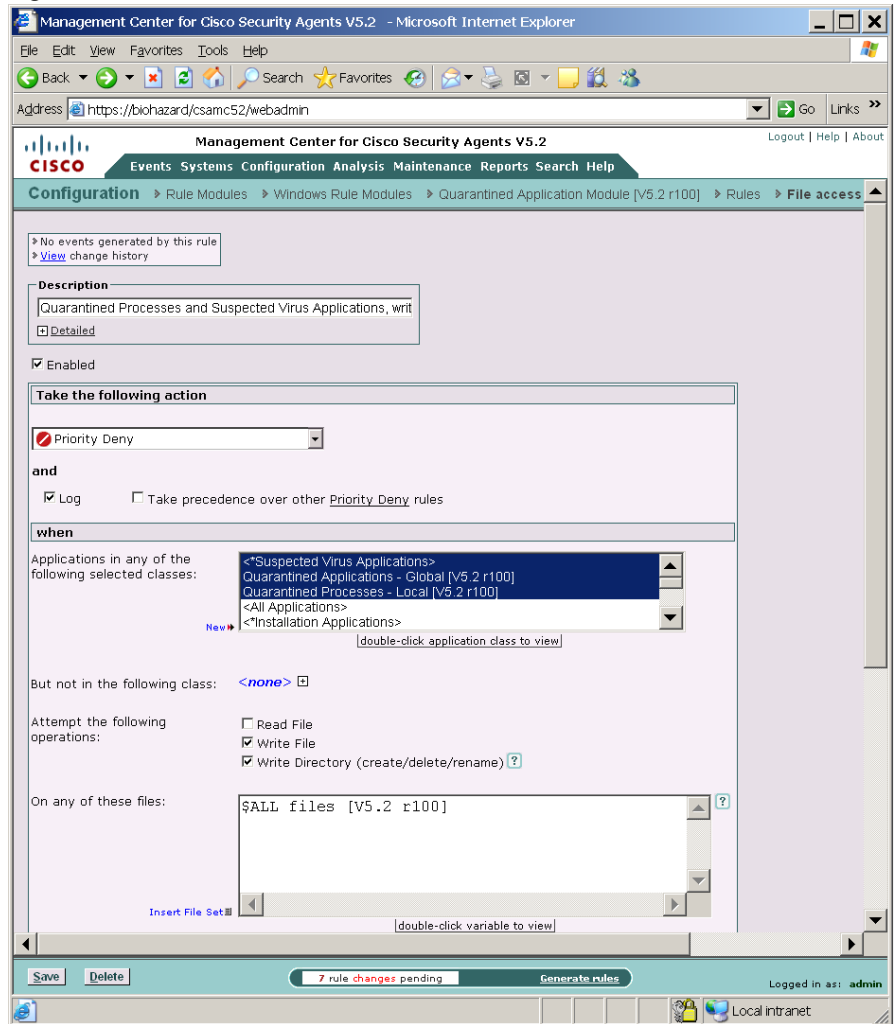
Figure 4-6 Add Rules to Module



- Step 4** In the File access control rule configuration view (see Figure 4-7), enter the following information:
- **Description**—Quarantined and Suspected Virus Applications, write All Files
 - **Enabled**—(This is selected by default. Don't change this setting for this example.)
- Step 5** Select **Priority Deny** from the action pulldown list. By selecting Priority Deny here, we are stopping the quarantined applications we're going to specify later from performing a selected operation on the files we will indicate. By default, when you create a deny rule, all other actions are allowed unless specifically denied by other rules. See the User Guide for information on allow/deny specifics.

- Step 6** Select the **Log** checkbox.
This means that the system action in question is logged and sent to the server. Generally, you will want to turn logging on for all deny rules so you can monitor event activity.
- Step 7** Select a preconfigured Application class from the available list to indicate the applications whose access to files we want exercise control over. For this rule, we'll select **Quarantined applications**. Note that when you click Save, selected application classes move to the top of the list.
- Step 8** Select the **Write File** and **Write Directory** checkboxes to indicate the actions we are denying.
- Step 9** Now we'll enter the system files we are protecting with this rule. In the files field, enter \$All files available from the **Insert File Set** option.
- Step 10** Click the **Save** button.
Next, we will create a policy to attach our rule module to.

Figure 4-7 File Access Control Rule



191446

Configure a Policy

Generally, when you configure a policy, you are combining multiple rule modules under a common name. That policy name is then attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts. You can have several different types of rules in a rule module and consequently within one policy.

The policy level is the common ground by which host groups acquire the rules that make up their security policy. You can attach rule modules of differing architectures to the same policy. This way, you can configure a task-specific, self-contained, inclusive policies across all supported architectures (Windows, Solaris, Linux) for software that is supported on all platforms.

**Note**

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

To configure a policy, do the following.

-
- Step 1** Move the mouse over **Configuration** in the menu bar of CSA MC and select **Policies** from the drop-down menu that appears. The policy list view appears.
 - Step 2** Click the **New** button to create a new policy entry. This takes you to the policy configuration page.
 - Step 3** In the available policy configuration fields, enter the following information:
 - **Name**—This is a unique name for this policy grouping of rule modules. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores. For this exercise, enter the name *Quarantined Applications*.
 - **Description**—This is an optional line of text that is displayed in the list view and helps you to identify this particular policy.
 - Step 4** Click the **Save** button.

Attach a Rule Module to a Policy

To apply our configured email quarantine rule module to the policy we've created, do the following.

-
- Step 1** From Policy edit view, click the **Modify rule module associations** link. This takes you to a view containing a swap box list of available modules.
 - Step 2** Select the **Quarantined Application Module** from the list box on the left and click the **Add** button to move it to the right side box.

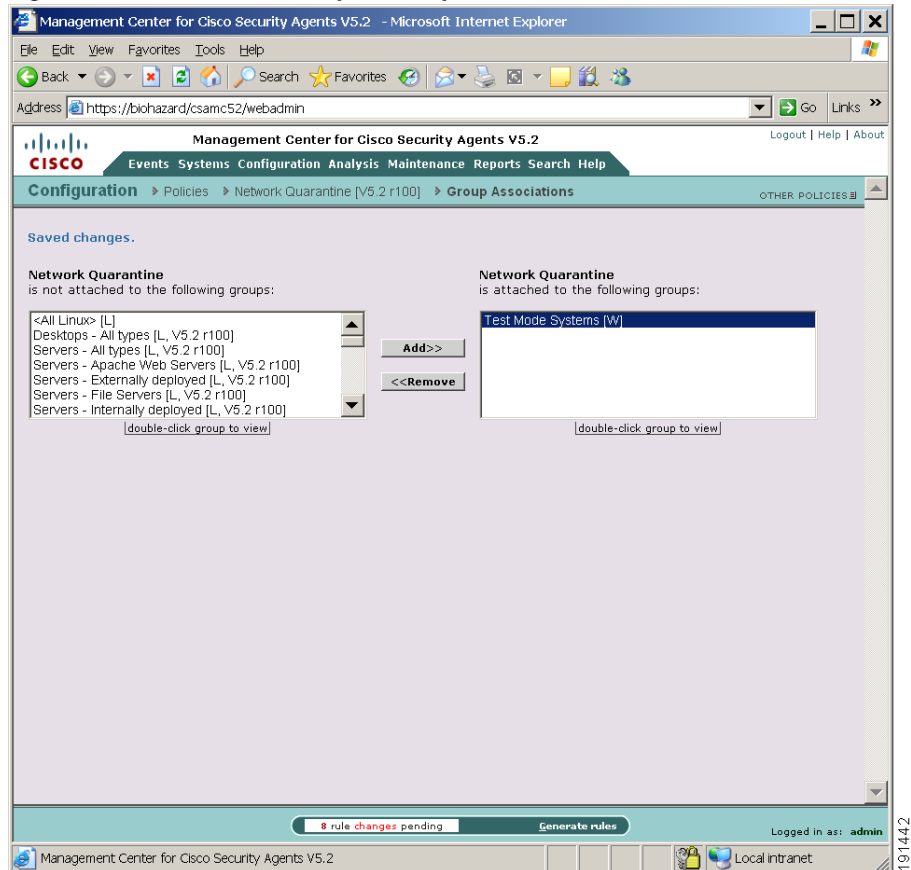
The rule module is now attached to this policy.

Attach a Policy to a Group

To apply our configured email quarantine policy to a particular group of host systems, we must attach this policy to that group.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears.
 - Step 2** From the group list view, click the link for the group you want to attach the policy to. This brings you to that group's edit view.
 - Step 3** From the edit view, click the **Modify policy associations** link. This takes you to a view containing a swap box list of available policies (see [Figure 4-8](#)).
 - Step 4** Select the appropriate policy from the list box on the left and click the **Add** button to move it to the right side box.
 - Step 5** The policy is now attached to this group.

Figure 4-8 Attach Policy to Group



191442

Generate Rule Programs

Now that we've configured our policy and attached it to a group, we'll next distribute the policy to the agents that are part of the group. We do this by first generating our rule programs.

Click **Generate rules** in the bottom frame of CSA MC. All pending database changes ready for distribution appear (see Figure 4-9).

If everything looks okay, you can click the **Generate** button that now appears in the bottom frame. This distributes your policy to the agents.

Figure 4-9 *Generate Rule Programs*

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface. The page title is "Generate Rule Programs". A warning box states: "Warning: The following policies are not attached to any hosts or groups: Application Behavior, Email client - Linux, Email Client - Multi-level Security - Windows, General application - Multi-level Security - Linux, General application - Multi-level Security - Windows, Insecure boot - sample only, Instant Messenger - Windows, Pilot Test, Samba Server - Linux, Security Classification, User Controlled Desktop". Below the warning is a checkbox for "Debug (will be removed)". A summary indicates "8 changes since the last rule program generation:". A table lists the actions:

#	Action	Time	Administrator
8	Attach policy 'Network Quarantine [V5.2 r100]' to group Test Mode Systems [W]	10/20/2006 1:41:01 PM	admin
7	Modify File Access Control rule in rule module Quarantined Application Module [W, V5.2 r100] [Details]	10/20/2006 1:19:17 PM	admin
6	Add File access control rule to rule module Quarantined Application Module [W, V5.2 r100]	10/20/2006 1:09:21 PM	admin
5	Modify rule module Quarantined Application Module [W] [Details]	10/20/2006 11:59:42 AM	admin
4	Create rule module Quarantined Application Module [W]	10/20/2006 11:59:03 AM	admin
3	Initialize agent kit Kit for Test Mode Group [W]	10/20/2006 11:46:57 AM	admin
2	Modify group Test Mode Systems [W] [Details]	10/20/2006 11:39:09 AM	admin
1	Create group Test Mode Systems [W]	10/20/2006 11:38:43 AM	admin

Below the table, it says "Press the **Generate** button to create and distribute rule programs based on the current configuration." At the bottom, there is a "Generate" button and a status bar showing "8 rule changes pending". The user is logged in as "admin".

You can ensure that agents have received this policy by clicking **Hosts** (accessible from **Systems** in the menu bar) and viewing the individual host status views. Click the Refresh button on your browser and look at the host Configuration version data in the host view to make sure it's up-to-date.

**Note**

Hosts poll into CSA MC to retrieve policies. You can shorten or lengthen this polling time in the Group configuration page. You can also send a hint message to tell hosts to poll in before their set polling interval. See the User Guide for details.

Now your agents are installed and protecting end user systems using the macro policy we've configured.

Refer to the User Guide to read about the configuration tasks described here in more detail.

