



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](#)
- [CiscoWorks Administrator Roles in CSA MC, page 4-3](#)
- [Cisco Security Agent Policies, page 4-4](#)
- [Configure a Group, page 4-5](#)
- [Creating Agent Kits, page 4-7](#)
- [The Cisco Security Agent, page 4-12](#)
- [View Registered Hosts, page 4-13](#)
- [Configure a Rule Module, page 4-14](#)
- [Configure a Policy, page 4-20](#)
- [Attach a Rule Module to a Policy, page 4-21](#)

- [Attach a Policy to a Group](#), page 4-21
- [Generate Rule Programs](#), page 4-22

Access Management Center for Cisco Security Agents

You access CSA MC from the CiscoWorks UI. An initial administrator account was created as part of the CiscoWorks installation process. Once that administrator account is entered to login into CiscoWorks, it is not necessary to login again to CSA MC.

- To access CSA MC locally on the system hosting CSA MC software, launch the CiscoWorks UI from **Start> Programs>CiscoWorks>CiscoWorks**. Login into CiscoWorks.
- To access CSA MC from a remote location, launch a browser application and enter

```
http://<ciscoworks system hostname>:1741
```

For example, enter `http://stormcenter:1741`

- From the CiscoWorks UI, the Security Agents item is located in the VPN/Security Management Solution “drawer.” Expand the **Management Center** or the **Administration>Management Center** folders.



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.

CiscoWorks Administrator Roles in CSA MC

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CiscoWorks installation automatically has configuration privileges.

CiscoWorks/CSA MC Administrator Roles:

- **Configure**—If the CiscoWorks administrator has the Network Administrator or System Administrator option enabled, this provides full read and write access to the CSA MC database.
- **Deploy**—If the CiscoWorks administrator has only the Network Operations option enabled, 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**—If the CiscoWorks administrator has none of the roles listed in the first two bullets enabled, this provides administrators with read access to the entire CSA MC database. Administrators can also create reports, alerts, and event sets.



Note

To view or edit your CiscoWorks administrator profile, in the CiscoWorks UI go to **Server Configuration>Setup>Security>Modify My Profile**.

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 8](#) 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.

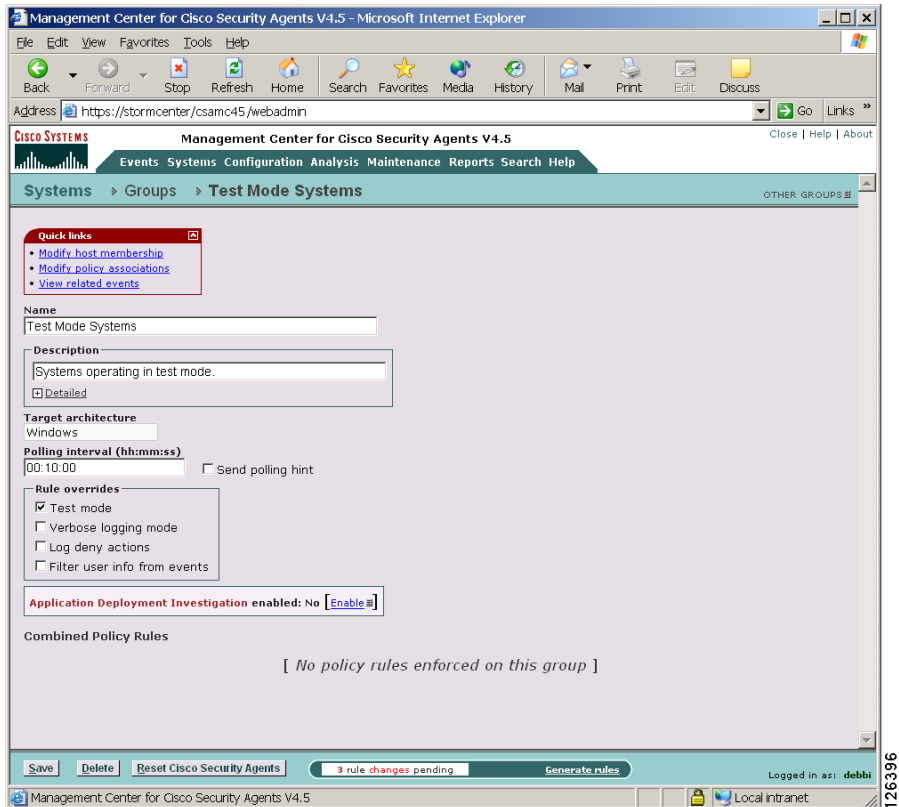
**Note**

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.

Creating Agent Kits

The Management Center for Cisco Security Agent allows for the creation of custom agent installation kits that greatly reduce the administrative burden of deploying the agent on new systems. 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). These kits place hosts in the corresponding groups and enforce the associated policies of each group.

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 groups(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 that you can use if they meet your needs. The desktop and server kits are distributed in test mode so they will not interfere with your work before you have had a chance to study their behavior. (If you use a preconfigured agent kit, you do not have to build your own kit as detailed in the following pages.)

To create agent kits, do the following.

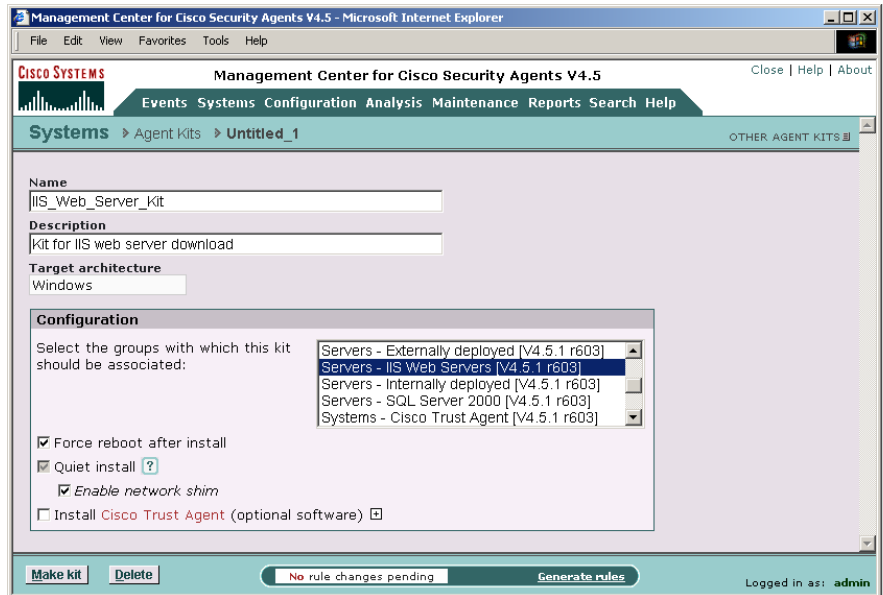
-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. Existing agent kits are displayed.
 - Step 2** Click the **New** button to create a new agent kit.

**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. (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 4-2](#)), 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 4-2 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 User Guide for details.)

- Step 7** For Windows kits, if you select Quiet install, you can also select whether the **Network shim** is enabled or not during the installation. (See the User Guide for more information on enabling the Network Shim.)
- Step 8** Click the **Make Kit** button. A new page opens with the message, “The kit was successfully created.”
- Step 9** Click the **rule generation** link to advance to the Generate Rule Program page. The rules that require generation are listed at the bottom of the page.
- Step 10** Click **Generate** to generate these rules and make your kit available for deployment. Once the generation rules operation completes, you receive the message, “Rule program generation successful.”
- Step 11** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. The agent kit you just created has been added to the list of available kits.
- Step 12** Click the name of your new kit to see its agent kit page. The page displays a URL for this particular kit (see [Figure 4-3](#)). 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 CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:

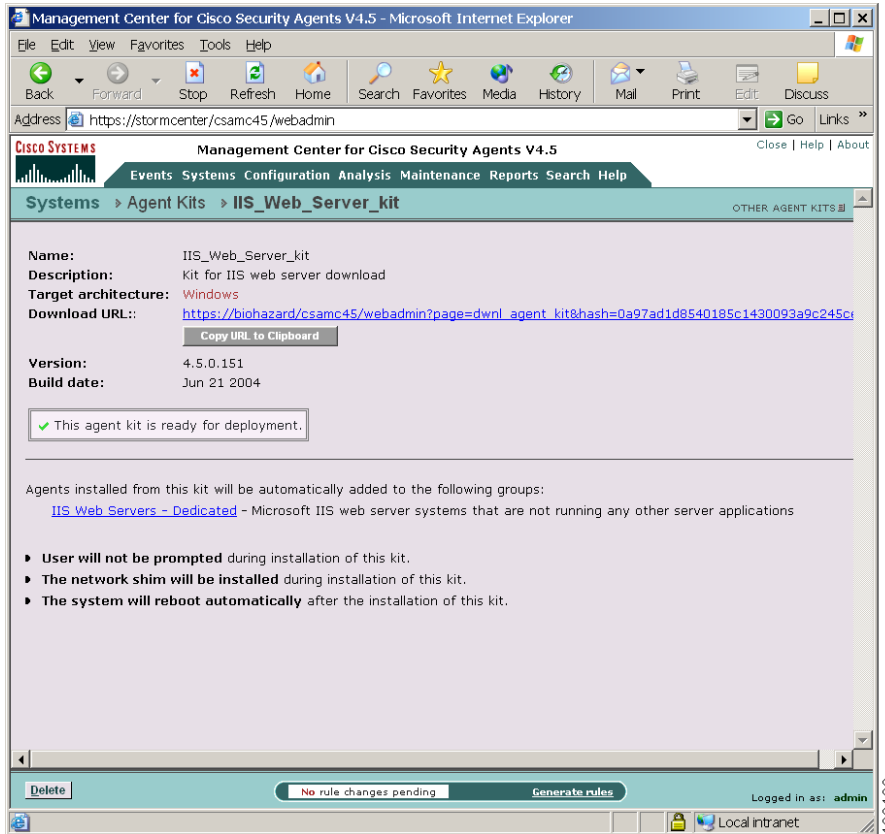
```
https://<ciscoworks system name>/csamc45/kits
```

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. See [Figure 4-4](#).



Note Note that the Registration Control feature also applies to the <ciscoworks system name>/csamc45/kits URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering, it also prevents you from viewing this “kits” URL.

Figure 4-3 Agent Kit Download URL



126426

Figure 4-4 Download Agent Kits

The screenshot shows the Management Center for Cisco Security Agents V4.5 web interface. The browser address bar shows the URL: https://client1027.cisco.com/csamc45/webadmin. The page title is "Management Center for Cisco Security Agents V4.5". The navigation menu includes: Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The current page is "Systems > Agent Kits".

Below the navigation menu, there is a table of agent kits. The table has columns for Name, Status, Description, and Architecture. There are 6 items listed, all with a status of "Ready".

Name	Status	Description	Architecture
Test_Mode_Desktop_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for desktops running in test mode	Linux
Test_Mode_Server_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for servers running in test mode	Linux
Test_Mode_Server_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for servers running in test mode	Solaris
CiscoWorks_VMS_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for systems running the Management Center for Cisco Security Agents	Windows
Test_Mode_Desktop_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for desktops running in test mode	Windows
Test_Mode_Server_V4.5.1.605	Ready	Cisco Security Agent V4.5.1.605 installation kit for servers running in test mode	Windows

At the bottom of the interface, there are buttons for "New" and "Delete", a status bar showing "No rule changes pending", and a "Generate rules" button. The user is logged in as "admin".

132645

The Cisco Security Agent

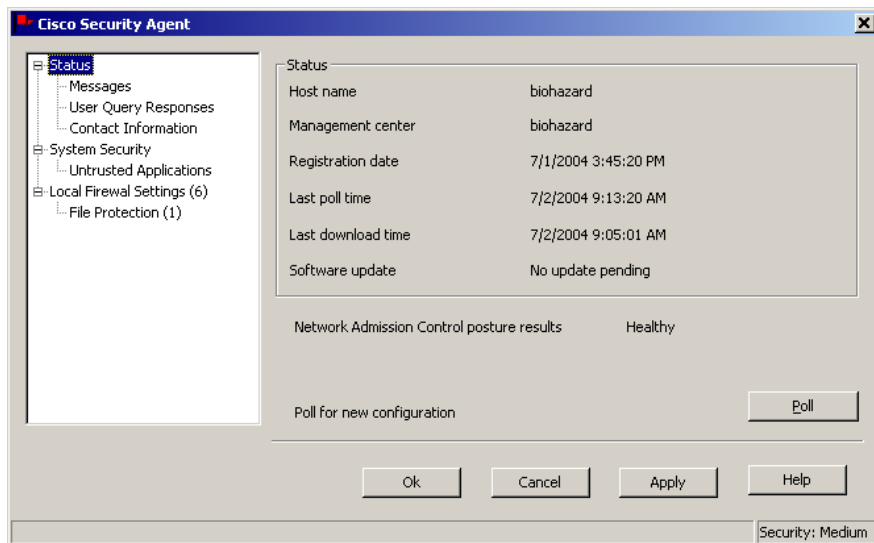
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on supported Windows, Linux, and Solaris platforms. (Note that on Solaris systems there is no agent user interface. See Appendix A in the User Guide for information 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 4-5 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 three 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

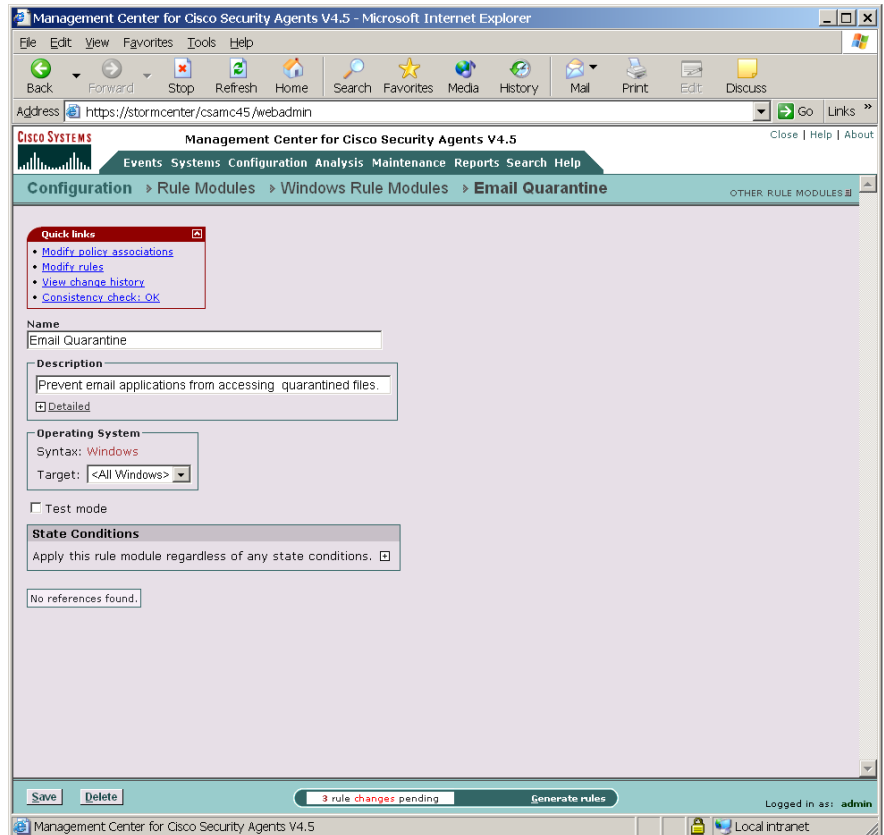
Cisco recommends that you do not edit the preconfigured policies shipped with the Management Center for Cisco Security Agents, but instead add new policies to groups for any changes you might want.

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 4-6](#).

- Step 3** In the configuration view, enter the **Name** *Email Quarantine*. 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 *Prevent email applications from accessing quarantined files*.
- 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.

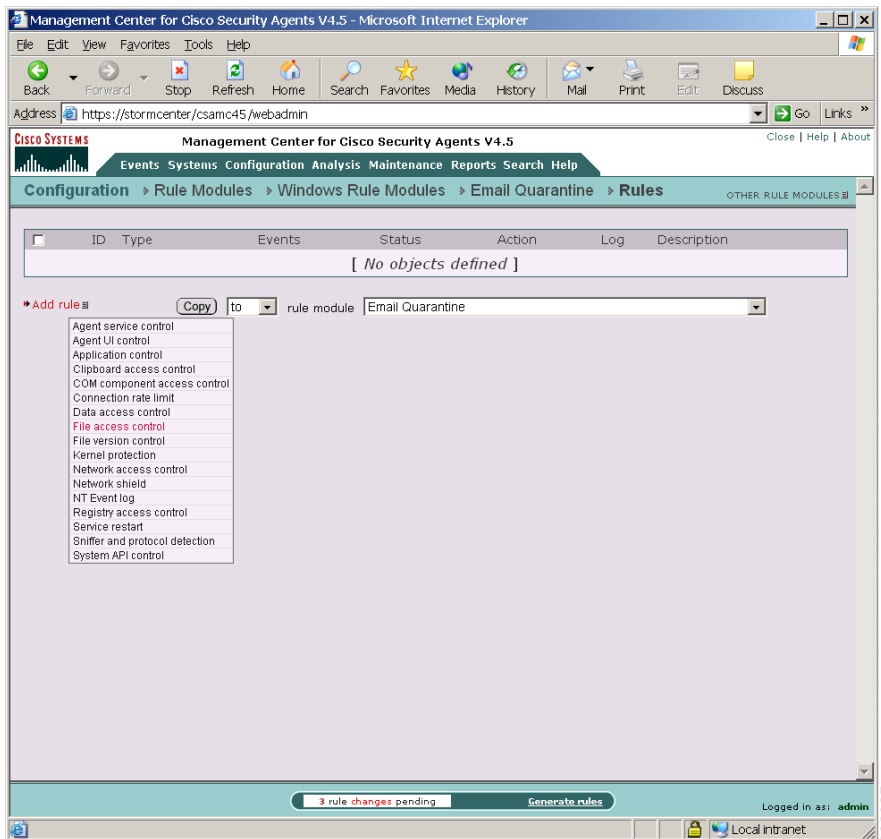
Figure 4-6 Rule Module Creation View



Create a File Access Control Rule

- Step 1** From the Rule Module configuration page (Figure 4-6), 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 4-7). This takes you to the configuration page for this rule.

Figure 4-7 Add Rules to Module

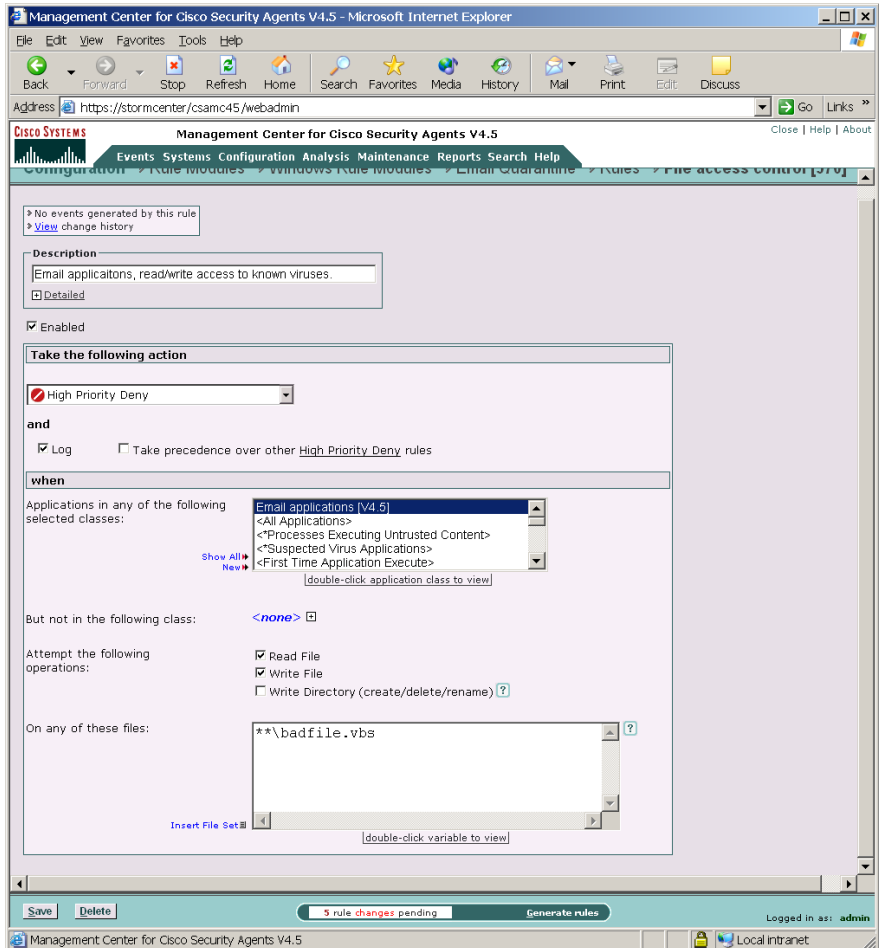


- Step 4** In the File access control rule configuration view (see [Figure 4-8](#)), enter the following information:
- **Description**—Email applications, read/write access for known virus files
 - **Enabled**—(This is selected by default. Don't change this setting for this example.)

- Step 5** Select **High Priority Deny** from the action pulldown list. By selecting High Priority Deny here, we are stopping the application 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 **Email applications**. Note that when you click Save, selected application classes move to the top of the list.
- Step 8** Select the **Read** and **Write Files** 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 the following:
- ```
**\badfile.vbs
```
- It is important to use the correct syntax when specifying files and file pathnames. The User Guide includes a discussion on this subject. In the meantime, in the files field, with this syntax we have indicated all executables in system directories and their subfolders found on any system drive.
- Step 10** Click the **Save** button.  
Next, we will create a policy to attach our rule module to.

Figure 4-8 File Access Control Rule



# 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 *Email quarantine*.
    - **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.

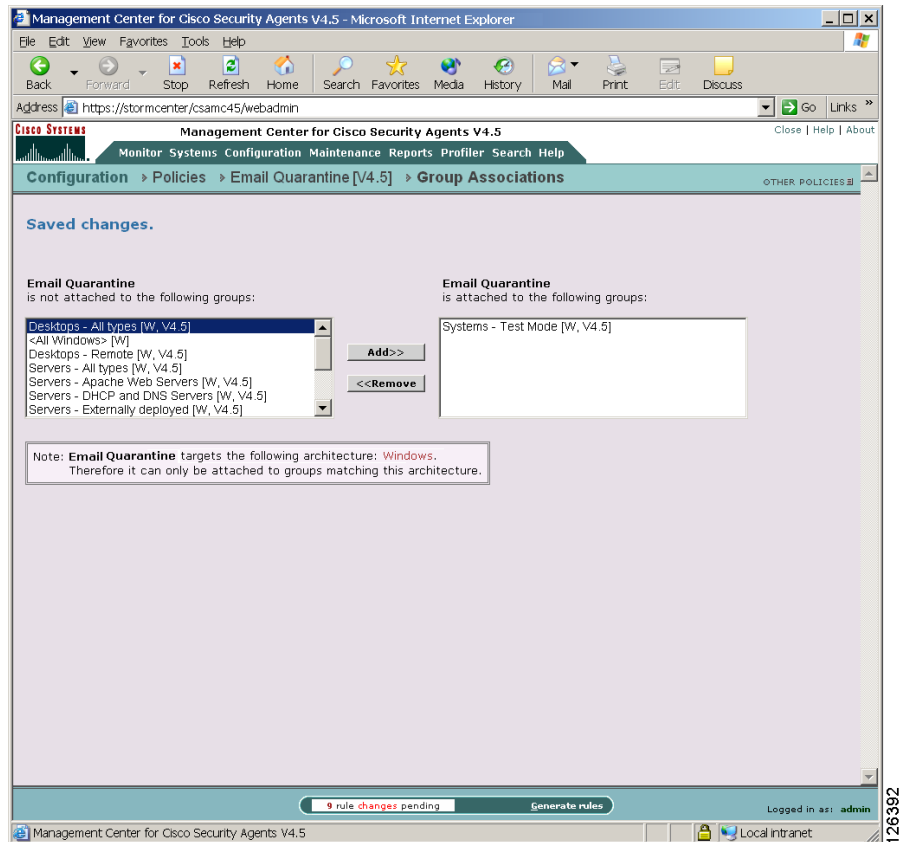
- 
- Step 1** From Policy edit view, click the **Modify rule module associations** link. This takes you to a view containing a swap box list of available modules.
  - Step 2** Select the **Email Quarantine** module from the list box on the left and click the **Add** button to move it to the right side 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 4-9](#)).
  - Step 4** Select the **Email Quarantine** 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 4-9 Attach Policy to Group



126392

## 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 4-10](#)).

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 4-10 Generate Rule Programs

Management Center for Cisco Security Agents - Microsoft Internet Explorer

Address: <https://stormcenter/csamc45/webadmin>

Management Center for Cisco Security Agents V4.5

Generate Rule Programs

**Warning:**  
The following policies are not attached to any hosts or groups:

- [File System Lockdown Module](#)
- [Insecure Management Module](#)
- [Restrictive SandWall Module](#)
- [CiscoWorks Restrictive VMS Module](#)
- [Data Theft Prevention Module](#)
- [Distributed Firewall Module](#)
- [File Integrity Module](#)
- [Windows Security Events Module](#)
- [Windows XP Help Center Module](#)

0 changes since the last rule program generation:

| Action                                                                 | Time                  |
|------------------------------------------------------------------------|-----------------------|
| Modify policy 'Email Quarantine' [Details]                             | 12/30/2004 3:14:39 PM |
| Add File access control rule to policy 'Email Quarantine'              | 12/30/2004 3:14:50 PM |
| Modify File access control rule in policy 'Email Quarantine' [Details] | 12/30/2004 3:15:12 PM |
| Create FS variable 'Untitled_1'                                        | 12/30/2004 3:15:21 PM |
| Modified file set variable 'Known virus files' [Details]               | 12/30/2004 3:18:23 PM |
| Modify File access control rule in policy 'Email Quarantine' [Details] | 12/30/2004 3:19:07 PM |
| Modify File access control rule in policy 'Email Quarantine' [Details] | 12/30/2004 3:38:49 PM |
| Add policy 'Email Quarantine' to group 'Default Desktops'              | 12/30/2004 4:47:50 PM |

Press the Generate button to create and distribute rule programs based on the current configuration:

Generate 3 rule changes pending

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.