



## CHAPTER 2

# Management Center for Cisco Security Agents Administration

---

## Overview

Management Center for Cisco Security Agents supports editing of the database by multiple administrators. Administrators must identify themselves and authenticate to CSA MC before they can access any CSA MC configuration data.

CSA MC's web-based user interface provides secure access to the database from anywhere on the network. All changes to the database are logged. The logged information includes a summary description of the modification, the time the changes were made, and the identity of the administrator who made the changes.

This section contains the following topics.

- [Management Center for Cisco Security Agents Description, page 2-2](#)
- [Browser Requirements, page 2-2](#)
- [About Management Center for Cisco Security Agents, page 2-3](#)
- [Accessing Management Center for Cisco Security Agents, page 2-4](#)
- [Configuring Role-Based Administration, page 2-5](#)
- [Configuring Role-Based Administration, page 2-5](#)
- [Changing Administrator Passwords, page 2-10](#)
- [Configure Monitor Role Administrator Access Restrictions, page 2-11](#)
- [Manage Administrator Active Login Sessions, page 2-13](#)

- [Administrator LDAP Authentication, page 2-14](#)
- [Using Audit Trail, page 2-15](#)
- [Using Management Center for Cisco Security Agents, page 2-16](#)
- [Creating, Saving, and Deleting Data, page 2-33](#)
- [Using the Correct Syntax, page 2-35](#)

## Management Center for Cisco Security Agents Description

The Management Center for Cisco Security Agents (CSA MC) is a web-based user interface which can be accessed from any machine connected to the Internet and running a web browser. Through CSA MC, administrators configure all aspects of Management Center for Cisco Security Agents.

## Browser Requirements

The browser you use to access CSA MC must meet the following requirements.

Internet Explorer:

- Version 6.0 or later
- You must have cookies enabled. This means using a maximum setting of "medium" as your Internet security setting. Locate this feature from the following menu, Tools>Internet Options. Click the Security tab.
- JavaScript must be enabled.

FireFox:

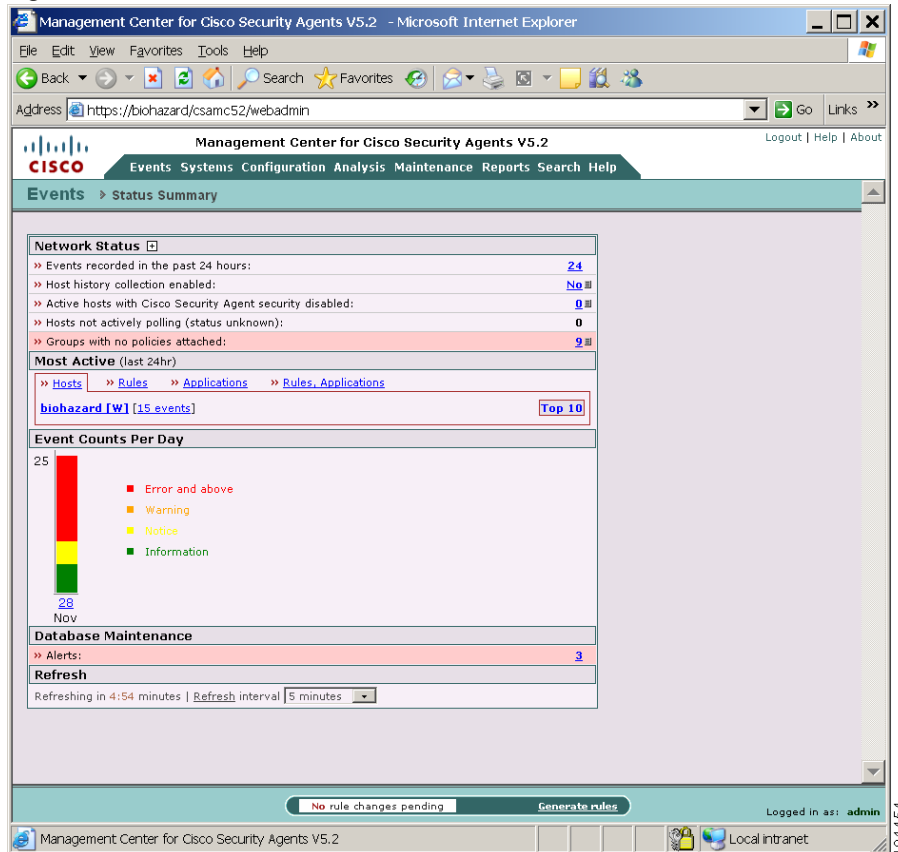
- Version 1.5.0.x or higher
- You must have cookies enabled. Locate this feature from the following menu, Tools>Options>Privacy>Cookies.
- JavaScript must be enabled.

# About Management Center for Cisco Security Agents

All Cisco Security Agent policies are configured and deployed through the CSA MC web-based user interface. CSA MC also provides a reporting tool, letting you generate reports with varying views of your network enterprise health and status. Providing an HTML web-based user interface enables an administrator to access CSA MC from any machine connected to the Internet and running a web browser.

CSA MC provides a menu bar for easy navigation among the configurable administrator task items. Configurable items are displayed in drop-down menus that appear when you move the mouse over a category in the menu bar. When you select an item, the properties and status for that item are displayed.

Figure 2-1 CSA MC Status View



191454

## Accessing Management Center for Cisco Security Agents

You access CSA MC locally or remotely from a supported Web browser. An initial administrator account was created as part of the CSA MC installation process. Use that administrator account to log into CSA MC.

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

- 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`

The CSA MC login appears. Enter your administrator account name and password in the edit fields provided in the initial screen.

**Note**

When you login to the CSA MC system, various messages or warnings may appear to notify you of system issues. These issues may include database maintenance and backup needs or CTA software upgrade requirements.

## Configuring Role-Based Administration

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.

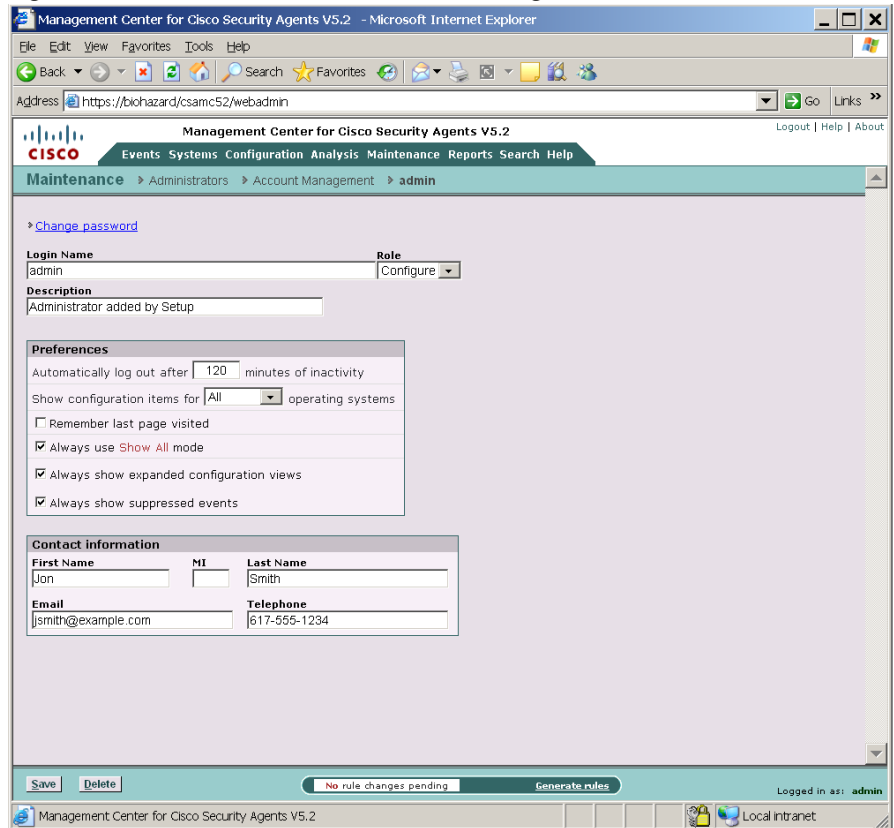
CSA MC Administrator Roles:

- **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.

Create new administrator accounts or manage existing ones by doing the following:

- 
- Step 1** From the CSA MC menu bar, go to **Maintenance>Administrators>Account Management**. The administrator created during the installation should already exist in the list page.
- Step 2** Click the **New** button to create a new administrator account or click on an existing account to edit it.

- Step 3** For each new administrator you create, enter the following information (see [Figure 2-2](#)):
- **Login Name** - This is the name the administrator uses each time he/she logs into the database. (This name must be unique.)
  - **Description** - This is an optional line of text that is displayed in the list view and helps you to identify this particular administrator.
  - **Role** - Configure role-based administration privileges for this administrator. The options are configure, deploy, and monitor privileges.
- Step 4** Configure **Administrator Preferences** as follows
- **Session timeout** - By default, administrator sessions timeout after 15 minutes of inactivity. Enter a value here, in minutes (1-120), to change the default.
  - **Operating System Views** - For this administrator, you can select to view configuration items for all operating systems or to view only those for a particular operating system. If you leave the default of "All" configuration items at the top of item list pages, you must then select an operating system when you configure items such as policies, groups, and agent kits. If you are only configuring or deploying policies to UNIX systems, it is likely that you will only want to see those items. The same holds true if you are deploying policies to only Windows systems. (See [Table 2-1](#) and [Figure 2-3](#) for further OS information.)

**Figure 2-2 Administrator Account Management Window**

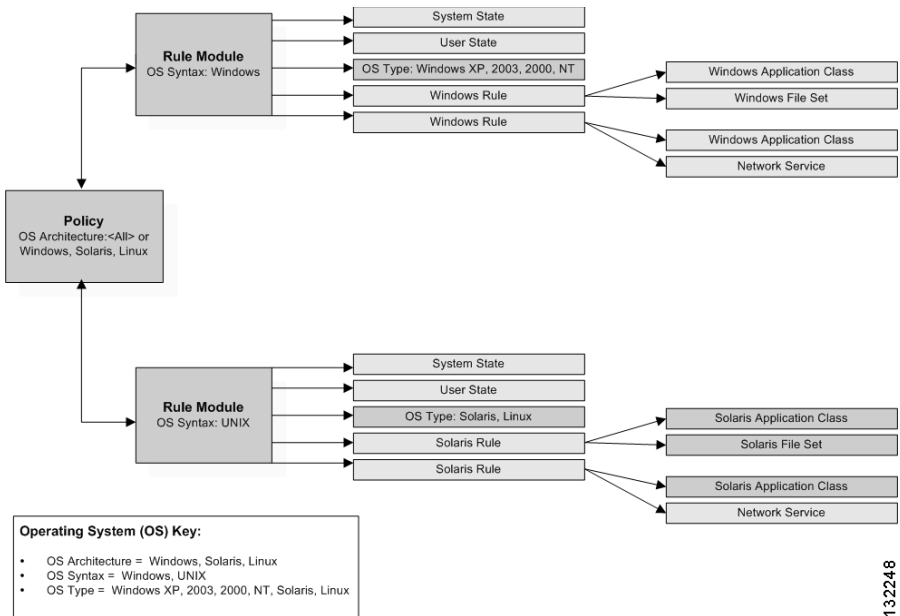
Operating system designation requirements and their granularity vary for different configuration items. Refer to the following chart and diagram for an overview of how and where operating systems designations are made.

**Table 2-1 Operating System Naming Conventions**

OS Naming Conventions	Available OS Options
OS Architecture	Windows, Solaris, Linux

OS Naming Conventions	Available OS Options
OS Syntax	Windows, UNIX
OS Type	Windows All, Windows XP, Windows 2003, Windows 2000, Windows NT, UNIX All, Linux, Solaris

Figure 2-3 Example: Operating System Specifications



132248

- **Remember last page visited**—Select this check box to have the management center display the last page you visited during your last session when you next log in. (This can be useful if the management center times out due to inactivity during a session.)
- **Always use Show All mode** If you have hidden configuration items by selecting the Display only in Show All mode check box for variables and application classes, selecting this check box for your admin preference causes all hidden items to appear in list pages and selection boxes. When you select the “Display only in Show All mode” check box for a configuration item, the only way to have the item reappear is to select the Always use Show All mode

check box for your admin preference and then all hidden items will also appear. Note that you can click “Show All” in rule pages to temporarily display hidden items for that rule page.



---

**Note** The Display only in Show All mode feature in configuration pages makes configuring CSA MC policies easier by paring down configuration items to only those you use most.

---

- **Always show expanded configuration views** To simplify product configuration, several management center pages, especially rule pages, contain fields that are not automatically displayed. In place of these fields is a + symbol signifying that the field is present and can be configured by clicking on the + symbol to expand it. If the field in question has a configuration setting (either an explicit setting or a default setting such as <none> or <all>) the configured setting is displayed textually beside the plus sign. The fields that are not expanded by default are considered fields that are used less often and are not shown in order to streamline the page and the configuration tasks.

Once a field is expanded manually on a page, you cannot collapse it again until you refresh the page. To always display all fields on all pages, select the **Always show expanded configuration views** check box as an Admin Preference.

- **Always show suppressed events** Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. When event suppression is enabled (this checkbox is not selected), all events of a particular type are no longer displayed in the event log. Suppressing an event removes all viewable instances of that event and causes further events of the same type to be hidden. Event suppression is configured through the Event Log Wizard. Select this checkbox to have all configured event suppression ignored and to display all events in the event log.
- **Contact information (optional)** - Name, Email, Telephone number

**Step 5** Click the **Save** button.

**Step 6** Click the **Set Password** link at the top of the page to enter a password for this administrator. Passwords must be at least 6 characters long. An administrator’s password cannot be the same as or contain the administrator’s login name. See [Changing Administrator Passwords, page 2-10](#).

## Changing Administrator Passwords

You can set or change an administrator's password at any time by accessing that administrator's configuration page.

**Note**

---

If you are using LDAP authentication for administrators, it is not required that you set a password. However, if LDAP authentication fails, the administrator cannot login unless a local password is set as well (as a fallback authentication means).

---

**Step 1** Click the **Set/Change Password link** from the administrator configuration page. (Access this page from the administrator list view.)

**Step 2** In the Administrator Change Password view, enter the

- **Current Session Password**, (This is the password of the current logged-in administrator that is entering the new administrator information, not the password of the administrator you are entering.) then enter...
- **New Password**, and then confirm the new password in the...**Confirm Password** field.

**Note**

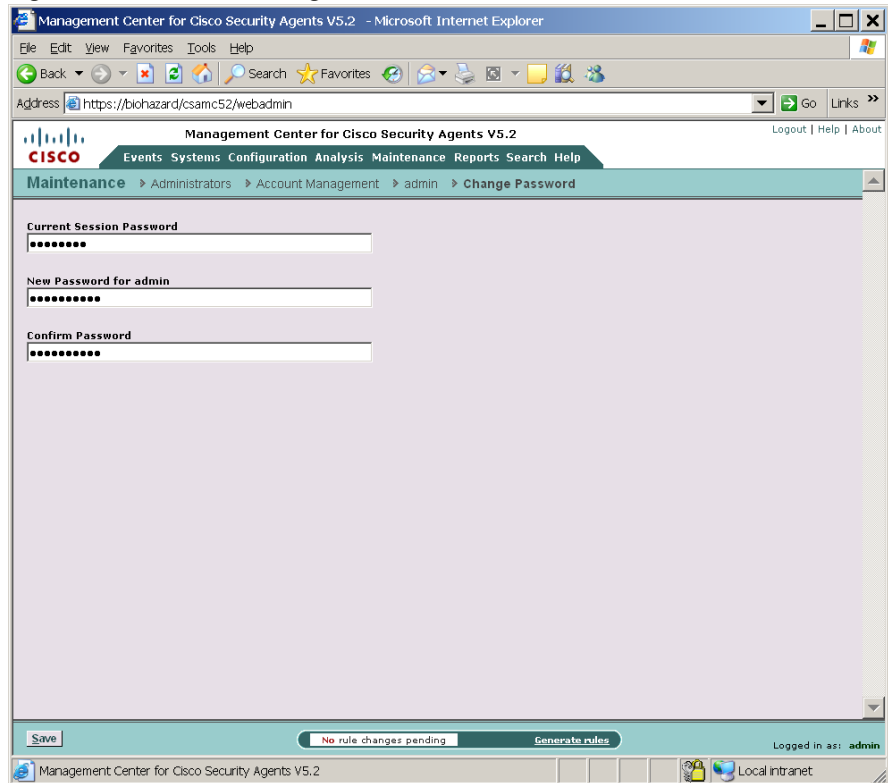
---

Passwords must be at least 6 characters long. An administrator's password cannot be the same as or contain the administrator's login name.

---

3. Click the **Save** button.

Figure 2-4 Set/Change Administrator Password



## Configure Monitor Role Administrator Access Restrictions

You can configure CSA MC administrators with a Monitor role to have access to only those configuration items you wish to allow viewing of. Therefore, you can place extra restrictions on that administrator's performing of monitor tasks on CSA MC.

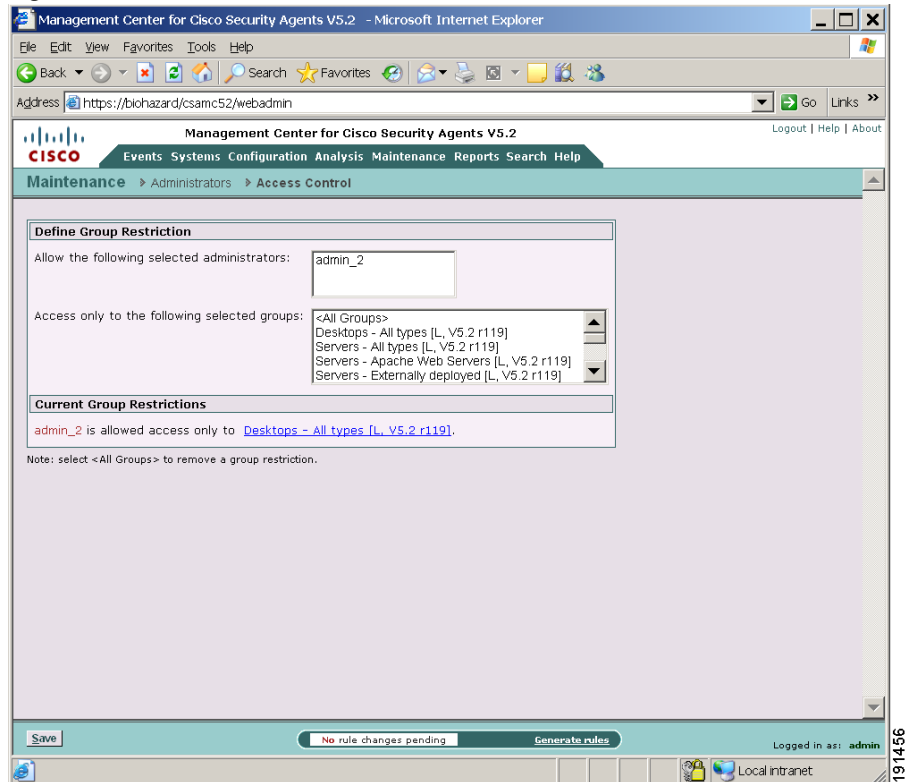
- Step 1** From the CSA MC menu bar, go to **Maintenance>Administrators>Access Control**. The existing administrators configured to have a Monitor role appear in the administrator selection box in the Define Group Restrictions section.

**Step 2** By selecting particular administrators and then selecting particular groups, you are indicating that the selected administrators can only view items pertaining to the selected groups they are allowed to view.

If an administrator is not permitted access to a group, that administrator cannot view any items related to the group, including events, policies, and application classes (unless those configuration items are also used by groups they are allowed to see.) You can configure several access control settings from this page.

All configured settings appear at the bottom of the single global page.

Figure 2-5 Administrator Access Restrictions



## Manage Administrator Active Login Sessions

You can view actively logged in CSA MC administrators and look at login information such as Role, Remote login address, the period of time for which the administrator has been logged in, and the time that has passed since the administrator has made changes on the system.

From the CSA MC menu bar, go to **Maintenance>Administrators>Active Login Sessions**. The list of logged in administrators appears. You can log an administrator out of the system by selecting the checkbox beside that administrator name and clicking the **Logout** button at the bottom of the page.

## Administrator LDAP Authentication

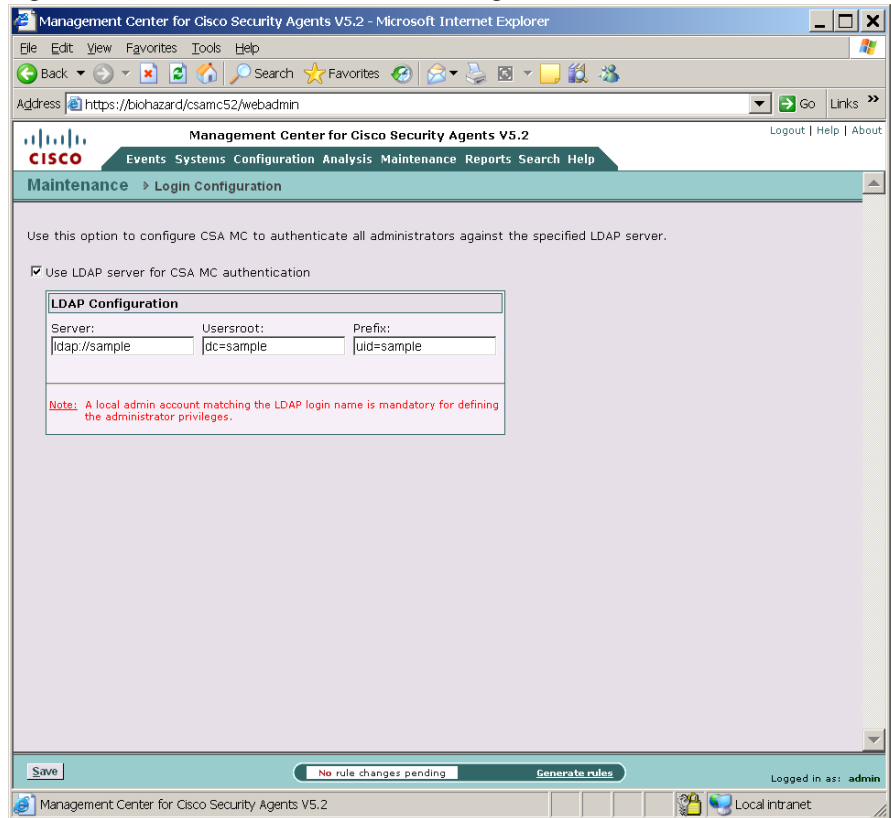
The CSA MC default authentication method for authenticating administrators to the system is local database configuration authentication. This is when administrator names and passwords are entered via CSA MC. Alternatively, you can configure CSA MC to authenticate administrators using LDAP. You must already have a configured LDAP server that can communicate with CSA MC to use this authentication type. See [Figure 2-6](#).

To use LDAP authentication, you must do the following:

- 
- Step 1** Configure an administrator account on CSA MC using the steps described in [Configuring Role-Based Administration, page 2-5](#). You do not have to create a password for this administrator. It is only required that you create a password if you are using local database authentication.
  - Step 2** On the MC, navigate to **Maintenance>Login Configuration**. This takes you the LDAP server configuration page. Once selected, this LDAP server authentication is global to the system. All administrators logging into CSA MC will first be authenticated to CSA MC using the LDAP server.
  - Step 3** To use LDAP authentication, select the **Use LDAP server for authentication** checkbox and enter the required LDAP server information in the edit fields provided.

Once you enable the **Use LDAP server for authentication** checkbox, the CSA MC login page **Authentication** field becomes available. (**Local** is always the default authentication type until you enable LDAP.) Therefore, you should logout of CSA MC and log back in again selecting LDAP from the Authentication field above the Username and Password fields if you intend to use LDAP authentication.

Figure 2-6 Global LDAP Server Configuration



191465

## Using Audit Trail

Accessible from the Reports drop-down list in the menu bar, the Audit Trail page displays a list of changes administrators have made to the CSA MC database. These changes are displayed according to the following information:

- The change itself.
- The type of change (configuration category: policies, file sets, groups, and so on).
- The date and time the change was made.

- The administrator who made the change.

Click the **Change Filter** link to edit the audit trail viewing parameters according to the following:

- Start date (enter date parameters using the same formats as in the Event Log).
- End date.
- The administrator who made the changes.
- The change type (configuration category: policies, file sets, groups, and so on).
- The number of changes to display per viewing page. Note that you can select <All> here to display all entries. This may be useful if you intend to archive or save the audit trail data.
- Filter by included or excluded text.

## Using Management Center for Cisco Security Agents

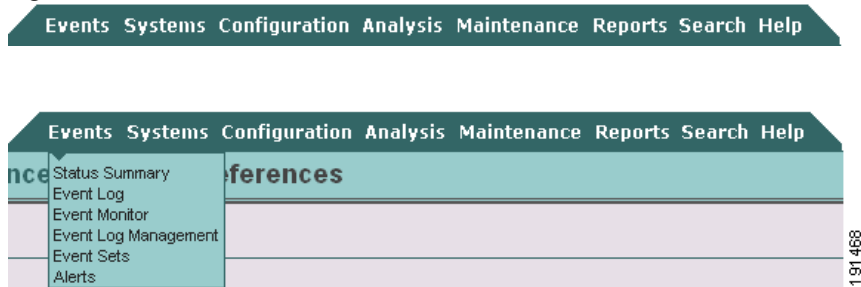
The sections in this chapter describe the various components you should understand in order to configure Cisco Security Agents using CSA MC.

### Menu Bar

The menu bar at the top of CSA MC provides links to all configuration pages and list views. Arrows indicate that there are subcategories for which you can choose from those top-level main items (see [Figure 2-7](#)). These subcategories appear when you move the mouse over the main item itself.

When you select an item from the menu bar, the list view page for that item appears.

Figure 2-7 Menu Bar

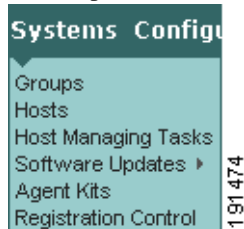


The configuration options available from each menu bar item are as follows.

**Events**—The Events drop-down list provide tools for viewing and managing system status and log files. You can also set alerts and alert parameters from here. (See [Chapter 10, “Event Logging and Alerts”](#).)



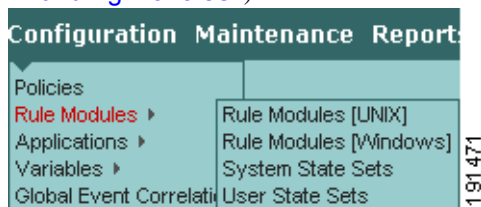
**Systems**—The items available from the Systems drop-down list let you configure the groups which agent host systems are placed into when they register with CSA MC. You can also deploy new agent kits and software updates for agents from this menu option. (See [Chapter 3, “Configuring Groups and Managing Hosts”](#).)



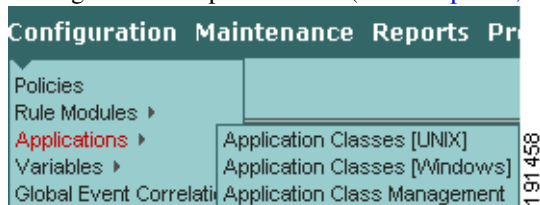
**Configuration**—The items available from the Configuration drop-down list provide you with the pages you will need to configure your policies for agents. This list provides links to the rule pages you use to develop your policies, as well as links to application classes and variables. (See [Chapter 4, “Building Policies”](#))



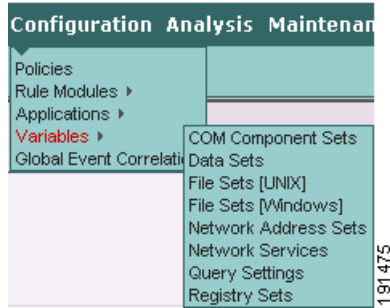
**Configuration>Rule modules**—System state sets and User state sets are accessible from the cascading Rule Modules menu that appears when you move your mouse over that item in the Configuration drop-down list. (See [Chapter 4, “Building Policies”](#))



**Configuration>Applications** are accessible from the cascading menu that appears when you move your mouse over the Applications item in the Configuration drop-down list. (See [Chapter 8, “Using Application Classes”](#))



**Configuration>Variables**, such as file sets and network addresses, which are the building blocks for policies, are accessible from the cascading menu that appears when you move your mouse over the Variables item in the Configuration drop-down list. (See [Chapter 9, “Configuring Variables”](#).)

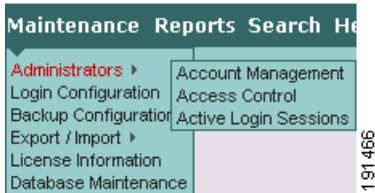


**Analysis**—The items in the Analysis menu are for diagnostic and investigative purposes, separate from general CSA MC configuration. Use these menu options to analyze application behavior and to investigate all resources being used across your enterprise with the purpose of securing these applications and resources using CSA MC Policies. (See [Chapter 13, “Using Cisco Security Agent Analysis”](#))



**Maintenance**—The items available from the Maintenance drop-down list let you import and/or export configuration files, backup your database configuration and enter your license key. When you move your mouse over the Export/Import item,

you can select further options from the cascading menu that appears. (See [Configuring Role-Based Administration, page 2-5](#), available from this menu item, as well.)



**Reports**—The items available from the Reports drop-down list let you generate reports by various categories such as event severity level, by the group(s) that generated the event and by individual host systems. (See [Chapter 11, “Generating Reports”](#).)



**Search**—Use the selections available from the Search drop-down list to search for a specific configuration item in the CSA MC database. You can limit your search to Hosts, Groups, Policies, Rules, Rule Modules, Variables, Application Classes, or All. Each option has its own criteria by which you can search.



## Using Search

Once you select a category to search on from the Search drop-down list, enter all or part of the name of the item for which you are searching in the Find field. (See [Figure 2-8](#).)

To further control your search, select one or more of the following check boxes.

- Show references—Select this check box to also display configuration items which reference the name being searched for. Clicking on the referenced item in the right column lets you access the configuration(s) using the string value.
- Search on description—Select this check box to search for the string value in Description fields.
- Search all fields—Select this checkbox to search all database fields (including Description fields) for the string value.

You can limit Results per page by entering a value in the corresponding field. (25 is the default). Click the **Find** button. Results are displayed as links. Click the item link to go to its configuration view.



### Tip

Once you click Find on the search page and have a list of findings, you can view each item in the list in a new browser window. When you move the mouse over each item in the found list, an **open in new window** option appears by the item. If you click that option, the item opens in a new window for you to view. This way, your original list of found items is preserved while you view individual items in a new window. If you do not open the item in a new window, you cannot click back to the found list and you must run the search again.



### Note

The search page does not search the event database.

(Use the Delete button to remove found items from the database. Once an item is deleted here, it cannot be recovered.)

- Replace—From the Search menu, Policies, Variables, and Application Classes allow you to perform a search and replace on items. Once you've selected a category from the Search menu, you can click the Replace link to access a pop-up box. In that box, you select references to an item and replace it where it appears with another item that you select. For example, you may

want to replace all references to a certain variable across the system.

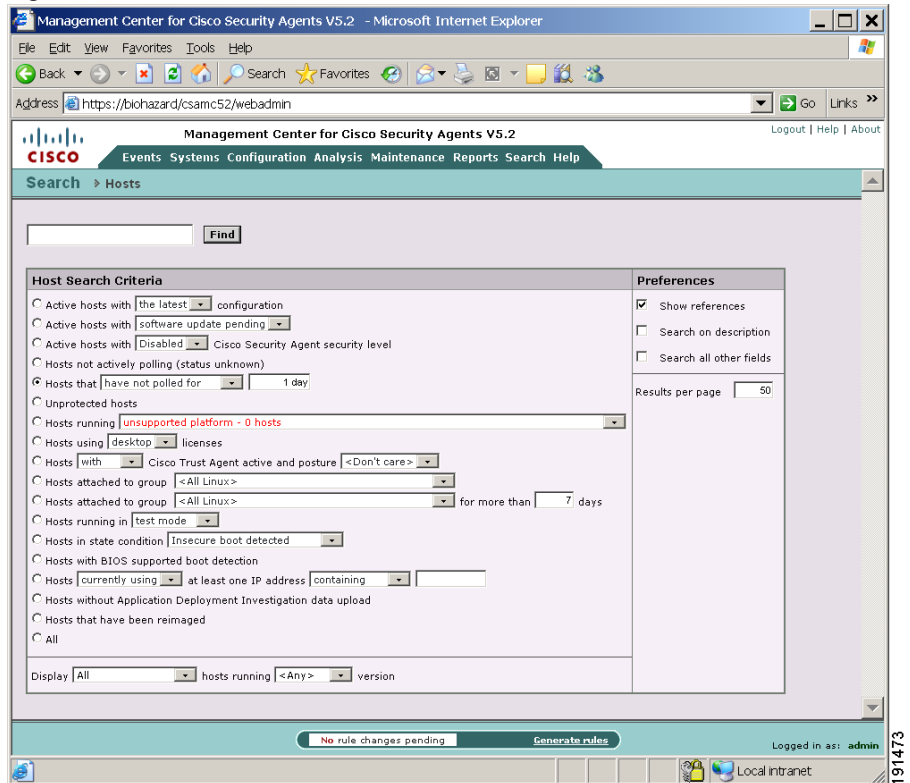
Selecting the Preview checkbox allows you to see where all references will be replaced before you actually do the replacement.

The Hosts search page lets you search for hosts based on several criteria. For example, you can search for hosts that are not actively polling or that are unprotected. Unprotected hosts are not members of any group or are members of a group that has no policies

You can also search for hosts according to those with "old rule sets", "the latest rule set", "old (outdated) software", "those with pending software updates", "hosts not actively polling" see Not active hosts for details on this item, "hosts that have not polled in for a specified time".

See [Host Detail View, page 3-27](#) for more information on Hosts.

Figure 2-8 Search Feature



## Using Help

**Help**—In addition to this configuration guide, CSA MC provides online help. When you click **Help** on the far right of the menu bar, you can select Online Help or you can click a link for the Technical Support web site. When you select Online help, a new browser window opens. This window contains help information on the

configuration item from which you have accessed the help. To view help on other topics, click the corresponding topic link in the Contents frame of the help window.

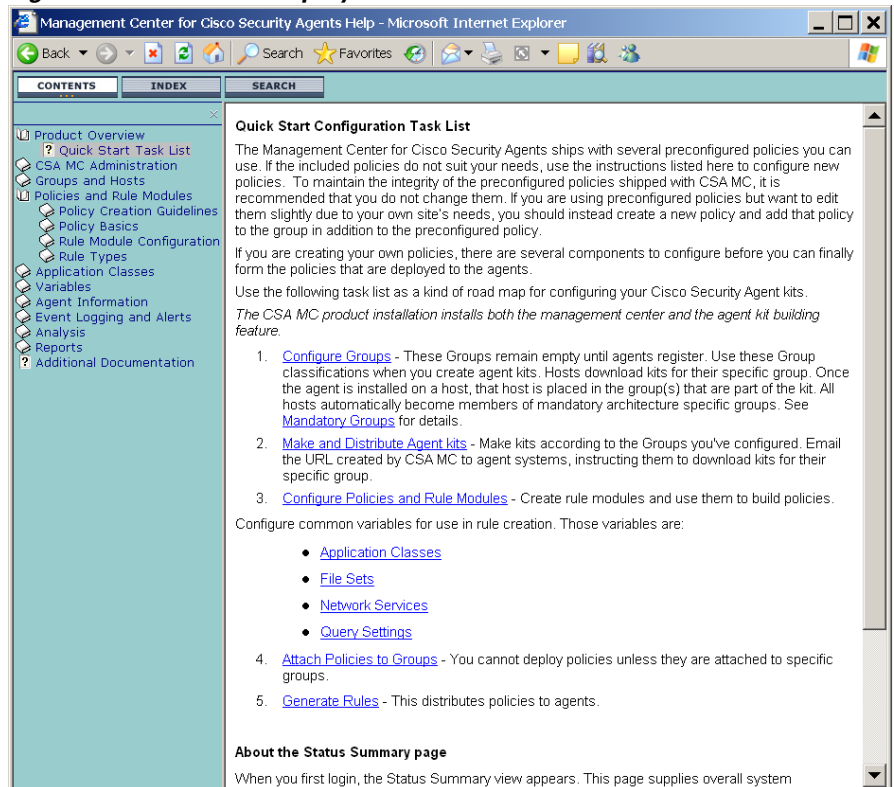
**Note**

---

You can also access Quick Help for fields that have question marks beside them. Quick Help provides information for specific text fields.

---

Figure 2-9 Main Help System



## Shortcuts and Hints

**Other <configuration item>**—In configuration views, an Other [Policies, Applications, File Sets, etc] link appears on the right side of the user interface below the menu bar. Click this link to view a drop-down list containing the names of other configurations within the category you are currently working (see [Figure 2-10](#)). Click one of these names to view the configuration page for that item.



### Note

If you jump to another configuration page without saving the page you are working in, the information on the current page is lost.

Figure 2-10 Other Policies Link

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface. 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 "Configuration", "Policies", and "General application - Basic Security - Windows". The "OTHER POLICIES" link is highlighted in the top right corner.

The main content area is divided into several sections:

- Quick links:**
  - Modify group associations
  - Modify rule module associations
  - Explain rules
  - View change history
- Name:** General application - Basic Security - Windows
- Description:** Basic, Application independent security policy for Windows
- Target Architectures:**
  - Linux [0 modules]
  - Solaris [0 modules]
  - Windows [3 modules; 23 rules]
- Attached Rule Modules:** Items: 3 [0 UNIX; 3 Windows]
 

Name	Version	Description	Target OS
<a href="#">General Application Permissions - all Security Levels</a>	5.2 r119	Application independent behavior enforcement, all Security Levels	All Windows
<a href="#">General Application Permissions - base security</a>	5.2 r119	Application independent behavior enforcement, base security	All Windows
<a href="#">User Authentication Auditing Module</a>	5.2 r119	Module for Auditing User Authentication	All Windows
- Combined Policy Rules:** View All rules

At the bottom of the page, there are buttons for "Save", "Delete", and "Generate rules". A status bar indicates "No rule changes pending" and "Logged in as: admin". The browser address bar shows [https://biohazard/csamc52/webadmin?page=policy\\_set\\_view&id=22#](https://biohazard/csamc52/webadmin?page=policy_set_view&id=22#).

191469

## Status Summary

**Status Summary**—The **Status Summary** window supplies overall system summary information including recorded events and agent rule versions (see Figure 2-11). You can access this page at any time by selecting it from the Events category in the menu bar. The various summary categories available from this page are as follows.

### Network Status

By default, items in the Network Status category do not appear in the list if their number is 0. Simply expand the Network Status view to see all available status items. The status items listed here generally have to do with overall host statistics such as hosts that are not running with up-to-date software versions or the latest rule programs. You can view the number of hosts running in test mode or learn mode, etc. Additionally, the numbers that appear in this status section are clickable and take you to a list of the hosts that comprise that number.

The following information is displayed in the Network Status section:

**Events recorded in the past 24 hours:** The number listed here provides a link to the most recent events as described.

**Host history collection enabled:** Host history collection is a feature that you enable and disable from this page. You optionally, globally enable Host history collection for all hosts if you want to maintain individual host histories of 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. Once this feature is enabled, to view a host's history, you access the details page for that host from **System>Hosts** in the menu bar and then click the link for that host. From the host details page, click the **Detailed status and diagnostics** link. A pop-up windows lets you view collected host history information. See [Host Status, page 3-29](#).

**Note**

---

Host history collection can cause your database to fill up faster if you have tens of thousands of hosts and an abundance of configuration changes.

---

**Active hosts with Cisco Security Agent security disabled:** The host is polling in at scheduled intervals and it is running the latest agent software and the latest policies, but agent security has been disabled and there is no policy enforcement.

**Active hosts with the current configuration:** The host is polling in at scheduled intervals and it is running the latest agent software and the latest policies.

**Active hosts running an old configuration:** The host is polling in at scheduled intervals and it is running the latest agent software but it has not downloaded the latest policies.

**Active hosts running old software:** The host is polling in at scheduled intervals and it is using the latest policies but it is not running the latest agent software.

**Active hosts with software update pending:** The host is polling in at scheduled intervals and it is using the latest policies but it is not running the latest agent software. It has a software update pending.

**Unprotected hosts:** The Cisco Security Agent on the host is not enforcing any policies or agent security as been disabled.

**Hosts running in test mode:** This number of hosts are in test mode. See [Using Test Mode, page 5-7](#).

**Hosts running in learn mode:** This number of hosts are in learn mode. See [Using Learn Mode, page 5-11](#).

**Hosts with BIOS supported boot detection:** This number of hosts have BIOS supported boot detection enabled. See [Setting State Conditions, page 5-13](#).

**Hosts in state condition Insecure boot detected:** This number of hosts are in the Insecure boot detection state. See [Setting State Conditions, page 5-13](#).

**Hosts in state condition Untrusted rootkit detected:** This number of hosts are in the Untrusted rootkit detection state. See [Setting State Conditions, page 5-13](#).

**Hosts in state condition Unprotected access detected:** This number of hosts are in the Unprotected access detection state. See [Setting State Conditions, page 5-13](#).

**Hosts with unsupported platform:** These hosts are attempting run Cisco Security Agent software on an unsupported operating system.

**Hosts without Cisco Trust Agent installed:** These hosts do not have CTA software installed.

**Hosts with Cisco Trust Agent installed but inactive:** These hosts are running CTA software that is inactive and not providing a posture.

**Hosts not actively polling (status unknown):** These host are running agent software that has missed three polling intervals or has not polled in to the MC in the past 24 hours.

**Hosts without Application Deployment Investigation data upload:** These hosts do not have Application Deployment Investigation enabled. See [Configuring Groups, page 3-4](#).

**Groups with no policies attached:** The MC has this number of groups configured with no policies attached and therefore no policy enforcement associated with these groups.

**Query rules with saved answer in the past 24 hours:** The number displayed here links to query rules that have triggered and been responded to on host systems.

### **Most Active**

Use the links available in the Most Active section to view the Hosts, Rules, Applications, or Rule/Application pairs that have been the most active or triggered the most (logged the most events to the MC). This information is useful to help you tune your policies for rules that are being tripped too often. This can also alert you to common unwanted occurrences that may be triggering across your enterprise. Additionally, you can purge the events that appear in these lists.

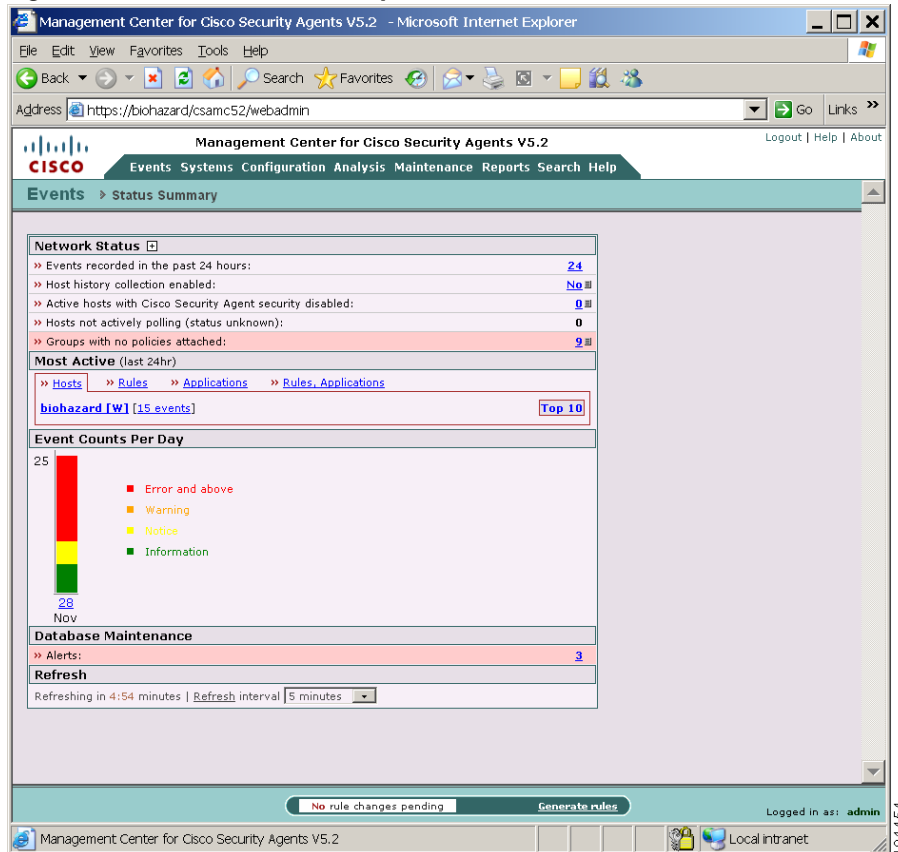
### **Event Counts Per Day**

A colored graph displays the event log according to severity level. Click on a color in the graph to view logged events of that severity level.

### **Database Maintenance**

If there is an alert present in the **Database Maintenance** category, we recommend that you access the Database Maintenance page from **Maintenance** in the menu bar and shrink the database. See [Database Maintenance \(Free Up Disk Space on CSA MC\)](#), page 12-8 for details.

Figure 2-11 Status Summary View



1317454

## CSA MC Views and Navigation

**List View**—Each CSA MC configuration category has a top level list view. This list view displays a list of links, each of which represent a configured item for that category. It is from this list view that you create configurations and delete existing configurations. Buttons for New, Clone and Delete actions are present on list view pages. From the list view, you click an item link to access the configuration page for that item.

**Configuration View**—Access the configuration view for an item by clicking on that item in the list view. Configuration views may contain edit fields, radio buttons, checkboxes, and/or listboxes depending on the configuration requirements. Enter the necessary information and click **Save** to store data in the CSA MC database. Configuration views contain Save and Delete buttons. See [Creating, Saving, and Deleting Data, page 2-33](#) for further details.

**Navigation Tools**—The heading link (below the menu bar, see [Figure 2-12](#)) contains hierarchal links for the item you’re configuring. Use these header links to switch between top level list views and subcategory configuration views. For example, in [Figure 2-12](#), the header bar contains links to the top level Policies list view and the MS IIS Server policy. Note that leaving a configuration view without clicking the Save button causes any newly entered data to be lost.

**Show reference list**—Configuration items that are used in other configurations have a “Show reference list” link on their pages. Clicking this link displays all the configurations where the current item is used. This display also links to the items that are shown.

**Note**

---

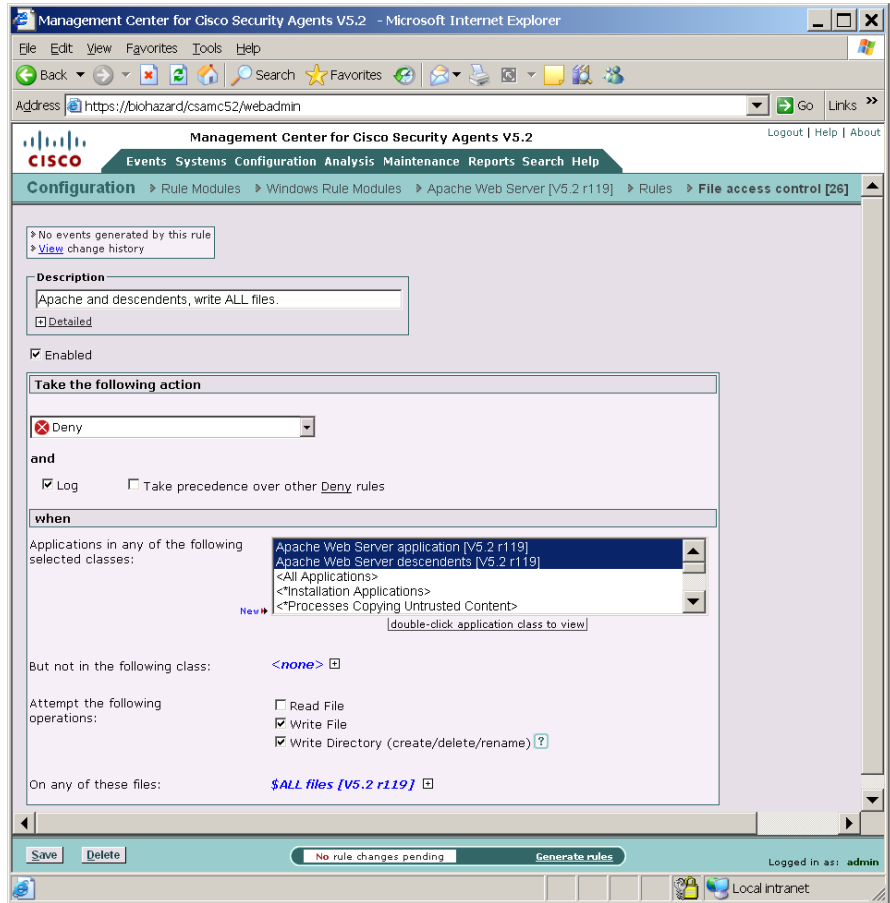
You can click the gray arrow on the right side of the Policy list page to go directly to the rules contained in the policy.

---

**Configuration Shortcuts**—Rule pages allow you to insert pre-configured variables such as file sets and COM components into your rules. If there is no pre-configured variable that you wish to use and you want to create a new one, you can do it without leaving the rule page. When you click the Insert link beside any edit box in the rule page, there is a New item in the list that appears first. Selecting the "New" item pops up a configuration page for that variable type. You can then configure a new variable and use it in the rule without having to leave the rule page to access the variable page. You can double-click on an existing item to view its configuration page.

Application classes also have a shortcut you can use to create a new item. Clicking the New link beside the list of application classes in each rule configuration page lets you create a new application for your rule.

Figure 2-12 Configuration View



# Creating, Saving, and Deleting Data

## CSA MC Button Frame

All CSA MC action items appear in a frame at the bottom of CSA MC. The buttons in this frame change in accordance with the actions available for the page you're viewing. Available CSA MC buttons and links are as follows.

**Generate rules (pending changes)**—When you are ready to deploy your configuration (policies, rules, variables, etc.) to Cisco Security Agent systems, you must click this link in the bottom frame to view all pending database changes and then to generate them. (See [Chapter 4, “Building Policies”](#).)

**New**—Use the New button to create a new configuration item within the list view you have selected. Click the New button and a new item appears in the list view. Click the new item link to access the configuration view for that item.

**Clone**—Use the Clone button in conjunction with the checkboxes beside each list view item. To clone a particular configuration, select its checkbox and click the Clone button. You can clone one item at a time. New links to the cloned configurations appear in the list view.



---

**Note**

In most list view pages in CSA MC, there are New, Clone, and Delete buttons (Clone is not present in all list views as you can only clone certain configurations)

---



---

**Note**

When you clone an item, such as a policy, that contains variable items like file sets or network services, the cloned rule uses the same variables used in the original rule. The variables themselves are not cloned.

---

**Delete**—Use the Delete button in conjunction with the checkboxes beside each list view item. To delete a configuration, select its checkbox (you can select several at once) and click the Delete button. All checked items are deleted. To quickly select all checkboxes, click the very top checkbox in the list view heading bar. Clicking the Delete button then deletes all items.

**Save**—When you enter configuration information, whether you are entering new data or editing existing data, you must click the Save button once you are finished to save your configuration in the CSA MC database. If you do not click Save before moving to another page in CSA MC, your data is lost.

**Note**

Although your information is stored in the database when you click Save, it is not distributed to the agents across your network until you generate rules. See [Using Learn Mode, page 5-11](#) for further information.

**Compare**—Groups, Policies, Rule Modules, Variables, and Application Classes provide a Compare button in their item list views. When you select the checkbox next to 2 items (you cannot compare more than 2 configurations at a time) and click the Compare button, CSA MC displays the configurations side by side and highlights the differences in red. Once you've examined how the configurations compare, you can select to merge them.

**Note**

The purpose of this compare tool is to assist you after you've imported configurations or upgraded CSA MC. These processes can cause you to have duplicate or very similar configuration items. Comparing and merging configurations can help you to more easily consolidate duplicate items. See [Chapter 4, "Building Policies"](#) for details on using Compare to merge configurations.

**Note**

Right-clicking your mouse on a CSA MC page displays a shortcut menu for performing the tasks provided by buttons on that page and for additional configuration tasks not as easily accessible from the current page you're viewing.

# Using the Correct Syntax

CSA MC contains text fields that require you to enter information using a specific syntax. Most of the text fields in these pages are similar and require similar syntax. The text fields are categorized and listed below with the required syntax.

When using configuration variables in rules, application classes, and alerts you must enter the variable name preceded by a dollar sign. The insert links beside each text field automatically insert variables using the correct syntax.

For example, if you have a file set variable named Web Browsers, clicking the Insert File Set link lets you select Web Browsers. It then places \$Web Browsers in the corresponding field using the correct syntax. The dollar sign tells CSA MC that this is a variable value.

When entering a Name for any item you configure, use the following syntax:

Names of items must be unique per operating system. Items may only have the same name if they have different operating system designations. (Host names, however, do not have to be unique.) All 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 \_ . (Note one exception, agent kits do not accept spaces in names.)

## File entry text boxes require:

In a list of items, each item must appear on a single line. Do not specify multiple items on a single line.

Leading and trailing spaces are removed from each line. Other spaces, such as the one located in "Program Files" are recognized. To indicate leading or trailing spaces you must use special characters. The following special characters are recognized. (Note that the need to use the characters listed below should occur very rarely.)

- 'b Leading/Trailing Space
- 't Tab
- 'n Line feed
- 'r Carriage return

**Note**

---

If you want to use a single quote (') in a file name, you must enter two single quotes (") for CSA MC to recognize the syntax correctly. Two single quotes are seen as one quote.

---

Local system files are entered using full path and disk drive.

Windows:

```
c:\Program Files\Outlook\msimn.exe
```

```
c:\winnt\regedit.exe
```

You can also use @fixed to indicate all local system drives without having to indicate the drive letters.

For example, @fixed:\Program Files\Outlook\msimn.exe

UNIX:

```
/etc/passwd
```

Local system files are entered using full path and disk drive (Windows) with optional wildcard notations.

Windows

```
c:\Program Files\Outlook\*.exe
```

UNIX

```
/usr/bin/*
```

**Note**

---

Windows peripherals, such as floppy and CD drives, can be referenced by their drive letter.

---

Use the wildcard notation (\* or ?) to indicate files within directories and whether directories and subdirectories are recursive.

**Table 2-2 Wildcard Operators**

Example	Translation
*	One wildcard entry indicates a single directory level or all files in a specified directory.
**	Two wildcards entered in this manner indicate a recursive directory path (including all directories, passing down as many levels as exist in the path).
?	Use the question mark wildcard to represent a single character. For example, ??? .doc. This indicates a file name containing only three characters with a .doc extension.

For example:

The following entry indicates all files one directory level down in the winnt directory. It does not include files in the winnt directory itself.

```
c:\winnt\*\*
```

The following entry indicates all files in the winnt directory and all subfolders recursively (digging down as deep as necessary) and files.

```
c:\winnt\**\*
```

The following entry indicates all files in the winnt directory and all subfolders recursively (digging down as deep as necessary) and files that contain exactly two characters in their name and have any extension.

```
c:\winnt\**\??.*
```

If you do not specify a drive path in a file text field, CSA MC always prepends the string \*\*\ to the named file. For example, if you enter foo.doc into a text field, it is saved as \*\*\foo.doc.



**Note**

You can use the same wildcard notations for indicating UNIX files and directories.

## File and Directory Protection

File access control rules provide three checkboxes which offer you the option of protecting files and/or directories. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.



### Caution

Directory protection ignores the file portion of the specified path and only matches the directory portion of the path. If the directory portion is not well specified, the protection will be overly broad. For example, if you select to protect a directory in a deny rule and enter the directory path as follows: `**\Program Files\**\Outlook.exe`, then no directories can be modified under Program Files. That is an overly broad protection to specify and would likely result in system instability. If you choose to protect directories, be sure to get very specific in your path string and understand the resulting behavior.

When protecting against directory creation, in particular, you should note that directory creation applies to an exact directory path match, but directory write and rename protection applies to all directories explicitly named in a path. If a directory name is completely wildcarded `\**\`, no protections exist for that particular component of the directory.

The following Windows example displays what protections exist for a literally entered resource in a Deny, File access control rule where the following checkboxes are selected: Read File, Write File, and Create, Delete, Rename Directory.

Example:

```
**\Program Files\**\*SQL*\bin\*.exe
```

In the example above, the following protections exist:

- Directory protection: `**\Program Files` cannot be renamed or deleted, but it can be created.
- Directory protection: `**\Program Files\**\*SQL*` cannot be renamed or deleted, but it can be created.
- Directory protection: `**\Program Files\**\*SQL*\bin` cannot be renamed, deleted, or created.
- Directory protection: A new directory cannot be created which matches `**\Program Files\**\*SQL*\bin`

- File protection: Executable files located in the specified directory path cannot be read or written to.

In the following UNIX example, `/usr/adm/sg/` is the directory and `x`, `y`, and `z` are files in the `sg` directory.

The following entry protects files `x`, `y`, and `z` in the `sg` directory and it protects the directory structure (if all checkboxes are selected in the File access control rule).

```
/usr/adm/sg/*
```

This example works just like the previous Windows example. Therefore, directory creates are only prevented if the directory attempted to be created exactly matches the entire path of `/usr/adm/sg/*`. Directory deletes and renames are prevented for each directory named in the path. Note that the only file protection provided here is within the `sg` directory because the last entry in a path is always assumed to be the file. If you only wanted to provide directory protection and not file protection, you would still have to enter the literal in the same manner. You must provide `/*` at the end of the path or the last entry would be seen as a file rather than a directory. In this case, you would only select the Write Directory checkbox and even though all files in the `sg` directory are specified, they are not protected.

To protect files in the `usr` directory, you would have to make that another entry, e.g. `/usr/*` would have to be entered on another line below the original UNIX example. (Note that Windows works the same way.)

For UNIX directory entries, because there is no drive letter to specify (as in Windows) the wildcarded path (`/**/`) is not automatically placed in front of a UNIX path that begins with “/”. If you begin the path with a forward slash, the directory path is taken literally. If you do not place a slash in front of the path, a wild card path is inserted before the entry when you save the rule.

**Caution**

You must make some file specification when you are entering literal paths. A wildcard is acceptable to specify all files in a named directory. CSA MC always assumes the last entry in a literal path (not a variable) is a file.

**Caution**

**Symbolic Links**—For UNIX, if you create a File access control rule to protect a symbolic link, **ONLY** that symbolic link is protected. The underlying resource, unless also specified, is **NOT** protected. For example, a File access control rule written for `/etc/hosts` does not protect `/etc/inet/hosts`. Similarly, a File access control rule written for `/etc/inet/hosts` does not protect `/etc/hosts`. If you want to

protect a symbolic link and its underlying resource, both must be specified in the rule. See [Resource Access Control, page 6-80](#) for further symbolic link protection information.

You can use the following "short hand" entries in File Sets, File access control rules, File monitor rules, and Application classes to indicate common system directories. The @symbol must appear at the start of the short hand name. These entries resolve to the Windows directory on each agent system.

**Table 2-3 Sample Short Hand File Tokens (Windows only)**

Example	Translation
@windows	Use @windows to indicate the directory pointed to by the %SystemRoot% environment variable  When using @windows, for example, in the File access control rule Files field, it is interpreted as @windows\* to indicate the files within the directory.
@system	Use @system to indicate %SystemRoot%system32
@(regpath Registry key/value pair default=default directory)	Use @(regpath Registry key/value pair default=default directory) to localize the directory structure of an application or other resource. This is useful to indicate software regardless of the directory to which it has been installed. Note that the default= field is optional but recommended, For example:  @(regpath HKLM\CCS\foo\instmdir default=**\Program Files\foo\bin)
@dynamic	Use @dynamic in the File set text field to indicate all files that have been quarantined by CSA MC as a result of correlated suspected virus application events, correlated virus scanner log messages, or files that were added manually by the administrator. This list updates automatically (dynamically) as logged quarantined files are received.  To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the Manage <b>dynamically quarantined files</b> link on the Global Event Correlation page. See <a href="#">Manage Dynamically Quarantined Files and IP Addresses, page 7-8</a> for more information.

You can use the following "short hand" entries in File Sets and in File access control and File monitor rules to indicate removable media. The @ symbol must appear at the start of the name. These entries resolve as follows:

**Table 2-4 Removable Media Token Syntax**

Example	Translation
@removable	This indicates all removable media. That includes, floppies, CDs, zip drives, etc. Note that if you want to indicate all removable media except floppies, for example, you'd have to configure a file set that explicitly excludes floppies from all removable media.
@floppy	This indicates all floppy drives. You can specify particular file paths on floppy media using the following syntax: @floppy:\<specify wildcards or paths>. Note that @floppy:\ means only the top level files on the floppy media. @floppy or @floppy:\** means all files on the floppy media.
@CD	This indicates all CD-ROM drives(including DVD). You can specify particular file paths on CD media using the following syntax: @CD:\<specify wildcards or paths>. Note that @CD:\ means only the top level files on the media. @CD or @CD:\** means all files on the media.



**Note**

USB connected drives are removable media.

You can also use **@fixed** to indicate all local system drives without having to indicate the drive letters. For example, @fixed:\Program

Files\Outlook\msimn.exe.

For correct directory path specifications on internationalized Windows versions, you can use the following universal tokens in File Sets, File access control rules, File monitor rules, and Application classes to indicate common system directories for the localized version of the OS. These entries resolve to the appropriate Windows directory on each localized agent system.

**Table 2-5 Universal Tokens for Localized Directory Paths**

Token	Translation
@startup	The file system directory that corresponds to the user's startup program group. The programs in the startup group start automatically when the user logs in.
@startmenu	The file system directory that contains the programs and folders that appear on the start menu for all users.
@program_files	This represents program files and program files\common. This folder is for installed programs and for components that are shared across applications.
@mydocuments	This represents documents and my documents. This folder contains documents that are common to all users.
@desktop or @desktopdirectory	The file system directory that contains files and folders that appear on the desktop for all users.



**Note**

When you specify one of the tokens in the table above, the next component is automatically wildcarded. This is necessary to correctly resolve the specified directory path.



**Tip**

Use the diagnostics tool on the Host page to view what a token translates to for an individual host.

**Network system paths (Windows only) entered using the following syntax:**

```
\\<machine name>\<share>\<path>\<filename>  
\\Backup_Server\finance\records\database.db
```

You can also use **@network** (on Windows and UNIX) to indicate all network shares. For example, @network:\finance\records\database.db

**Caution**

---

Do NOT enter a drive letter for network share paths.

---

**Network address text boxes require addresses entered in any of the following formats:**

Enter single fully qualified addresses.

```
a.b.c.d
```

Enter address ranges.

```
a.b.c.d-y.z
```

This address range indicates all addresses from a.b.c.d-a.b.y.z

Enter address ranges using "network address class" notation.

```
10.0.0.0/24
```

This address range indicates all address from 10.0.0.0 to 10.255.255.255

You can use the following "short hand" entry in Network Address Sets and in Network Access Control rules to indicate all local addresses on the agent system in question. The @ symbol must appear at the start of the short hand name.

Use **@local** to indicate all local addresses on the agent system.

Use **@remote** to indicate all addresses that are not on the local agent system.

Use **@subnet** to indicate the local subnet addresses of the agent system. This is useful for allowing communications on your internal network but not to the outside world. This gives you more granularity for specifying internal communications without having to know all subnet addresses.

Use **@recent** to track addresses with which agent systems have recently communicated. This is useful for restricting callback connections to addresses with which you've recently initiated communications. You can also use this to restrict server connections to only those hosts that have initiated the control channel.

Use **@dynamic** in the Network address set text field to indicate all IP addresses that have been quarantined by CSA MC as a result of correlated communications with untrusted hosts events or IP addresses that were added manually by the administrator. This list updates automatically (dynamically) as logged quarantined IP addresses are received.

To view the IP addresses that are added to the dynamically quarantined IP addresses list and to manually add IP addresses to be quarantined, click the Manage dynamically **quarantined IP addresses** link on the Global Event Correlation page. See [Manage Dynamically Quarantined Files and IP Addresses, page 7-8](#) for more information.

Use **@smb-null-session** in Network access control rules (as the network service). A null session is an unauthenticated session to one of the NetBIOS or CIFS ports on a system. These ports are typically used for file and print sharing, but they can also be used as an attack vector (e.g. SMB die). Use the **@smb-null-session** token to control connections to the system via an unauthenticated null-session.

**Caution**

---

On UNIX platforms, IPV6 addresses are not officially supported; however, an IPV6 connection will work as the applied rules dictate if the address in question is covered by the "all" addresses range (0.0.0.0-255.255.255.255 includes IPV6 addresses) or by **@local**. Local addresses on the agent system (indicated by **@local**) also include IPV6 addresses.

---

See [Network Access Control, page 6-28](#) for more information.

**Network service text boxes require protocols and port ranges entered in the following formats:**

Format all entries as:

```
protocol/port or port range
```

```
TCP/80
```

```
UDP/53
```

```
TCP/1024-65535
```

The protocol here is either "TCP" or "UDP".

Port ranges are designated in the range 0-65535.

Designating ephemeral ports—In some cases, an application may want to offer a temporary service port for callback data connections. An ephemeral port is a temporary system-assigned port for this purpose.

For example, an ephemeral port would be the likely data connection for active FTP. If you do not specify an ephemeral port range for accepting an active FTP connection, you would have to allow clients to listen on a wide range of ports to accept this connection type. This would unnecessarily open a wide range of data channels and possibly create a vulnerability that could be exploited by a Trojan.

You can specify an ephemeral port range for a Network service as follows:

```
TCP/ephemeral
```

```
UDP/ephemeral
```

**Note**

---

It only makes sense to use ephemeral ports on systems accepting connections. Also note that Deny log messages triggered by a rule using an ephemeral port range appear in the event log containing the real port number.

---

**Caution**

---

Ports that are ephemeral allocated are only matched against an explicit ephemeral class. Ephemeral ports are treated as "port 0" for rule comparisons. For example, ephemeral port 2000 matches port 0, not port 2000.

---

