



CHAPTER 12

Using Management Center for Cisco Security Agents Utilities

Overview

The Management Center for Cisco Security Agents provides various utilities for advanced product maintenance tasks that extend beyond the administrator configuration and policy generation tasks done through the CSA MC user interface. Those utilities are documented here.

This section contains the following topics.

- [Start and Stop Server Service, page 12-2](#)
- [Start and Stop Agent Service, page 12-2](#)
- [Backing Up Configurations, page 12-3](#)
- [Restoring Backup Configurations, page 12-6](#)
- [Database Maintenance \(Free Up Disk Space on CSA MC \), page 12-8](#)
- [Using the Webmgr Utility, page 12-10](#)
- [Using the COM Extract Utility, page 12-11](#)
- [Manual Agent Data Filter Installation, page 12-12](#)
- [Exporting and Importing Configurations, page 12-16](#)
- [View Import History, page 12-21](#)

- [Cisco Security Agent Posture Plug-in for CTA, page 12-22](#)

Start and Stop Server Service

As needed, you can start stop the Management Center for Cisco Security Agents service on a host by running the following commands from a command prompt window on the server host system:

From the CSA MC /bin directory, run the following:

To stop the service:

```
csacontrol.exe -c end -t s -a <login name> -p <password>
```

To start the service

```
csacontrol.exe -c start -t s -a <login name> -p <password>
```

Start and Stop Agent Service

As needed, you can start and stop the Cisco Security Agent service on a Windows host by running the following commands from a command prompt window on the agent host system:

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

As needed, you can start and stop the Cisco Security Agent service on a UNIX host by running the following commands from a command prompt window on the agent host system:

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

**Note**

Running this stop command to stop the agent service on a system disables all rules on that system. Running a start csa command starts the agent service and reinstates all rules.

The shipped UNIX rule module, "Secure Management Module," allows secured management applications to stop the agent service. For example, after having logged in by selecting Command Line Login from the login screen in the options

menu, you can issue the command `/etc/init.d/ciscosec stop`. Refer to the policy in CSA MC to see how these secured management applications are already defined and may be modified using application builder rules.

**Note**

The UNIX agent has a utility (csactl) to provide capabilities that the Windows agent provides in its user interface. See [Appendix A, “Cisco Security Agent Overview”](#) for details.

If an agent has a policy containing an Agent service control rule that denies the stopping of the agent, administrators cannot stop the agent service on the system in question. See [Agent Service Control, page 6-3](#).

Backing Up Configurations

It is a good idea to back up your management server configurations at regular intervals. If your server system fails for any reason, and a copy of your configuration database is not stored elsewhere, you could lose your policy information.

**Caution**

Specifically, it is recommended that you backup all necessary files, at least once a week (e.g. auto-backup on Monday at 1 AM), to a safe, remote, and unique location for each backup. This way, previously backed up files are not overwritten by new ones.

**Caution**

The CSA MC Backup Configuration feature is not available if you are using a remote database configuration.

The **Backup Configuration** feature, available from the **Maintenance** category in the menu bar, lets you backup your local database at regularly scheduled intervals or as needed.

To backup your CSA MC configuration, do the following.

-
- Step 1** Move the mouse over **Maintenance** in the menu bar and select **Backup Configuration** from the drop-down list that appears.
- Step 2** In the Backup Configuration window you can select the following radio buttons:
- **No database backup**—Select this option if you do not want backups to occur automatically at scheduled intervals but want to perform them manually. After selecting this radio button, enter the **directory path** (including drive letter) to which you want to save your backup configuration. Then click the **Backup now** button.
 - **Scheduled database backup**—Select this option to schedule regular backups and then choose one of the scheduled backup options: Low frequency, Medium frequency, and High frequency. Enter the directory path (including drive letter) to which you want to save your backup configuration and click the Save button. Backups will now occur as scheduled.

Backup types are categorized as follows:

full—A full backup occurs every Sunday night at midnight. This full backup includes the entire database with license information.

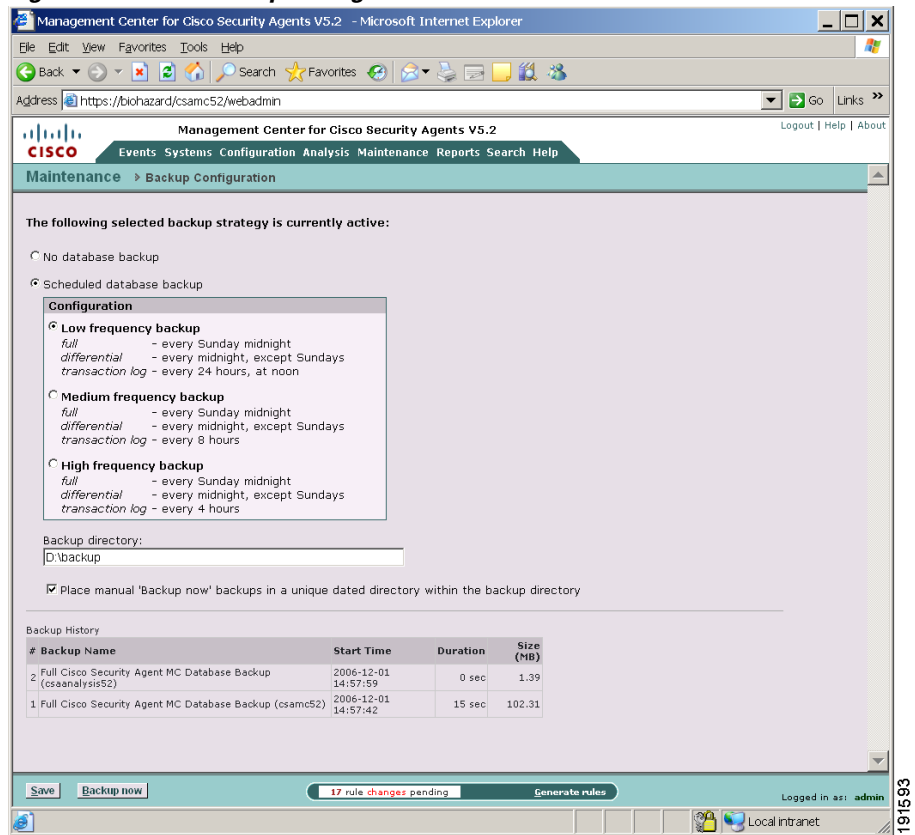
differential—This type of backup occurs every night at midnight (except Sunday nights when a full backup occurs). A differential backup includes only data that has changed since the last backup (full or differential) occurred.

transaction log—This backup occurs every 24 hours (low), 8 hours (medium), or 4 hours (high) depending on the frequency you select. The presence of this transaction log allows administrators to back out configuration changes to a certain point. Please refer to Microsoft documentation for details about the transaction log.



Note When you configure a scheduled database backup and click **Save**, an initial backup is performed immediately.

Figure 12-1 Backup Configuration Window



Backup Files appears as follows in the directory you select:

- full_backup_[db_name].bak—for full backups
- diff_backup_[db_name].bak—for differential backups
- log_backup_[db_name]_[x].bak—for log backups, where x is an integer from 1 to 23 (backup hour)
- crt_log_backup_[db_name].bak—for current transaction log backup

- Step 3** Optionally, click the **Copy manual 'Backup now' backups to a unique dated directory within the backup directory** checkbox. With this checkbox selected, when you click the Backup now button (only when you manually click the Backup now button), the backup file is saved to the specified directory and a copy is saved to a unique directory.

Restoring Backup Configurations

Restore backup CSA MC configurations, including database, license information, and transaction logs by running the Restore utility, called **Restore Configuration**, located in the default CSAMC52\bin directory:

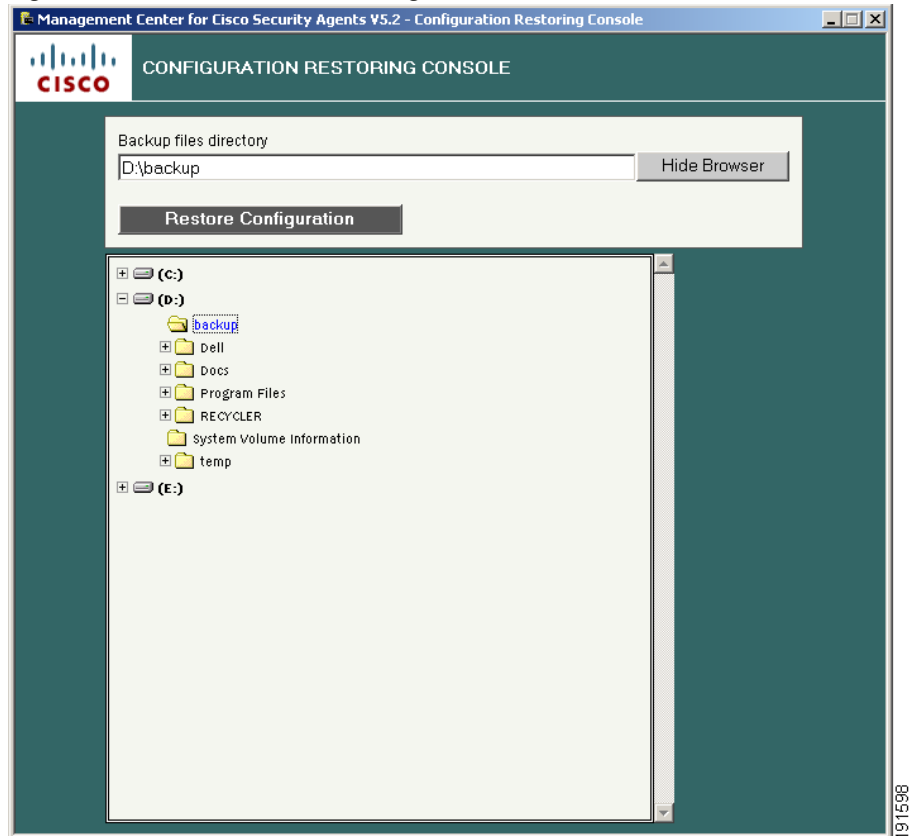


Note

If you are restoring a backup configuration due to a disk failure, after you re-install CSA MC and then restore the backup configuration, you may find that the final set of uncommitted transactions (no rule generation occurred) were lost.

- Step 1** Double-click the **Restore Configuration** file (located in the CSAMC\CSAMC52\bin directory) to display the CSA MC restore user interface. See [Figure 12-2](#).
- Step 2** Enter or browse to the directory path where the backup files are stored.

Figure 12-2 Database Restoring Console



- Step 3** Click the **Restore Configuration** button. When you click the Restore Configuration button, you are asked if you want to restore the backup configuration. Click **Yes** to do so.

The restore process now takes place. Once the restore is complete, a log file, the Database Restoring Log, is displayed.

**Note**

When you restore backup configurations, you cannot select to restore only the transaction log, or only a differential backup. All files are automatically restored from the most recent backup that exists in the directory. It is recommended that you reboot the system after restoring from backup.

Database Maintenance (Free Up Disk Space on CSA MC)

The **Database Maintenance** page is available from the **Maintenance** category in the menu bar. If you access this page and find that there are checkboxes available next to the database type(s), then the recommendation is for you to shrink your database files and log files to increase the amount of free disk space on your CSA MC system.

If the **Database Maintenance** category on the **Status Summary** page is issuing an alert about the database size or if your CSA MC event log contains an "insufficient disk space" message, this is an appropriate procedure for freeing up space.

**Note**

If no checkboxes appear on this page, your database size is currently sufficient.

The following information points explain what you see on this Database Maintenance page:

Database csamc52

If you are using a database that is remote to the CSA MC system, you will see only this database category on this page. The database size is broken into two categories: **Event and configuration data** and **Application Deployment data**.

If the **Unallocated space** number listed on this page is more than 10% of the database size, a checkbox appears beside Database csamc52. If the checkbox is present, it is recommended that you select it and click the **Shrink database** button available from the bottom footer of this page.

Note that **Transaction log size** is also displayed here. SQL Server 2005 breaks that out as a separate category when calculating the database size.

The **Event full-text search** function is present here and disabled by default. (See [Figure 12-3](#).) Enabling this feature allows you to utilize the SQL Server full-text search function. If this feature is disabled and you perform an event text-filtering search, when it completes, we will warn you that you can enable this feature to perform a full-text search. NOTE that full-text search configuration changes can only be performed if the db user is part of the

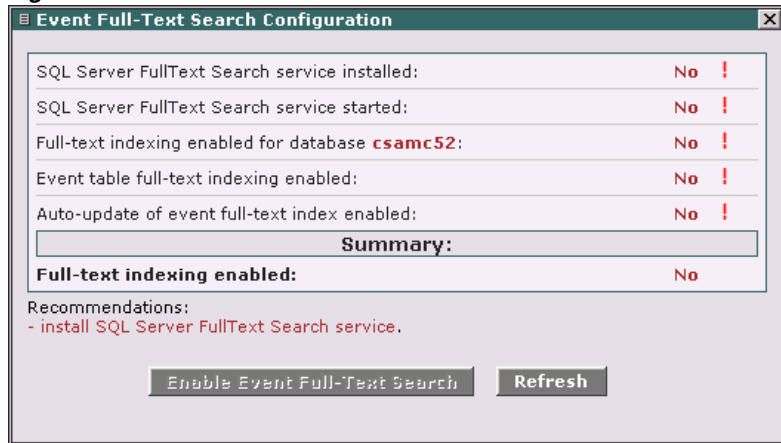
db_owner fixed database role (for remote db this is not required). If the full-text enabling/disabling fails, you will see a message advising you to adjust the db user rights or run the operation from the command line.



Note

Full-text searching is an optional component of SQL Server. When installed, it offers additional string querying abilities such as string comparisons similar to internet search engines, returning both results and a matching score or weight. Without full-text searching, string matching is usually limited to an exact match, or a wildcard match. Full-text searching allows for searching for phrases, groups of words, words near one another, or different tenses of words.

Figure 12-3 Event Full-Text Search Function Window



Database csaanalysis52 (behavior analysis data)

If you are using a database that is local to the CSA MC system, you will see this database category in addition to the one above. You can shrink only this database or the csamc52 database, if necessary (if both checkboxes are available). If the **Unallocated space** number listed here is more than 10% of this database size, a checkbox appears beside Database csaanalysis52 (behavior analysis data). If the checkbox is present, it is recommended that you select it and click the **Shrink database** button available from the bottom footer of this page.

**Note**

Even if both database categories are present, these are separate databases and their space allocations are independent.

**Note**

Maintenance operations for remote databases must be done manually with the CSA MC service stopped (`net stop csamc52`).

Using the Webmgr Utility

Use the `webmgr` (webmanager) command to add a new administrator with monitoring rights to the CSA MC database without accessing the user interface. Running `webmgr` also lets you unblock an existing administrator and reset their password. You would want to do this in cases where an administrator is locked out of the MC due to too many invalid login attempts (25 invalid login attempts allowed before administrator blocking occurs).

Using this utility, you can also log out all currently logged in administrators, effective immediately. This is useful if the server has reached the maximum number of administrators that can be logged in at once (20 admins can be logged in to the MC at the same time).

From a command prompt window, run `webmgr` from the `CSAMC\CSAMC52\bin` directory. It displays the syntax required to make the administrator changes described above.

- Add a new administrator by entering the new name and new password followed by your existing user name and password, as follows:

```
webmgr newuser NAME PASSWORD DESCRIPTION
EXISTINGNAME EXISTINGPASSWORD
```

**Note**

If you have spaces in the description part of your entry, you must put quotation marks around the entire description phrase.

- Unblock an existing administrator (resetting the password) by entering data in the following manner:

```
webmgr unblock NAME OLDPASSWORD NEWPASSWORD
```

- Log out all currently logged in administrators:
`webmgr clearsessions`

Using the COM Extract Utility

CSA MC provides a COM component extraction utility on agent systems, called `extract_com`, which installs in the `\Cisco Systems\CSAgent\bin` directory with each Cisco Security Agent. Running this utility extracts all COM component PROGID's and CLSID's for software running on the system in question and places this data into a text file. You can cut and paste these ID's from the text file into your COM component sets and access rules.

Run the `extract_com` utility on an agent system in the following manner:

Step 1 Open a command prompt window.

Step 2 From the `\Cisco Systems\CSAgent\bin` directory type in `extract_com filename`

"filename" is the name of the text file you want the utility to create. It is into this file that all COM PROGID and CLSID data is placed.

For example, enter:

```
\Cisco Systems\CSAgent\bin>extract_com foo.txt
```

The Cisco Security Agent creates the "foo.txt" file in the same `\bin` directory as the `extract_com` utility. You can access it from there.



Caution

Both COM Component access control rule fields and Variable COM Component set fields require a very specific syntax for entering PROGID's and CLSID's. The COM component file created by the `extract_com` utility may display PROGID's and CLSID's without the proper syntax in the output file. Despite this, when you enter these ID's into text fields for rules or variables you **MUST** use the correct syntax detailed on [page 9-3](#).

Manual Agent Data Filter Installation

On Windows platforms, if you install Web server software (IIS or Apache) after you install the Cisco Security Agent on the server system, or if you have installed the Web server in a directory other than the default, you must manually install the Cisco Security Agent data filter in order to use Data access control rules on the system in question.

**Note**

If your Web server software is already installed (in its default directory) when you install the agent on Windows, the server software is detected by the agent and the data filter capability is automatically installed with the agent.

On Solaris and Linux, in order to use Data access control rules (on Apache servers for Solaris and Linux) you must install the data filter manually after you install the Cisco Security Agent. Unlike Windows, the Solaris and Linux installations do not detect Web server software and do not install the data filter with the agent. You must always manually install it.

Install Data Filter on Windows

If you have installed Web server software (IIS or Apache) after you install the Cisco Security Agent on the server system, or if you have installed the Web server in a directory other than the default, run the following command(s) to manually install the CSA data filter on the server system making use of Data access control.

For a Microsoft IIS Web server, run the following command:

```
csa_datafilter -i iis
```

For an Apache Web server, run one of the following Apache version appropriate commands:

```
csa_datafilter -i apache13 <.conf file with full path name>  
<modules directory path>  
csa_datafilter -i apache20 <.conf file with full path name>  
<modules directory path>
```

For example, if Apache 2.0 was installed with its default settings after the agent is installed, you would run the following command to install the data filter:

```
csa_datafilter -i apache20 "c:\Program  
Files\Apache\conf\httpd.conf" "c:\Program  
Files\Apache\modules"
```



Note

If there are spaces in the directory path, you must put quotations around the pathname.



Caution

You must restart the web server service after the data filter is installed for data access control rules to take effect.

Uninstall Data Filter on Windows

For a Microsoft IIS Web server, run the following command to uninstall the data filter:

```
csa_datafilter -u iis
```

For an Apache Web server, run one of the following Apache version appropriate commands to uninstall the data filter:

```
csa_datafilter -u apache13 <.conf file with full path name>  
<modules directory path>  
csa_datafilter -u apache20 <.conf file with full path name>  
<modules directory path>
```

Install Data Filter on Solaris or Linux

Run the following command to manually install the CSA data filter on the server system making use of Data access control.

```
webserver:root>./csa_datafilter -i  
[output:]
```

```
CSA web server filter installation:  
Enter the path of the Apache root (null for none):  
webserver:root>
```



Caution

You must restart the web server service after the data filter is installed for data access control rules to take effect.



Note

On Linux, Data access control rules are only supported for Apache 2.0 servers.

Uninstall Data Filter on Solaris or Linux

```
webserver:root>./csa_datafilter -u
[output:]
SA web server filter removal:
Should I uninstall filters for Apache [No] y
Enter the path of the Apache root (null for none):
webserver:root>
```

Exporting and Importing Configurations

Under the Maintenance category in the menu bar, use the Export utility to export your policies to other CSA MCs. If you have multiple CSA MCs, you might want to export some basic policies to those servers for deployment. Likewise, using the Import utility, you can download and import those policies as well as preconfigured policies that Cisco provides.

**Note**

The Export utility exports entire rule modules and policies (not individual rules), including the accompanying application classes and configuration variables. Because of communication channels established in the original configuration, some site-specific imported configuration information (IP addresses) may not work on another server. Exporting an item will also export related data. In particular, exporting policies will export application classes and configuration variables referenced in rules within the policy. Exporting a group will export associated policies but not hosts.

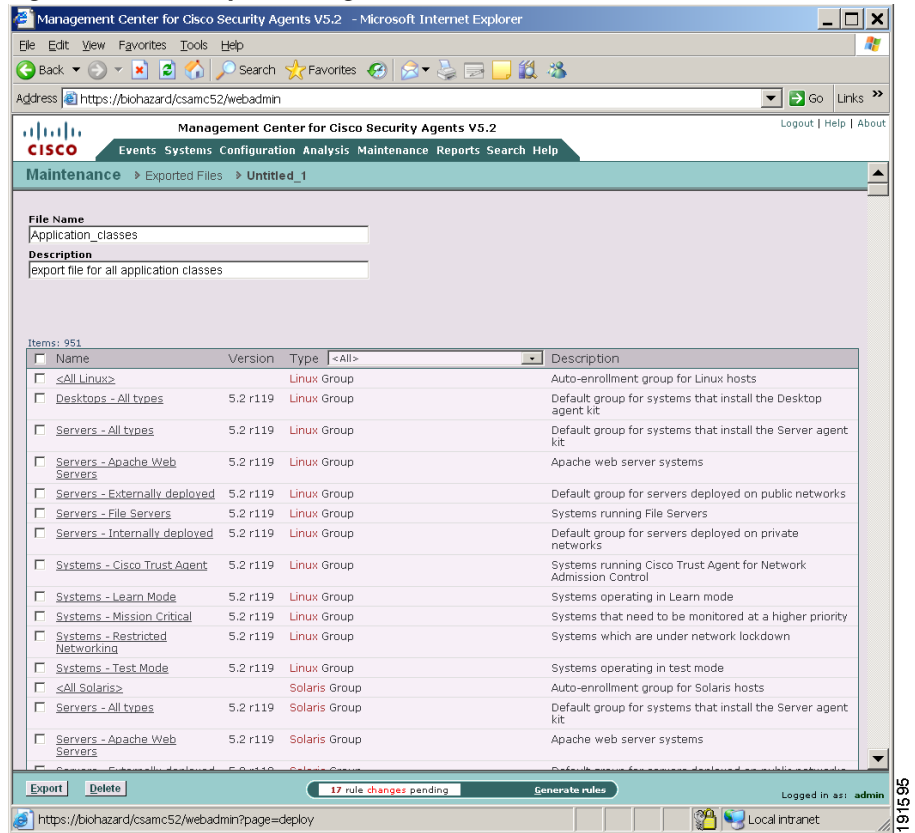
**Caution**

The Export/Import functions are not intended to be used as a backup/restore mechanism as they do not preserve system specific information such as group-host memberships.

To Export configurations, do the following.

-
- Step 1** From the menu bar **Maintenance** drop-down list, move the mouse over **Export/Import**. A cascading menu with further selections appears. Select **Export** from the drop-down list that appears. Any previously exported files are shown.
 - Step 2** Click the **New** button to create a new exported file. This takes you to a checkbox list of all configuration items.
 - Step 3** **Check** the box beside the configurations you want to export. (See [Figure 12-4](#).) (You can also select the top checkbox beside the Name field to select all items.)

Figure 12-4 Export Configurations

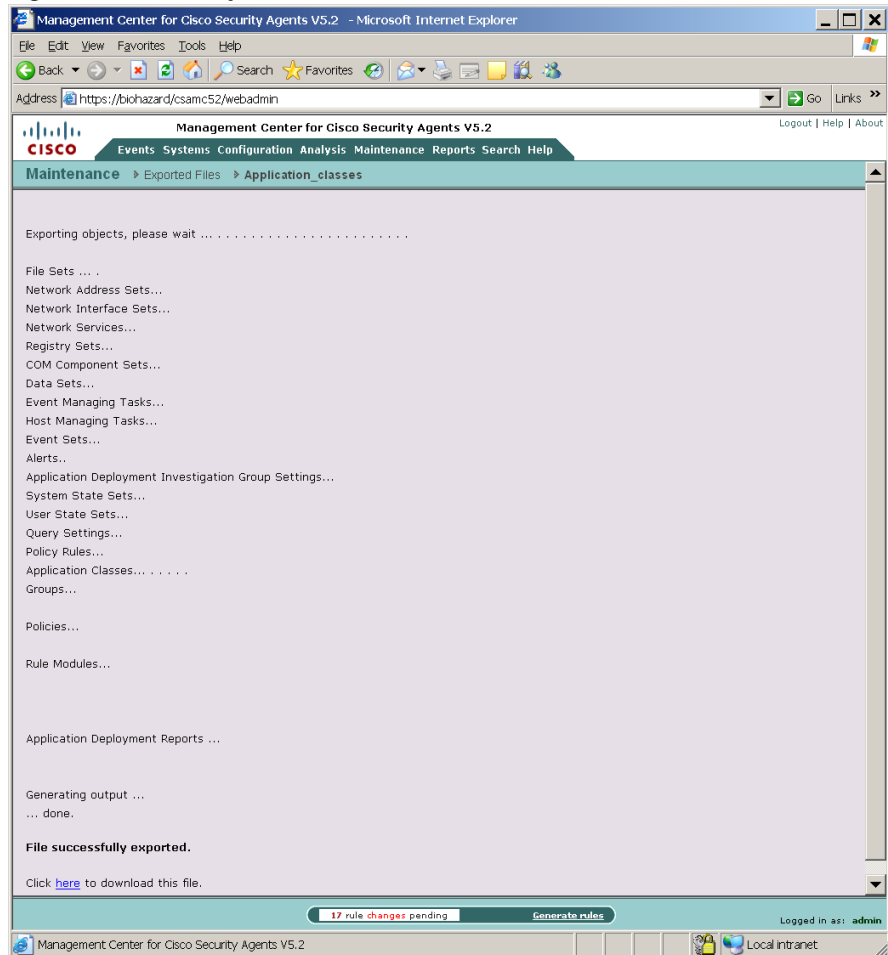


- Step 4** At the top of the page, enter a **File Name** for the exported file you are creating. CSA MC will append an ".export" extension to the file name you enter.
- Step 5** Click the **Export** button. The files are exported under the file name you create. Now you must save the file to the system.
- Step 6** Once the export has completed, a link is displayed that allows you to save the exported file. The link reads "Click [here](#) to download this file." **Click** on the "here" link to save the file to a directory you specify (see [Figure 12-5](#)).
- Once you save the file, you can import it to any server.

**Note**

When you export analysis reports, you are only exporting the report itself and the names of objects referenced in the report, such as a group or policy. The group and policy objects themselves are not automatically exported with the report. There is no cascading inheritance when you export either reports or event sets as occurs when other items are exported. You must select groups and policies separately if you want to export them for the purpose of the report.

Figure 12-5 Export Download View

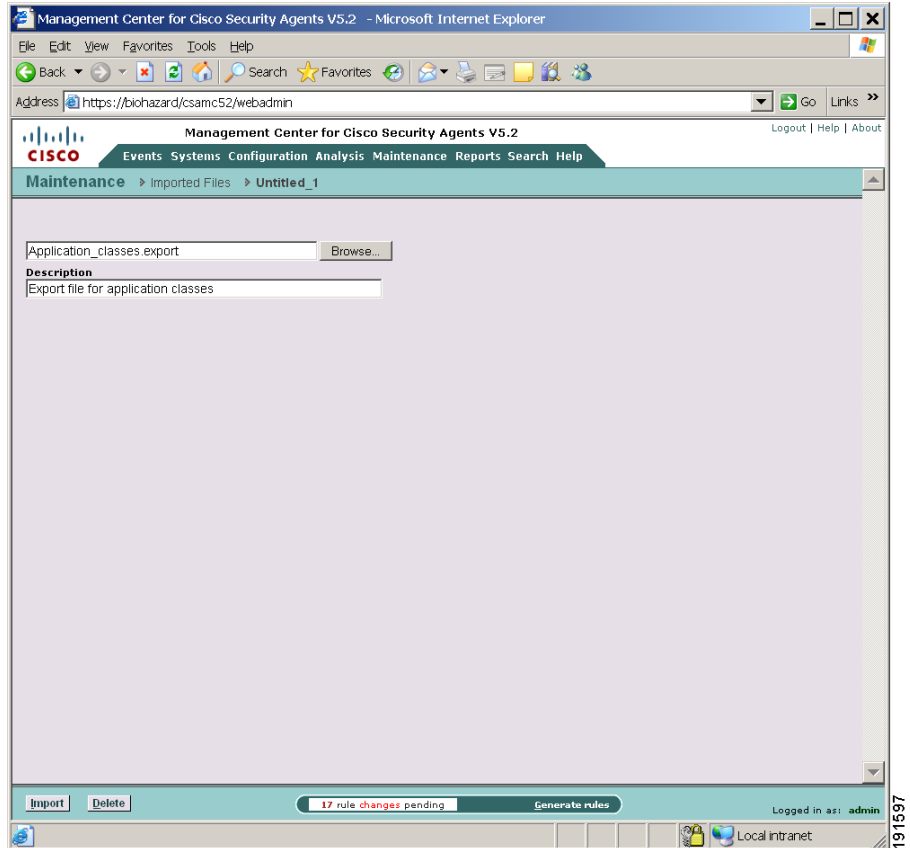


To Import configurations, do the following.

- Step 1** From the menu bar **Maintenance** drop-down list, move the mouse over **Export/Import**. A cascading menu with further selections appears. Select **Import** from the drop-down list that appears. Any previously imported files are shown.

- Step 2** Click the **New** button to create a new imported file. This takes you to the configuration Browse view (see [Figure 12-6](#)).
- Step 3** Click the **Browse** button to locate the exported file you want to import.
- Step 4** Enter a Description and then click the **Import** button to import the configuration.

Figure 12-6 *Import Configurations*



Imported files are automatically entered into the CSA MC database of the server you're importing them to. You don't have to do anything beyond the import function to unpack the exported file.

**Note**

Configuration items shipped with CSA MC and provided by Cisco contain a version column with a version number. Administrator-created items have no version number.

When you import configuration items provided by Cisco, if it is found that there is already an existing exact match for an item, the new configuration data is not copied over. Instead, the existing item will be reused and the name will reflect the new versioning.

If the import process finds that there is an existing item with the same name and different configuration components (variables, etc.), the newly imported item is changed by adding a new version number. The new item is always the item that is re-versioned. Existing items are not renamed or reversioned if there is a collision.

Also note that CSA MC automatically appends the name of the export file to any non-Cisco item collision it finds during administrator imports. The imported item is given a different name and both new and old items can co-exist in the database.

View Import History

Access this page from the CSA MC **Maintenance>Export/Import>Import History** menu path.

- The Import History List Page

The Import History page lets you view lists of files that were imported to CSA MC from exported XML files. From this page, you can select the checkbox beside any file name and click the **Delete** button. This deletes the entire import, rolling your configuration back to its pre-import state.

- The Import History View Page

When you click on the name of a specific Import file, you can view another page listing all imported configuration items for that import file. You have the ability to purge specific imported items from CSA MC by selecting an item or items (via checkbox) and clicking the **Purge Objects** button. You can also use the **Delete** button to simply delete the history of the imported items, not the items themselves.

**Note**

Items shipped with CSA MC are imported during the installation process. Therefore, the import done during the installation appears with any other imports shown on the Import History page.

Cisco Security Agent Posture Plug-in for CTA

The Cisco Trust Agent(CTA) is a component of the Cisco NAC solution. The CTA client software may be installed separately or as part of the Cisco Security Agent installation. See [Creating Agent Kits, page 3-10](#) for CTA installation information.

CTA communicates with all installed plug-ins on the system to extract various types of system information. The Cisco Security Agent sends posture state information (through its own posture plug-in) to CTA.

The Cisco Security Agent posture plug-in returns the following five attributes to CTA which then passes them on to NAC.

- CSAVersion—This is the software version of the installed Cisco Security Agent.
- CSAOperationState—This indicates whether the agent is up and running. A 1 value here indicates the Cisco Security Agent is enabled and running, providing security. A 0 value here indicates the agent is either not installed, not running, or security is turned off
- CSAMCName—This is the fully qualified domain name of the management center the Cisco Security Agent is registered with.
- CSAStatus—This may contain the following strings: global_testmode_on, rootkit_detected, or ipforwarding_on. (See other chapters in this manual for details on group test mode and rootkit detection.)
- DaysSinceLastSuccessfulPoll—This indicates the number of days that have passed since the Cisco Security Agent last polled in to the management center. If the agent has successfully polled within a period of time that is less than 1 day, the value represented here is 0.