



AntiVirus Protection

Overview

The AntiVirus feature provides protection from computer viruses that have been identified by a signature and malware that has been identified by its suspicious or dangerous behavior. Signature-based AntiVirus functions and behavior-based AntiVirus functions provide complimentary protection.

This chapter contains these sections:

- [AntiVirus Basics, page 15-2](#)
 - [Signature-based AntiVirus, page 15-2](#)
 - [Behavior-based AntiVirus, page 15-2](#)
 - [Enabling AntiVirus Protection, page 15-3](#)
 - [How AntiVirus Signatures are Updated, page 15-3](#)
 - [Signature-based Scanning for Viruses, page 15-4](#)
 - [The @virusscan Token, page 15-6](#)
 - [Quarantined Files, page 15-7](#)
 - [Differences Between Signature-based AntiVirus and Automatic Signature Generation, page 15-7](#)
- [Administrative Signature-based AntiVirus Tasks, page 15-8](#)
 - [Scheduling a Background Scan, page 15-8](#)
 - [Performing an On-Demand AV Scan, page 15-9](#)
 - [Identifying a Host AntiVirus Scan Schedule, page 15-9](#)
 - [Forcing a Signature Update for a Group, page 15-9](#)
 - [Forcing a Signature Update for a Host, page 15-10](#)
 - [Creating Exemptions for AntiVirus Tags, page 15-10](#)
- [End-user AntiVirus Tasks, page 15-19](#)
- [AntiVirus Reporting, page 15-12](#)
- [Creating Signature-based AntiVirus Rules and Components, page 15-12](#)
- [Configuring Behavior-based AntiVirus Policy, page 15-19](#)
- [End-user AntiVirus Tasks, page 15-19](#)

AntiVirus Basics

This section provides an overview of the AntiVirus features.

Signature-based AntiVirus

The signature-based AntiVirus function protects the endpoint by identifying infected files and quarantining them. CSA scans files when they are opened or closed and compares their contents to a local database of known virus signatures. If a file is infected, CSA tags it with an AntiVirus tag. Once the file receives a tag, CSA quarantines it and security policies limit the actions of, or the access to, the file.

CSA signature-based AV is designed to have minimal impact on users. Scanning has been optimized to scan mostly when files are modified and written to disk instead of when opened. The only files scanned when opened are files which CSA has defined as “untrusted content.” Untrusted content is defined by a number of rules; files that have been downloaded from the network, files that are launched from temporary directories, files on external drives such as removable disks and USB keys, and files that reside on network shares are all examples of untrusted content. These files are always scanned when they are opened. Typically, files that reside on the fixed disks, and are not included in one of the untrusted content categories, are not scanned when opened.

While this approach is efficient and has minimal user-impact, it does have a disadvantage: If a virus exists on a fixed disk on the host, prior to the agent installation, the virus will evade detection until the background scan reaches it. To minimize the interval where an existing virus, prior to the agent installation, evades detection, CSA signature-based AntiVirus begins a background scan as soon as the agent is installed.

CSA uses three types of virus scanning: on access scanning, on demand scanning, and background scanning. See [Signature-based Scanning for Viruses, page 15-4](#) for more information.

Virus signatures and the signature-matching infrastructure are supplied by Clam AntiVirus (<http://www.clamav.org>). Clam AntiVirus, or ClamAV™, is an open-source antivirus toolkit. A community of users submit files infected with viruses to ClamAV, ClamAV creates a signature for the virus and then distributes signature updates back to its user community.

Incorporating a traditional antivirus scanner in CSA provides fast and efficient defense against known viruses along with a low rate of false positives. This feature compliments CSA’s ability to defeat unknown, day-zero attacks based on identifying malicious behavior.

The signature-matching infrastructure supplied by ClamAV and the CSA policies to restrict infected files are only available for Windows platforms.

**Note**

The *Anti-Virus - Signature based* security policy is one component in an interdependent set of security policies designed to protect the endpoint. CSA’s signature-based AntiVirus feature should be deployed and tested together with the default desktop or server policies.

Behavior-based AntiVirus

The behavior-based AntiVirus function protects the endpoint by examining an untrusted application’s behavior. If an application acts in such a way that is suspicious, malicious, or dangerous, the application receives a behavior-based AntiVirus tag and the application is placed in an application class that reflects its behavior.

As the application continues to act, the end-user is made aware of the application's behavior through pop-up notifications and events in the agent GUI. The user can allow the application to act or prevent the application from acting. As the user prevents an application's actions, the application is placed in application classes that are subject to increasingly restrictive rules or terminated based on the user's response to queries.

After an application has violated a certain number of different policies, the default rules can severely limit its actions or terminate the application automatically.

There are also some actions that an application may take which are automatically denied and the application is automatically terminated without prompting the user for input.

Behavior-based AntiVirus policies are available for Linux, Unix, and Windows platforms.

Enabling AntiVirus Protection

Signature-based AntiVirus protection is enabled when the *AntiVirus - Signature based* policy is deployed to a group. A group's details page and an individual host's details page indicate that the function is enabled. When signature-based AntiVirus protection is deployed, end-users will be able to perform on-demand scans, manage quarantined files, and manage restored files.



Note

CSA installs a signature database on the host; it is used in identifying infected files. If other antivirus applications are installed on the host, it is likely that they will interpret these signature database files as infected and quarantine them. So that there are no conflicts, we strongly recommend that users uninstall other antivirus applications when using CSA's AntiVirus feature.

Behavior-based AntiVirus protection is enabled when the *AntiVirus - Behavior based* policy is deployed to a group. A group's details page and an individual host's details page indicate that the function is enabled. When behavior-based AntiVirus protection is deployed, end-users will see the AntiVirus pane on their Cisco Security Agent. Users will be able to Restore and Quarantine files with behavioral AntiVirus tags using the AntiVirus screen but they will not be able to perform on-demand scans.

How AntiVirus Signatures are Updated

For signature-based AntiVirus protection, the CSA MC maintains a cached version of the Clam AntiVirus signature files and acts as a proxy server when a signature update is requested by an agent.

Agent requests for signature file updates trigger the CSA MC to obtain and provide virus definitions. When agents request updated virus signature files from the CSA MC, the CSA MC compares the timestamp of the signature files on the Clam AntiVirus server with its cached version of the file. If the timestamp of the files on the Clam AntiVirus server matches the copy of the signature files cached on the CSA MC, the CSA MC provides the agent with the signature updates from its own cache. If the CSA MC's cached version is out of date, the CSA MC passes the agent's request directly to the Clam AntiVirus server and then caches the new version of the signature files when they are returned.



Note

In order for the CSA MC to obtain signature updates from ClamAV server (db.local.clamav.net) should be reachable over HTTP either directly or through proxy server.

These files comprise the virus signature database found on the CSA MC and are stored in this directory: `\Program Files\Cisco\CSA MC\CSAMC60\bin\WebServer\htdocs\clamav`

- Main signature file (main.cvd). This is the main signature file stored on the CSA MC and downloaded to every agent. This file is updated with every new release of ClamAV.
- Daily updates file (daily.cvd). This is the database of updated signatures. It is stored on the CSA MC and downloaded to every agent. This file is updated several times a day and stores the latest virus definitions.

These files comprise the virus signature database found on a Windows host running the agent and are stored in this directory: `\Program Files\Cisco\CSAgent\dclass\csa-av`.

- Main signature file (main.cld). This is the main signature file stored on the agent. It is a complete signature file which contains the initial main.cvd file plus updates provided to the main.cvd by ClamAV.
- Daily updates file (daily.cld). This is the database of updated signatures stored on the agent. It contains the original daily.cvd file and all the subsequent virus definition updates.

An agent contacts the CSA MC for signature updates as a result of one of these events:

- **A scheduled request for antivirus updates.** An agent contacts the CSA MC every 24 - 25 hours for updated virus definitions.
- **Forced antivirus updates from a host.** Users can force an antivirus update from the AntiVirus screen of Cisco Security Agent interface.
- **Forced antivirus update for a group.** CSA MC administrators can force an antivirus update for a group from the group's properties page.

If the Cisco Security Agent is standalone, or if the agent can not reach the CSA MC for two days, the agent will try to communicate directly with the internet server, `http://db.local.clamav.net` to get signature updates directly from ClamAV.

Signature-based Scanning for Viruses

For signature-based AntiVirus protection, the goal of virus scanning is to determine if a file is infected or clean. Infected files are tagged with the name of the virus that infects them. Clean files receive an empty tag. Once the files are tagged, rules in the AntiVirus policy protect the host from the infected files.

CSA scans for viruses using these methods

- [Background Scans](#)
- [Scanning Files when Accessed](#)
- [On-demand Scan](#)



Note

These scans do not change a file's modification date.

Background Scans

Background scans are performed on any host that uses the default *AntiVirus - Signature-based* server or desktop policy provided with this release. The *AntiVirus - Signature-based* server and desktop policies contain rules that specify which files will be scanned during a background scan. By default, files on fixed local drives are scanned during an AntiVirus background scan.

Background scans compare the contents of files to the local database of known virus signatures. The scans are conducted when an agent is first installed on a host and when it is scheduled by a CSA administrator. Background scans are non-intrusive, they run in low priority occurring mostly when the system is not in use. See [Scheduling a Background Scan, page 15-8](#) for more information.

**Note**

We recommend regular background scans for all hosts.

Scanning Files when Accessed

Scanning for virus signatures also occurs when files are opened, closed, or executed. Rules in the *Anti-Virus - Signature-based* server or desktop policies determine which files are scanned and under what circumstances.

On-demand Scan

If a host is protected by the *AntiVirus - Signature-based* policy, for desktops or servers, then the AntiVirus pane will be visible to the user in the agent user interface. Users start on-demand scans from that screen.

An on-demand scan examines all files on fixed local drives including archive files such as .zip files and mail files, such as .pst. On-demand scans do not scan files based on rules in a policy.

See [AntiVirus Protection, page A-12](#) for the procedure to perform an on-demand scan. Users can view the procedure in the Agent user interface help by clicking the **AntiVirus** task and clicking the help icon associated with that screen.

Optimized Scanning

To optimize scanning performance, CSA does not scan files over 2GB in size. During an on-access scan or background scan, smaller files are partially scanned based on CSA's scanning algorithm. During an on-demand scan, all files smaller than 2GB are scanned completely.

AntiVirus Tagging

Content files receive AntiVirus tags when virus signatures are found in them. Applications receive AntiVirus tags when they take some action that is considered, suspicious, dangerous, or malicious.

Signature-based AntiVirus Tagging

Once a file is scanned it acquires a tag. Once a file is tagged, rules protect the host from the file based on the file's tag. If a file is infected, it is tagged with the name of the virus that infects it. For example, if a file has been scanned and it is infected with the CodeRed worm, it is tagged: <Virus:Worm.CodeRed>. If a file has been scanned and it is not infected, the file receives an empty tag, "".

If a file has not yet been scanned, it has no tag. While a file is being scanned, it gets the temporary tag, <CSA_SCAN_IN_PROGRESS>. If a file cannot be scanned, it is tagged <CSA_UNSCANNABLE>. An encrypted file is an example of an unscannable file.

There is also a <CSA_SCAN_NOT_ATTEMPTED> tag. Files could receive this tag if the file scanner is not ready to scan a file or if the file scanner does not have permission to open a file, for example. If a file is tagged with <CSA_SCAN_NOT_ATTEMPTED> the file scanner will make additional attempts to scan the file. A file only has the <CSA_SCAN_NOT_ATTEMPTED> tag during the scanning transaction. After the attempted scan, the <CSA_SCAN_NOT_ATTEMPTED> tag is removed from the file.

When CSA scans files, the file scanner checks to see if a file has an existing tag. If the file has an existing tag, and has not been modified since the previous scan, the existing tag is still considered valid and the file is not re-scanned.

“Clean” files, those with empty tags, lose their tags when the file scanner is shut down. This would happen, for example, if the host is rebooted. When a file loses its clean tag, it will be subject to scanning again in the future.

If a file is found to have a virus, it will be listed in the **Quarantined files** tab of the AntiVirus screen, in the agent user interface. Users then have the option of “restoring” their access to Quarantined files.

Behavior-based AntiVirus Tagging

Many types of rules can assign a behavioral AntiVirus tag to an application when the application interacts with another application an attempts a certain activity. Behavior AntiVirus tags are “static.” The tags can be assigned to an application and they can be configured by the administrator but their names cannot be changed.

Based on the kind of interaction, the application can receive one of these tags:

- <Virus:Behavior.Excessive Policy Violations>
- <Virus:Behavior.Malicious Activity>
- <Virus:Behavior.Dangerous Activity>
- <Virus:Behavior.Suspicious Activity>
- <Virus:Behavior.Potential Unwanted Application>

An application can also be specifically assigned “no static tag.” If there are two rules with the same tagging requirements and one rule applies a “no static tag” and one rule applies one of the behavior static tags, the rule with the “no static tag” classification takes precedence and the application does not receive a static tag.

Applications that have an AntiVirus tag can be grouped in with application classes. This allows other rules to allow and restrict the activities of all the applications in a class the same way.

If an application receives a behavior-based AntiVirus tag, it will be listed in the **Quarantined files** tab of the AntiVirus screen, in the agent user interface. Users then have the option of “restoring” their access to Quarantined files.

The @virusscan Token

The @**virusscan** token is used in the content matching field of a file set. All tags, attributed to files because of AntiVirus scanning, are attributes of the @virusscan token. The @virusscan token allows a rule to refer to a group of files rather than naming them all specifically.

When associating a behavior-based AntiVirus tag with the @virusscan token, the syntax is @virusscan=<behavior_based_tag_name> For example:

```
@virusscan=<Virus:Behavior.Excessive Policy Violations>
```

See [Content Matching in File Sets, page 2-40](#) for more examples of @virusscan token syntax.

Quarantined Files

Files and applications are quarantined if they receive a signature-based AntiVirus tag or a behavior-based AntiVirus tag. Quarantined files remain in place and are rendered inert by the rules that govern quarantined files; they are not moved to a special directory.

Users see quarantined files in the Quarantined files tab, on the AntiVirus screen, of the agent's user interface. Through that interface, users can remove files from the quarantine list by "restoring" them and they can re-quarantine a file that they once restored. Users can also delete quarantined files.

Quarantined files are automatically deleted from the users system after 60 days if the following conditions are met:

- Automatic deletion only applies to files found to have a signature-based virus.
 - Files found to have behavior-based viruses will not be automatically deleted; they remain in the quarantine state.
 - Applications identified as PUA are not automatically deleted; they remain in the quarantine state. The PUA label is short for Potentially Unwanted Application. These applications are not malicious by themselves but can be used in a malicious or unwanted context. See <http://www.clamav.org/support/faq/> for more information about applications labeled PUA.
- The file is not touched by another user or application for 60 days.
- The file's status remains in quarantine for 60 days. For example, if a file is quarantined, restored, and then moved back to quarantined, the 60 day timer is reset when the file returns to the quarantined state.

After a quarantined file is deleted, an event is sent to the CSA MC.



Warning

Because quarantined files are restrained by AntiVirus rules, if security on the agent is turned off, the infected files become uncontrolled. They can be read, modified, or executed.



Caution

If the agent is reset, all files in the Quarantined files and Restored files lists are removed.

Differences Between Signature-based AntiVirus and Automatic Signature Generation

Signature-based AntiVirus protection in this release of CSA is a traditional antivirus security feature. It scans the contents of files and compares the content to a library of known virus signatures. If a file contains a virus, the file is rendered inert by CSA policies which prevent the file from being read, written to, or executed.

All local files are scanned periodically. Some files are scanned when they are opened or closed, based on rules in the *AntiVirus - Signature based* policies for desktops and servers. Regular updates of virus signature files are required to ensure that AntiVirus properly identifies the latest known viruses residing in files.

The Automatic Signature Generation feature is designed to protect MSRPC and LPC interfaces from buffer overflow and denial of service attacks. As one of these interfaces is being attacked, the Automatic Signature Generation feature dynamically creates a signature that identifies the attack. That signature is then used by rules to prevent other similar attacks.

Automatically generated signatures are created in real time, this feature does not depend on static signatures which you need to download periodically.

Administrative Signature-based AntiVirus Tasks

This section describes signature-based AntiVirus tasks CSA MC administrators perform.

Scheduling a Background Scan

Administrators can schedule AntiVirus background scans of all hosts that use the default *AntiVirus - Signature-based* provided with this release. These policies contain a rule that specifies which files will be scanned during a background scan. By default, files on fixed local drives are scanned during an AV background scan.

-
- Step 1** Log on the CSA MC as an administrator with configure privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, in the CSA MC interface, navigate **Host Tasks > Host Scanning Tasks**.
 - Step 3** Click **New**.
 - Step 4** Give the task a **Name** and a **Description**.
 - Step 5** Select **Enabled** if you want to enable this task immediately after rules are regenerated and software updates are distributed to hosts.
 - Step 6** In the Configuration area, define the task:
 - In the **Run this task** fields, choose to run this task every week and on a particular day of the week, or choose to run this task every month and on a particular day of every month.



Note We recommend regular background scans of all hosts.



Note If a scan is scheduled on the 31st of the month, the scan will not be performed on months with fewer days.

- In the **At** field, specify the time of day the scan is to run. Time is expressed in twenty-four hour format.
- Check **Perform background AV search on all hosts in group** and select a group from the drop-down list. You can only specify one group for a background scan.



Note Combining an AntiVirus scan with a Data Loss Prevention scan causes two separate system scans.

- Step 7** Click **Save**.

You will then need to generate rules for the task to be distributed to all hosts in that group.

Performing an On-Demand AV Scan

An on-demand AV scan searches fixed drives on the host for files with AntiVirus tags. In order for an on-demand AV scan to work you need to have *Signature-based AntiVirus protection* enabled. See [Enabling AntiVirus Protection, page 15-3](#) for more information.

-
- Step 1** Log on to CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, click **Hosts**.
 - Step 3** Click the link for the host on which you want to start an immediate scan.
 - Step 4** At the end of the **AV full-scan schedule** row, click **View AV Scan Results**.
 - Step 5** In the Scanning dialog box, click **AV Scan Results** if the tab is not open already.
 - Step 6** Click **Scan Now**. A polling hint is sent to the host, after the host receives the polling hint, the on-demand scan begins automatically. If the host does not receive the polling hint, the scan will begin the next time the host polls.

While the scan is in progress, you can click **Get Results** to receive the information gathered so far. After clicking Get Results, the agent on the host forwards the information it has collected the next time the agent polls.

When the on-demand scan is complete, the agent sends the results to the CSA MC automatically.

The AV Scan Results page refreshes the information it has periodically. Upon refresh, the latest information forwarded from the agent is displayed on the page.

Identifying a Host AntiVirus Scan Schedule

-
- Step 1** Log into the CSA MC as any level of user and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Hosts**.
 - Step 3** Click the link for the host you want to investigate.
 - Step 4** Expand the **Host Status** area.
 - Step 5** The **AV Full Scan Schedule** field identifies the scanning schedule for the host.

Forcing a Signature Update for a Group

-
- Step 1** Log into the CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Groups**.
 - Step 3** Click the link for the group which will receive the virus signature updates.
 - Step 4** In the Features area, click the link to **Force AV Update**. A green check mark flashes with the word Done to indicate that the agent has been notified to start an update.

Forcing a Signature Update for a Host

-
- Step 1 Log into the CSA MC as an administrator with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2 From the **Systems** menu, select **Hosts**.
 - Step 3 Click the link for the host for which you want to force a virus signature update.
 - Step 4 Expand the Host status area.
 - Step 5 In the **Time since last AV signature update** row, click the link to **Force AV Update**. A green check mark flashes with the word Done to indicate that the agent has been notified to start an update.

Creating Exemptions for AntiVirus Tags

AntiVirus exemptions can be created for signature-based AntiVirus tags that you have determined to be false positives. Creating an exemption for a tag prevents any files, that have been given the tag, from being restricted by AntiVirus rules that pertain to that tag. Creating an exemption for an individual file, with a particular AntiVirus tag, prevents that file from being restricted by AntiVirus rules that pertain to that tag.

You can create an exception for a virus tag through the **Event Management Wizard** or from scratch using the **AntiVirus Exemptions** page.

Here is an example of how an end-user and a CSA MC administrator would be affected by an AntiVirus exemption: Assume that files have been quarantined on various hosts because they have been tagged with an AntiVirus tag. The CSA MC administrator determines that the tag represents a false positive and then creates an exemption for that tag either using the wizard or by hand. The exemption is then listed on the AntiVirus Exemptions page on the CSA MC. When the administrator is ready, he or she generates rules.

The next time the host's CSA polls in to the CSA MC, it receives the AntiVirus exemption information. Within the next minute, any files with that AntiVirus tag that have already been quarantined are removed from the Quarantined files tab of the agent. The files are not put in the Restored tab. The AntiVirus exemption is global and individual users are not given the opportunity to re-classify the file as Quarantined.

Creating AntiVirus Exemptions Using the Event Management Wizard

-
- Step 1 Log on to the CSA MC as a user with configure privileges. You can perform this task in either Simple Mode or Advanced Mode.
 - Step 2 From the **Events** menu, select **Event Log**.
 - Step 3 Find the event that identifies the virus and quarantines the file because of the presence of the virus. Click the **Wizard** link for the rule.
 - Step 4 Different rules act on a file with an identified virus in different ways. When the wizard launches, accept the suggested action presented by the wizard. When given the option to remove a file from quarantine, you have these options:
 - In the **Remove from AV Quarantine** area, select one of these two radio buttons:
 - **All Windows files** - This allows you to exempt every file, with the specified AntiVirus tag, from being restricted by AntiVirus rules that pertain to that tag. This is the default setting offered by the wizard.

- **Only this Windows file** - This allows you to exempt the file identified by the wizard from being restricted by AntiVirus rules because it has the specified tag.

You can modify the file location with two wildcards (**) to generalize where this file might be found. For example:

```
**\Documents and Settings\Administrator\Desktop \Temp\virus.doc
```

indicates the virus.doc file on Administrator's desktop.

```
**\Desktop\Temp\virus.doc
```

indicates virus.doc on any desktop.

- In the **Justification** field, explain why you are creating the AntiVirus exemption.
- Under the Justification field is a link to **Report the file as false-positive to Cisco/ClamAV**. Clicking the link opens up the default email client available on the host. See [Reporting ClamAV False Positive Viruses to Cisco, page 15-12](#) for more information.

Step 5 Click **Finish** to exempt the file from further AntiVirus enforcement rules.

Step 6 **Generate rules** after clicking finish to deploy the exemption to the host. The exemption is listed in the global **AntiVirus Exemptions** page on the CSA MC. You can reach this page by mousing-over the **Configuration** menu and navigating **Global Settings > AntiVirus Exemptions**.

After rules are generated, the host receives a polling hint, automatically polls in to the CSA MC, and receives the exemption information for this AntiVirus tag. In this case, the exempted files would be removed from the **Quarantine** tab of their local agent and, because the AntiVirus tag was exempted by the CSA MC, the files are not placed in the Restored files tab.

Creating AntiVirus Exemptions Using the Global AntiVirus Exemptions Page

Step 1 Log on to the CSA MC as a user with configure privileges. You can perform this task in either Simple Mode or Advanced Mode.

Step 2 From the **Configure** menu, navigate **Global Settings > AntiVirus Exemptions**.

Step 3 Click **New**. The **Edit AntiVirus Exemption** dialog box opens.

Step 4 Select one of these two radio buttons:

- **All Windows files** - This allows you to exempt every file, with the specified AntiVirus tag, from being restricted by AntiVirus rules that pertain to that tag. This is the default setting offered by the wizard.
- **Only this Windows file** - This allows you to exempt the file identified by the wizard from being restricted by AntiVirus rules because it has the specified tag.

You can specify wildcards at the beginning of the path to indicate “all drives” but you may not specify wildcards in any other part of the directory path. For example:

```
**\Documents and Settings\Administrator\Desktop\virus.txt
```

Step 5 In the **With content matching virus** field, enter the name of the AntiVirus tag you want to exempt from being placed in quarantine. The name has to match exactly to be exempted. Obtain the virus name from the event text.

Step 6 In the **Justification** field, enter a short explanation of why you are creating an exemption for this virus tag.

Step 7 Click **Save**.

Step 8 **Generate rules** to deploy the exemption. The exemption is listed in the global AntiVirus exemptions page on the CSA MC.

Reporting ClamAV False Positive Viruses to Cisco

You can report ClamAV false positives to Cisco as you create an AntiVirus exemption using the Event Management Wizard. See [Creating AntiVirus Exemptions Using the Event Management Wizard, page 15-10](#) for this procedure. Clicking the link to **Report the file as false-positive to Cisco/ClamAV** opens up the default email client and provides a partially composed email with additional instructions.

The email's address field is pre-populated with **csa-clamav-falsepositive@external.cisco.com**. The false positive report lists the filename "infected" with the false positive, the name of the reported infection, and the version of CSA that found the infection.

Before sending the email, please compress the file "infected" with the false positive virus and attach the compressed file to the email.



Note

In order to report the ClamAV false positive to Cisco, you must have the email client configured on the host from which you intend to send the email.

Reporting false positives is best performed from a remote host that can access CSA MC using a web browser. If you attempt to report false positives while logged on to the server on which the CSA MC is installed, you may need to reconfigure the rules in the *CSA Management Center policy* in order to allow the email to be sent.

A false positive occurs when CSA classifies a file or application as being infected by a virus when it is not. When members of the user community report examples of ClamAV false positives to Cisco, these examples are analyzed and if the false positive virus is accepted by the ClamAV signature writers, it is added to ClamAV's database and distributed to the greater ClamAV user community. This makes the AntiVirus scanning faster and more efficient for everyone using ClamAV.

AntiVirus Reporting

You can generate reports that describe the age of signature libraries on hosts, the number and type of viruses infecting hosts, and the location of infected files. See [Clam AntiVirus Reports, page 11-6](#) for the AntiVirus reports you can generate.

Creating Signature-based AntiVirus Rules and Components

The *AntiVirus - Signature based* policies for desktops and servers are provided by default with this release of CSA. They include rules that scan files and applications for viruses, and rules to protect the host from files and applications that are infected with viruses.

If you want to create customized rules and file sets for your enterprise, this section provides procedures to do that.

Creating Virus Scanning Rules

There are two types of rules that, when triggered, scan files for viruses:

- File Access Control Rule (FACL)
- Application Control Rule (APCR)

Creating File Access Control Rules to Scan Files

Use file access control rules to trigger AntiVirus scans on files. Generally, by using a FACL, you can trigger a virus scan on a file when an application has opened or closed it, the application has attempted to read or write the file, and the attempt to read or write the file has been allowed or denied by CSA.



Note See [Configuring Rule Modules, page 5-3](#) to create your own rule module into which you will put this rule.

- Step 1** To add rules to your module, expand the **Rules** area of the rule module configuration screen and click the **Add** button. A pop-up list of the available rule types appears.
- Step 2** Select **File access control** rule. This takes you to the configuration view for this rule type.
- Step 3** Enter the following information for the rule:
- **Description**—Enter a description of this rule.
This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
 - **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.
- Step 4** In the **Take the following action list box**, select **Set** from the pulldown list.
- Step 5** In the Attributes list box, select **Virus scan on CLOSE** or **Virus scan on OPEN**. See [Attribute: Virus scan on CLOSE, page 5-28](#) or [Attribute: Virus scan on OPEN, page 5-28](#) for descriptions of these set attributes.
- Step 6** In the Value field select **NOT being required for this file** to prevent a file from being scanned for viruses or **Being required for this file** to require that the file be scanned for viruses.
- Step 7** Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for these set rules.
- Step 8** **When** —
- **Applications in any (or all) of the following selected classes**
Select one or more preconfigured application classes here to indicate the application(s) whose access to the listed files you want to control. You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 9, “Using Application Classes”](#)
If you choose **Applications in any of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.
If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.
 - **But not in the following class**—
Optionally, select application classes here to exclude from the application class(es) you’ve selected in the included applications field. Note that the entry <None> is selected by default. You may also create a new application class by clicking the blue **New** link next to the application class list box.



Note When your rule is configured, currently selected application classes appear at the top of the list.

Step 9 Attempt the following operations—In this step, you specify the file operation that the application you are controlling is attempting.

If you are creating a **Scan on OPEN** rule, you must select both the **Read File** and **Write File** operations you are allowing or denying on the files named in the **On any of these files box**. If you are creating a **Scan on CLOSE** rule, you can only select the **Write File** operation.

For either Scan on OPEN or Scan on CLOSE, you can also choose the “Write” directory operation. The Write actions you are allowing or denying are **Create**, **Delete**, and **Rename**. Refer to File and Directory protection in [Using the Correct Syntax, page 2-29](#).



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.

Step 10 On any of these files—In this step you configure the files you want to scan for viruses.

Click the **Insert File Set** link to enter a pre-configured file set here. When you click this link, a list of the File Sets you've configured appears here, allowing you to select one or more. Instead of file sets, you can list the literal files you want to protect, using the file paths (including wildcards).

For information on entering file path literals here rather than using pre-configured File Sets, see [Using the Correct Syntax, page 2-29](#).

For local system paths, you must specify the disk drive. You can use a wildcard designation. When protecting directory creates, 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. For example:

Windows:

```
*:\Program Files\winnt\*
or @system\** (this indicates all files below the system directory)
```

For network machines (Windows only), enter:

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

You can enter more than one file path, but each entry must appear on its own line. For File Set configuration details, see [page 8-9](#).



Note

Use **@dynamic** in the File set text field to indicate all files that have been quarantined by CSA MC as a result of correlated email worm 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 globally quarantined files** link on the Global Event Correlation page. See [Manage Dynamically Quarantined Files and IP Addresses, page 7-7](#) for more information.

Step 11 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered by a rule** scans files that applications have been allowed to read or write by other rules. Specifying **Terminated** or **Denied by rule** scans files that other applications have been prevented from acting on.

Step 12 When you are finished configuring your File access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.



Note In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See [page 5-12](#) for instructions.

Creating Application Control Rules to Scan Files

Use application control rules (APCR) to trigger virus scans on applications. Generally, by using an APCR, you can trigger a virus scan on “Application B” when there is an attempt to run it by “Application A” and the operation has been allowed or denied by CSA.



Note See [Configuring Rule Modules, page 5-3](#) to create your own rule module into which you will put this rule.

Step 1 To add rules to your module, expand the Rules area of the rule module configuration page and click the **Add** button. A pop-up list of the available rule types appears.

Step 2 Select the **Application control** rule. This takes you to the configuration view for this rule type.

Step 3 Enter the following information for the rule:

- **Description**—Enter a description of this rule.

This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.

- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)

By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

Step 4 In the **Take the following action list box**, select **Set** from the pulldown list.

Step 5 In the Attributes list box, select **Virus scan**. See [Attribute: Virus scan, page 5-27](#) for descriptions of this set attribute.

Step 6 In the Value field select **NOT being required for this application** to prevent a an application from being scanned for viruses or **Being required for this application** to require that the application be scanned for viruses.

Step 7 Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for this set rule.



Note Creating dynamic application classes from the Application control rule is a bit different than creating them from other rule types. Because this rule has two application class fields, you can choose to add the current application to the dynamic class or choose to add the new application that is invoked by the first application to the dynamic class.

Step 8 When — In this step, specify the application that will attempt to run the application that you want to scan. You are not scanning the application you specify in this step.

- **Applications in any (or all) of the following selected classes**

If you want to scan an application running on a system, no matter how it is invoked, allow “All Applications” to remain selected by default.

If you want to control which application(s) can invoke other applications, select one or more preconfigured application classes here to indicate the application that is doing the invoking (such as Network Applications).

If you choose **Applications in any of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 9, “Using Application Classes”](#)

When your rule is configured, currently selected application classes appear at the top of the list. See [Configuring Static Application Classes, page 9-6](#) for configuration details.

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you’ve selected in the included applications field. Note that the entry <None> is selected by default. You may also create a new application class by clicking the blue New link next to the application class list box.

Step 9 attempt to run — In this step, configure the application that you want to scan for viruses.

- **New applications in any of the following selected classes**—Select the application you want to scan if an attempt is being made to run it by the application defined by the **Applications in any (or all) of the following selected classes** field.

If you choose **New applications in any of the following selected classes** the rule will control an application that is a member of one of the selected application classes.

If you choose **New applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

If you selected “All Applications” in the top application field, selecting “All Applications” in this second field will cause a scan of any file or application when any application launches any file or application. This will significantly diminish the performance of the host.

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you’ve selected in the included applications field. Note that the entry <None> is selected by default.



Note Most dynamic application classes are not available in this second application class inclusion field.

Step 10 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered** by a rule scans applications that have been allowed to run by other rules. Specifying, **Terminated** or **Denied by rule** scans applications that have been prevented from running by other rules.


Step 11 When you are finished configuring your Application control rule, click the **Save** button. This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.

Creating File Sets That Refer to Infected Files

Configure file sets for use in file access control rules and application classes. File sets are groupings of individual files and directories under one common name. This name is then used in rules that control directory and file permissions and restrictions. All the parameters that exist under that name are then applied to the rule where the name is used.

In the case of the AntiVirus feature, the file set defines what files your FACL will scan for viruses. The *File Content - Virus - All signatures* file set, provided by default in this release, represents any file in any directory that has been tagged as containing any virus. If you want to create a file set that represents a specific virus, follow this procedure:

-
- Step 1** From the menu bar **Configuration** drop-down list, mouse over **Variables** and select **File Sets**.
- Step 2** Click the **New** button to create a new file set.
- Step 3** If you have not configured an operating system preference for your administrator account, click **Windows** in the pop-up box. If you have configured an operating system preference for your administrator account, the new file set will automatically be created for that operating systems. This takes you to the file set configuration view (see [Figure 8-3](#)).
- Step 4** In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-29](#). You can also click the Quick Help question mark beside each field for syntax information.):
- **Name**—This is a unique name for this file set. Generally, it's a good idea to adopt a naming convention that lets you quickly enter file set names in a corresponding rule configuration field. When using configuration variables in file access rules, network access rules and application classes, you must enter the variable name preceded by a dollar sign:

For example, if you have a file set variable named `cgi_files`, you must enter `$cgi_files` into any edit field where you are using this variable. The dollar sign tells CSA MC that this is a variable value.
 - **Description**—This is a line of text that is displayed in the list view helping you to identify this particular file set configuration.
 - **OS**—Optionally, you can select to target an operating system more narrowly by selecting a specific Windows operating system from the **OS** list box.
- Step 5** **Directories matching**—Enter the directories and files here (one per line) to which you want to impose restrictions.
- By default, this field has an `<all>` entry indicating all directories. When you click inside this field, the `<all>` disappears so that you can enter your own directory restrictions. When entering directory restrictions, use the following syntax:
- Windows example:
- ```
c:\Program Files***SQL*\bin**
\Program Files***SQL*\bin
```
-  **Note** See [Using the Correct Syntax, page 2-29](#) for details for information on protecting directory paths and files.
- 
- Step 6** **but not**—Make exceptions to the files and directories you've entered in the directories matching field. For example:
- Windows example:
- ```
c:\Program Files\**\*SQL*\bin\temp
```

**Caution**

The exclusion entry above means that any temp files in the bin folder are ignored by the restrictions you apply using this file set. This also means that the path you're protecting in the Directories matching field is NOT protected when the excluded directory "temp" is being accessed.

By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

Step 7 Files Matching—Enter the names of the files to which you are controlling access.

You can use wildcards here to indicate all of a specific file type. For example, *.exe to specify all executables.

By default, this field has an <all> entry indicating all files. When you click inside this field, the <all> disappears so that you can enter your own file restrictions.

Step 8 but not—Make exceptions to the file names you enter in the Files Matching field. For example, all executables, but not regedit.exe.

By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

**Note**

Use **@dynamic** in the File set text field to indicate all files that have been quarantined by CSA MC. 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 dynamically quarantined files** link on the Global Event Correlation page. See [Manage Dynamically Quarantined Files and IP Addresses, page 7-7](#) for more information.

Step 9 Content matching — The Content matching field allows you to describe a set of files that all have the same AntiVirus tag. The entry for each AntiVirus tag is placed on its own line in the Content matching box and must conform to the syntax for **@virusscan** tokens described in [Using the Correct Syntax, page 2-29](#).

- a. Next to the Content matching edit fields, click the **Insert content** link. The **File Content Selector** pop-up opens.
- b. In the Scan type field, select **Virus scanning**.
- c. In the Tag field, type the virus tag name and click **OK**.

If you prefer, you can also edit the Content matching field directly by clicking in the edit box. By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions. Be sure to follow the syntax guidelines for the @virusscan token described in [Using the Correct Syntax, page 2-29](#).

- d. When you have added all the virus scanning tags, close the File Content Selector pop-up box.

Step 10 When all required information is entered, click the **Save** button to save your file set in the CSA MC database.

You can now enter this file set name by clicking the **Insert File Set** link in the application class files field and in the file access control rule files field.

**Note**

In the Tasks menu of each variable page, there is a **View change history** link. Click this link to go to a page which lists all the changes that have been made to the item in question. This View change history link is also available for application classes, policies, and rules.

Configuring Behavior-based AntiVirus Policy

The rules in the rule modules that comprise the *AntiVirus - Behavior based* policies for desktops and servers are complex and have many interdependencies. Instead of creating your own behavior-based AntiVirus rules and components, we strongly recommend that you deploy the *AntiVirus - Behavior based* policies that are provided with this release.

This policy requires a minimal amount of configuration before it is deployed. To configure the policy, follow this procedure:

-
- Step 1** Logon to the CSA MC as a user with configure privileges.
 - Step 2** From the **Configuration** menu, select **Host Security**.
 - Step 3** Expand the Group to which you want to deploy the policy.
 - Step 4** Check the box for the *AntiVirus - Behavior based* policy.
 - Step 5** Click the red **warning** link after the policy name.
 - Step 6** Click the links for the rules you need to configure and save each one after you configure it. If you need help configuring the rules, click the help icons next to the fields that require configuration.
 - Step 7** **Generate** rules. Users will receive the updated policy when they next poll in or when they download the agent kit for the group.

End-user AntiVirus Tasks

End-users have some local control over the AntiVirus feature. Users can perform these tasks if their host is protected with AntiVirus policies:

- Start an On-demand virus scan.
- Change a file's quarantine status.
- Delete quarantined files.
- Force an AntiVirus signature update.

See the [“AntiVirus Protection” section on page A-12](#) for more information about how users can perform these tasks. Users can also view these procedures by clicking the AntiVirus icon in the Tasks panel of the agent user interface and then clicking the help icon.

