Anti-Virus

This chapter contains the following sections:

- Anti-Virus Scanning Overview, on page 1
- Sophos Anti-Virus Filtering, on page 2
- McAfee Anti-Virus Filtering, on page 5
- How to Configure the Appliance to Scan for Viruses , on page 6
- Sending an Email to the Appliance to Test Anti-Virus Scanning , on page 15
- Updating Virus Definitions, on page 17

Anti-Virus Scanning Overview

The appliance includes integrated virus scanning engines from third party companies Sophos and McAfee. You can obtain license keys for the appliance to scan messages for viruses using one or both of these virus scanning engines, and then configure your appliance to scan for viruses using either anti-virus scanning engine.

The McAfee and Sophos engines contain the program logic necessary to scan files at particular points, process and pattern-match virus definitions with data they find in your files, decrypt and run virus code in an emulated environment, apply heuristic techniques to recognize new viruses, and remove infectious code from legitimate files.

You can configure the appliance to scan messages for viruses (based on the matching incoming or outgoing mail policy), and, if a virus is found, to perform different actions on the message (including “repairing” the message of viruses, modifying the subject header, adding an additional X-header, sending the message to an alternate address or mailhost, archiving the message, or deleting the message).

If enabled, virus scanning is performed in the “work queue” on the appliance , immediately after Anti-Spam scanning. (See Email Pipeline and Security Services.)

By default, virus scanning is enabled for the default incoming and outgoing mail policies.

Related Topics

- Evaluation Key, on page 2
- Scanning Messages with Multiple Anti-Virus Scanning Engines, on page 2

Evaluation Key

Your appliance ships with a 30-day evaluation key for each available anti-virus scanning engine. You enable the evaluation key by accessing the license agreement in the System Setup Wizard or Security Services > Sophos/McAfee Anti-Virus pages (in the GUI) or running the `antivirusconfig` or `systemsetup` commands (in the CLI). Once you have accepted the agreement, the Anti-Virus scanning engine will be enabled, by default, for the default incoming and outgoing mail policies. For information on enabling the feature beyond the 30-day evaluation period, contact your Cisco sales representative. You can see how much time remains on the evaluation via the **System Administration > Feature Keys** page or by issuing the `featurekey` command. (For more information, see Feature Keys.)

Scanning Messages with Multiple Anti-Virus Scanning Engines

AsyncOS supports scanning messages with multiple anti-virus scanning engines — multi-layer anti-virus scanning. You can configure your appliance to use one or both of the licensed anti-virus scanning engines on a per mail policy basis. You could create a mail policy for executives, for example, and configure that policy to scan mail with both Sophos and McAfee engines.

Scanning messages with multiple scanning engines provides “defense in depth” by combining the benefits of both Sophos and McAfee anti-virus scanning engines. Each engine has leading anti-virus capture rates, but because each engine relies on a separate base of technology (discussed in McAfee Anti-Virus Filtering, on page 5 and Sophos Anti-Virus Filtering, on page 2) for detecting viruses, the multi-scan approach can be even more effective. Using multiple scanning engines can lead to reduced system throughput, please contact your Cisco support representative for more information.

You cannot configure the order of virus scanning. When you enable multi-layer anti-virus scanning, the McAfee engine scans for viruses first, and the Sophos engine scans for viruses second. If the McAfee engine determines that a message is virus-free, the Sophos engine scans the message, adding a second layer of protection. If the McAfee engine determines that a message contains a virus, the appliance skips Sophos scanning and performs actions on the virus message based on settings you configured.

Sophos Anti-Virus Filtering

The appliance includes integrated virus-scanning technology from Sophos, Plc. Sophos Anti-Virus provides cross-platform anti-virus protection, detection and disinfection.

Sophos Anti-Virus provides a virus detection engine that scans files for viruses, Trojan horses, and worms. These programs come under the generic term of *malware* , meaning “malicious software.” The similarities between all types of malware allow anti-virus scanners to detect and remove not only viruses, but also all types of malicious software.

Related Topics

- Virus Detection Engine, on page 3
- Virus Scanning, on page 3
- Detection Methods, on page 3
- Virus Descriptions, on page 4
- Sophos Alerts , on page 4
- When a Virus is Found, on page 4

Virus Detection Engine

The Sophos virus detection engine lies at the heart of the Sophos Anti-Virus technology. It uses a proprietary architecture similar to Microsoft's COM (Component Object Model), consisting of a number of objects with well-defined interfaces. The modular filing system used by the engine is based on separate, self-contained dynamic libraries each handling a different "storage class," for example, file type. This approach allows virus scanning operations to be applied on generic data sources, irrespective of type.

Specialized technology for loading and searching data enables the engine to achieve very fast scanning speeds. Incorporated within it are:

- A full code emulator for detecting polymorphic viruses
- An on-line decompressor for scanning inside archive files
- An OLE2 engine for detecting and disinfecting macro viruses

The appliance integrates with the virus engine using SAV Interface.

Virus Scanning

In broad terms, the engine's scanning capability is managed by a powerful combination of two important components: a classifier that knows where to look, and the virus database that knows what to look for. The engine classifies the file by type rather than by relying on the extension.

The virus engine looks for viruses in the bodies and attachments of messages received by the system; an attachment's file type helps determine its scanning. For example, if a message's attached file is an executable, the engine examines the header which tells it where the executable code starts and it looks there. If the file is a Word document, the engine looks in the macro streams. If it is a MIME file, the format used for mail messaging, it looks in the place where the attachment is stored.

Detection Methods

How viruses are detected depends on their type. During the scanning process, the engine analyzes each file, identifies the type, and then applies the relevant technique(s). Underlying all methods is the basic concept of looking for certain types of instructions or certain ordering of instructions.

Related Topics

- Pattern Matching, on page 3
- Heuristics, on page 4
- Emulation, on page 4

Pattern Matching

In the technique of pattern matching, the engine knows the particular sequence of code and is looking for an exact match that will identify the code as a virus. More often, the engine is looking for sequences of code that are similar, but not necessarily identical, to the known sequences of virus code. In creating the descriptions against which files are compared during scanning, Sophos virus researchers endeavor to keep the identifying code as general as possible so that – using heuristics, as explained below – the engine will find not just the original virus but also its later derivatives.

Heuristics

The virus engine can combine basic pattern matching techniques with heuristics – a technique using general rather than specific rules – to detect several viruses in the same family, even though Sophos researchers might have analyzed only one virus in that family. The technique enables a single description to be created that will catch several variants of one virus. Sophos tempers its heuristics with other methods, minimizing the incidence of false positives.

Emulation

Emulation is a technique applied by the virus engine to polymorphic viruses. Polymorphic viruses are encrypted viruses that modify themselves in an effort to hide themselves. There is no visible constant virus code and the virus encrypts itself differently each time it spreads. When it runs, it decrypts itself. The emulator in the virus detection engine is used on DOS and Windows executables, while polymorphic macro viruses are found by detection code written in Sophos's Virus Description Language.

The output of this decryption is the real virus code and it is this output that is detected by the Sophos virus detection engine after running in the emulator.

Executables that are sent to the engine for scanning are run inside the emulator, which tracks the decryption of the virus body as it is written to memory. Normally the virus entry point sits at the front end of a file and is the first thing to run. In most cases, only a small amount of the virus body has to be decrypted in order for the virus to be recognized. Most clean executables stop emulating after only a few instructions, which reduces overhead.

Because the emulator runs in a restricted area, if the code does turn out to be a virus, the virus does not infect the appliance .

Virus Descriptions

Sophos exchanges viruses with other trusted anti-virus companies every month. In addition, every month customers send thousands of suspect files directly to Sophos, about 30% of which turn out to be viruses. Each sample undergoes rigorous analysis in the highly secure virus labs to determine whether or not it is a virus. For each newly discovered virus, or group of viruses, Sophos creates a description.

Sophos Alerts

Cisco encourages customers who enable Sophos Anti-Virus scanning to subscribe to Sophos alerts on the Sophos site at http://www.sophos.com/virusinfo/notifications/. Subscribing to receive alerts directly from Sophos will ensure you are apprised of the latest virus outbreaks and their available solutions.

When a Virus is Found

When a virus has been detected, Sophos Anti-Virus can repair (disinfect) the file. Sophos Anti-Virus can usually repair any file in which a virus has been found, after which the file can be used without risk. The precise action taken depends on the virus.

There can be limitations when it comes to disinfecting, because it is not always possible to return a file to its original state. Some viruses overwrite part of the executable program which cannot be reinstated. In this instance, you define how to handle messages with attachments that could not be repaired. You configure these settings on a per-recipient basis using the Email Security Feature: the **Mail Policies > Incoming or Outgoing**

Mail Policies pages (GUI) or the `policyconfig -> antivirus` command (CLI). For more information on configuring these settings, see Configuring Virus Scanning Actions for Users, on page 7.

McAfee Anti-Virus Filtering

The McAfee® scanning engine:

- Scans files by pattern-matching virus signatures with data from your files.
- Decrypts and runs virus code in an emulated environment.
- Applies heuristic techniques to recognize new viruses.
- Removes infectious code from files.

Related Topics

- Pattern-Matching Virus Signatures, on page 5
- Encrypted Polymorphic Virus Detection, on page 5
- Heuristics Analysis, on page 5
- When a Virus is Found, on page 4

Pattern-Matching Virus Signatures

McAfee uses anti-virus definition (DAT) files with the scanning engine to detect particular viruses, types of viruses, or other potentially unwanted software. Together, they can detect a simple virus by starting from a known place in a file, then searching for a virus signature. Often, they must search only a small part of a file to determine that the file is free from viruses.

Encrypted Polymorphic Virus Detection

Complex viruses avoid detection with signature scanning by using two popular techniques:

- **Encryption**. The data inside the virus is encrypted so that anti-virus scanners cannot see the messages or computer code of the virus. When the virus is activated, it converts itself into a working version, then executes.
- **Polymorphism**. This process is similar to encryption, except that when the virus replicates itself, it changes its appearance.

To counteract such viruses, the engine uses a technique called emulation. If the engine suspects that a file contains such a virus, the engine creates an artificial environment in which the virus can run harmlessly until it has decoded itself and its true form becomes visible. The engine can then identify the virus by scanning for a virus signature, as usual.

Heuristics Analysis

Using only virus signatures, the engine cannot detect a new virus because its signature is not yet known. Therefore the engine can use an additional technique — heuristic analysis.

Programs, documents or email messages that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients, or use other means to replicate themselves. The engine analyzes the program code to detect these kinds of computer instructions. The engine also searches for legitimate

non-virus-like behavior, such as prompting the user before taking action, and thereby avoids raising false alarms.

By using these techniques, the engine can detect many new viruses.

When a Virus is Found

When a virus has been detected, Sophos Anti-Virus can repair (disinfect) the file. Sophos Anti-Virus can usually repair any file in which a virus has been found, after which the file can be used without risk. The precise action taken depends on the virus.

There can be limitations when it comes to disinfecting, because it is not always possible to return a file to its original state. Some viruses overwrite part of the executable program which cannot be reinstated. In this instance, you define how to handle messages with attachments that could not be repaired. You configure these settings on a per-recipient basis using the Email Security Feature: the **Mail Policies > Incoming or Outgoing Mail Policies** pages (GUI) or the `policyconfig -> antivirus` command (CLI). For more information on configuring these settings, see Configuring Virus Scanning Actions for Users, on page 7.

How to Configure the Appliance to Scan for Viruses

How to Scan Messages for Viruses

	Do This	More Info
Step 1	Enable anti-virus scanning on the appliance .	Enabling Virus Scanning and Configuring Global Settings , on page 7
Step 2	Define the groups of users whose messages you want to scan for viruses.	Creating a Mail Policy for a Group of Senders and Recipients
Step 3	(Optional) Configure how you want the virus quarantine to handle messages.	Configuring Policy, Virus, and Outbreak Quarantines
Step 4	Determine how you want the appliance to handle messages with viruses.	Configuring Virus Scanning Actions for Users, on page 7
Step 5	Configure the anti-virus scanning rules for the user groups you defined.	Configuring the Anti-Virus Policies for Different Groups of Senders and Recipients, on page 12
Step 6	(Optional) Send an email message to test the configuration.	Sending an Email to the Appliance to Test Anti-Virus Scanning , on page 15

Related Topics

- Enabling Virus Scanning and Configuring Global Settings , on page 7
- Configuring Virus Scanning Actions for Users, on page 7
- Configuring the Anti-Virus Policies for Different Groups of Senders and Recipients, on page 12
- Notes on Anti-Virus Configurations, on page 13
- Flow Diagram for Anti-Virus Actions, on page 14

Enabling Virus Scanning and Configuring Global Settings

You may have enabled a virus scanning engine when you ran the System Setup Wizard. Regardless, configure settings using this procedure.

Note Depending on your feature keys, you can enable Sophos, McAfee, or both.

Procedure

Step 1 Navigate to the **Security Services > McAfee** page.

Or

Navigate to the **Security Services > Sophos** page.

Step 2 Click **Enable**.

Note Clicking **Enable** enables the feature globally for the appliance . However, you must later enable per-recipient settings in Mail Policies.

Step 3 After reading the license agreement, scroll to the bottom of the page and click **Accept** to accept the agreement.

Step 4 Click **Edit Global Settings**.

Step 5 Choose a maximum virus scanning timeout value.

Configure a timeout value for the system to stop performing anti-virus scanning on a message. The default value is 60 seconds.

Step 6 (Optional) Click **Enable Automatic Updates** to enable automatic update of the engine.

The appliance fetches the required updates for the particular engine from the update server.

Step 7 Submit and commit your changes.

What to do next

Configure anti-virus settings on a per-recipient basis. See Configuring Virus Scanning Actions for Users, on page 7.

Configuring Virus Scanning Actions for Users

The virus scanning engine integrated into the appliance processes messages for viruses for incoming and outgoing mail based on policies (configuration options) you configure using the Email Security Manager feature. You enable Anti-Virus actions on a per-recipient basis using the Mail Policies > Incoming or Outgoing Mail Policies pages (GUI) or the `policyconfig > antivirus` command (CLI).

Related Topics

- Message Scanning Settings, on page 8
- Message Handling Settings, on page 8

- Configuring Settings for Message Handling Actions, on page 9

Message Scanning Settings

- Scan for Viruses Only:

  Messages processed by the system are scanned for viruses. Repairs are *not* attempted for infected attachments. You can choose whether to drop attachments and deliver mail for messages that contain viruses or could not be repaired.

- Scan and Repair Viruses:

  Messages processed by the system are scanned for viruses. If a virus is found in an attachment, the system will attempt to "repair" the attachment.

- Dropping Attachments

  You can choose to drop infected attachments.

  When infected attachments to messages have been scanned and *dropped* by the anti-virus scanning engine, the attachment is replaced with a new attachment called "Removed Attachment." The attachment type is text/plain and contains the following:

```
This attachment contained a virus and was stripped.
 Filename: filename
Content-Type: application/filetype
```

Users will always be notified if their messages were modified in any way because they were infected with a bad attachment. You can configure a secondary notification action, as well (see Sending Notifications, on page 11). The notify action is *not* needed to inform users that a message was modified if you choose to drop infected attachments.

- X-IronPort-AV Header

  All messages that are processed by the Anti-Virus scanning engine on the appliance have the header X-IronPort-AV: added to messages. This header provides additional information to you when debugging issues with your anti-virus configuration, particularly with messages that are considered "unscannable." You can toggle whether the X-IronPort-AV header is included in messages that are scanned. Including this header is recommended.

Message Handling Settings

You configure the virus scanning engine to handle four distinct classes of messages that are received by a listener, with separate actions for each. *Figure - Options for Handling Messages Scanned for Viruses* summarizes the actions the system performs when the virus scanning engine is enabled.

For each of the following message types, you can choose which actions are performed. The actions are described below (see Configuring Settings for Message Handling Actions, on page 9). For example, you can configure your anti- virus settings for virus-infected messages so that the infected attachment is dropped, the subject of the email is modified, and a custom alert is sent to the message recipient.

Repaired Message Handling

Messages are considered *repaired* if the message was completely scanned and all viruses have been repaired or removed. These messages will be delivered as is.

Encrypted Message Handling

Messages are considered encrypted if the engine is unable to finish the scan due to an encrypted or protected field in the message. Messages that are marked encrypted may also be repaired.

Note the differences between the encryption detection message filter rule (see Encryption Detection Rule) and the virus scanning actions for "encrypted" messages. The encrypted message filter rule evaluates to "true" for any messages that are PGP or S/MIME encrypted. The encrypted rule can only detect PGP and S/MIME encrypted data. It does not detect password protected ZIP files, or Microsoft Word and Excel documents that include encrypted content. The virus scanning engine considers any message or attachment that is password protected to be "encrypted."

Note If you upgrade from a 3.8 or earlier version of AsyncOS and you configured Sophos Anti-Virus scanning, you must configure the Encrypted Message Handling section after you upgrade.

Unscannable Message Handling

Messages are considered unscannable if a scanning timeout value has been reached, or the engine becomes unavailable due to an internal error. Messages that are marked unscannable may also be repaired.

Virus Infected Message Handling

The system may be unable to drop the attachment or completely repair a message. In these cases, you can configure how the system handles messages that could still contain viruses.

The configuration options are the same for encrypted messages, unscannable messages, and virus messages.

Configuring Settings for Message Handling Actions

- Action to Apply, on page 9
- Quarantines and Anti-Virus Scanning, on page 10
- Modify the Message Subject Header, on page 10
- Archive Original Message, on page 10
- Sending Notifications, on page 11
- Add Custom Header to Message, on page 11
- Modify Message Recipient, on page 11
- Send Message to Alternate Destination Host, on page 11
- Send Custom Alert Notification, on page 12

Action to Apply

Choose which overall action to take on each message type for encrypted, unscannable, or virus positive messages: drop the message, deliver the message as an attachment to a new message, deliver the message as is, or send the message to the anti-virus quarantine area (Quarantines and Anti-Virus Scanning, on page 10).

Configuring the appliance to deliver the infected messages as an attachment to a new message allows the recipient to choose how to deal with the original, infected attachment.

If you choose to deliver the message or deliver the message as an attachment to a new message, you can additionally:

- Modify message subject

- Archive original message
- Send generic notificationThe following actions are available in the “Advanced” section of the GUI:
- Add custom header to message
- Modify message recipient
- Send message to alternate destination host
- Send custom alert notification

Note These actions are not mutually exclusive; you can combine some or all of them differently within different incoming or outgoing policies for different processing needs for groups of users. See the following sections and Notes on Anti-Virus Configurations, on page 13 for more information on defining various scanning policies using these options.

Repaired messages have only two advanced options: Add custom header and Send custom alert notification. All other message types have access to all of the advanced options.

Quarantines and Anti-Virus Scanning

When flagged for quarantine, the message continues through the rest of the email pipeline. When the message reaches the end of the pipeline, if the message has been flagged for one or more quarantines then it enters those queues. Note that if the message does not reach the end of the pipeline, it is not placed in a quarantine.

For example, a content filter can cause a message to be dropped or bounced, in which case the message will not be quarantined.

Archive Original Message

You can archive messages the system has identified as containing (or possibly containing) viruses to the “avarchive” directory. The format is an mbox-format log file. You *must* configure an “Anti-Virus Archive” log subscription to archive messages with viruses or messages that could not be completely scanned. For more information, see Logging

Note In the GUI, you may need to click the “Advanced” link to reveal the “Archive original message” setting.

Modify the Message Subject Header

You can alter the text of identified messages by prepending or appending certain text strings to help users more easily identify and sort identified messages.

Note White space is not ignored in the “Modify message subject” field. Add spaces after (if prepending) or before (if appending) the text you enter in this field to separate your added text from the original subject of the message. For example, add the text `[WARNING: VIRUS REMOVED]` with a few trailing spaces if you are prepending.

The default text is:

Default Subject Line Text for Anti-Virus Subject Line Modification

Verdict	Default Text to Add to Subject
Encrypted	`[WARNING: MESSAGE ENCRYPTED]`
Infected	`[WARNING: VIRUS DETECTED]`
Repaired	`[WARNING: VIRUS REMOVED]`
Unscannable	`[WARNING: A/V UNSCANNABLE]`

Any message with multiple states causes a multi-part notification message informing users what actions the appliance performed on the message (for example, the user is notified that the message was repaired of a virus, but another part of the message was encrypted).

Sending Notifications

When the system has identified a message as containing viruses, you can send the default notification to the sender, the recipient, and/or additional users. When specifying additional users to notify, separate multiple addresses with commas (in both the CLI and the GUI). The default notification messages are:

Default Notifications for Anti-Virus Notifications

Verdict	Notification
Repaired	The following virus(es) was detected in a mail message: <virus name(s)> Actions taken: Infected attachment dropped (or Infected attachment repaired).
Encrypted	The following message could not be fully scanned by the anti-virus engine due to encryption.
Unscannable	The following message could not be fully scanned by the anti-virus engine.
Infectious	The following unrepairable virus(es) was detected in a mail message: <virus name(s)>.

Add Custom Header to Message

You can define an additional, custom header to be added to all messages that are scanned by the anti-virus scanning engine. Click **Yes** and define the header name and text.

You can also create filters that use the `skip-viruscheck` action so that certain messages bypass virus scanning. See Bypass Anti-Virus System Action.

Modify Message Recipient

You can modify the message recipient, causing the message to be delivered to a different address. Click **Yes** and enter the new recipient address.

Send Message to Alternate Destination Host

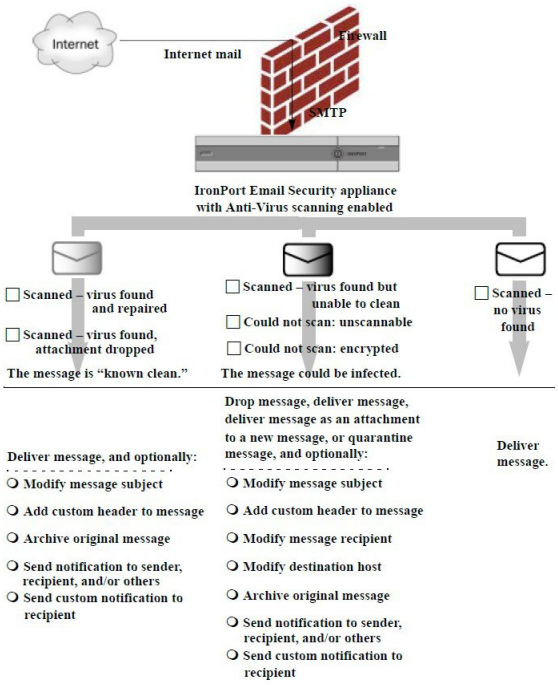
You can choose to send the notification to a different recipient or destination host for encrypted, unscannable, or virus infected messages. Click **Yes** and enter an alternate address or host.

For example, you could route suspected messages to an administrator's mailbox or a special mail server for subsequent examination. In the case of a multi-recipient message, only a single copy is sent to the alternative recipient.

Send Custom Alert Notification

You can send a custom notification to the sender, recipient, and/or other users (email addresses). To do so, you must first create the custom notification prior to configuring the settings. See Understanding Text Resources for more information.

Figure 1: Options for Handling Messages Scanned for Viruses



Note By default, Anti-Virus scanning is enabled in the $TRUSTED mail flow policy for public listeners, which is referenced by the ALLOWED_LIST sender group. See Defining Access Rules for Email Senders Using Mail Flow Policies.

Configuring the Anti-Virus Policies for Different Groups of Senders and Recipients

The process for editing the per-user anti-virus settings for a mail policy is essentially the same for incoming or outgoing mail.

Individual policies (not the default) have an additional field to "Use Default" settings. Select this setting to inherit the default mail policy settings.

You enable anti-virus actions on a per-recipient basis using Incoming or Outgoing Mail Policies. You can configure mail policies in the GUI or in the CLI using the policyconfig > antivirus command. After you enable anti-virus settings globally, you configure these actions separately for each mail policy you create. You can configure different actions for different mail policies.

Procedure

Step 1 Navigate to the Mail Policies > Incoming Mail Policies or Mail Policies > Outgoing Mail Policies page.

Step 2 Click the link for the anti-virus security service for the policy you want to configure.

Note Click the link in the default row to edit the settings for the default policy.

Step 3 Click **Yes** or **Use Default** to enable Anti-Virus Scanning for the policy.

The first setting on the page defines whether the service is enabled for the policy. You can click **Disable** to disable the service altogether.

For mail policies other than the default, choosing "Yes" enables the fields in the Repaired, Encrypted, Unscannable, and Virus Infected Messages areas to become active.

Step 4 Select an Anti-Virus scanning engine. You can select McAfee or Sophos engines.

Step 5 Configure Message Scanning settings.

See Message Scanning Settings, on page 8 for more information.

Step 6 Configure settings for Repaired, Encrypted, Unscannable, and Virus Infected messages.

See Message Handling Settings, on page 8 and Configuring Settings for Message Handling Actions, on page 9.

Step 7 Click **Submit**.

Step 8 Commit your changes.

Notes on Anti-Virus Configurations

The drop attachments flag makes a considerable difference in how anti-virus scanning works. When the system is configured to "Drop infected attachments if a virus is found and it could not be repaired," any viral or unscannable MIME parts are removed from messages. The output from Anti-Virus scanning, then, is almost always a clean message. The action defined for *Unscannable Messages* , as shown in the GUI pane, rarely takes place.

In a "Scan for Viruses only" environment, these actions "clean" messages by dropping the bad message parts. Only if the RFC822 headers themselves are attacked or encounter some other problem would this result in the unscannable actions taking place. However, when Anti-Virus scanning is configured for "Scan for Viruses only" and "Drop infected attachments if a virus is found and it could not be repaired," is *not* chosen, the unscannable actions are very likely to take place.

The following table lists some common Anti-Virus configuration options

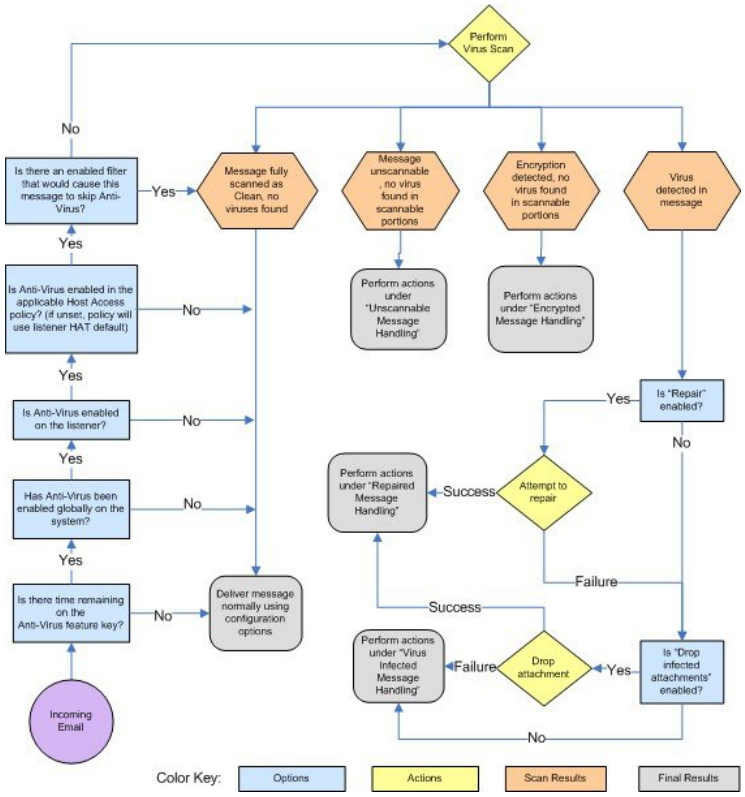
Common Anti-Virus Configuration Options

Situation	Anti-Virus Configuration
Widespread Virus Outbreak Any viral message is simply dropped from the system with little other processing taking place.	**Drop-attachments:** NO **Scanning:** Scan-Only **Cleaned messages**: Deliver **Unscannable messages**: DROP message Encrypted messages: Send to administrator or quarantine for review. Viral messages: Drop message
Liberal Policy As many documents as possible are sent.	**Drop-attachments:** YES **Scanning:** Scan and Repair **Cleaned messages:** [VIRUS REMOVED] and Deliver **Unscannable messages**: Forward as attachment Encrypted messages: Mark and forward Viral messages: Quarantine or mark and forward.
More Conservative Policy	**Drop-attachments**: YES **Scanning:** Scan and Repair **Cleaned messages:** [VIRUS REMOVED] and Deliver (Archive cleaned messages for a more cautious policy.) **Unscannable messages**: Send notification(s), quarantine, OR drop and archive. Encrypted messages: Mark and forward OR treat as unscannable Viral messages: Archive and drop
Conservative with Review Possible virus messages are sent to a quarantine mailbox so that an administrator can review the content.	**Drop-attachments:** NO **Scanning:** Scan-Only **Cleaned messages:** Deliver (this action won't normally be taken) **Unscannable messages**: Forward as attachment, alt-src-host , or alt-rcpt-to actions. Encrypted messages: Treat as unscannable Viral messages: Forward to quarantine or administrator.

Flow Diagram for Anti-Virus Actions

The following figure explains how anti-virus actions and options affect messages processed by the appliance .

Figure 2: Flow Diagram for Anti-Virus Actions



Note If you configure multi-layer anti-virus scanning, the Cisco appliance performs virus scanning with the McAfee engine first and the Sophos engine second. It scans messages using both engines, unless the McAfee engine detects a virus. If the McAfee engine detects a virus, the appliance performs the anti-virus actions (repairing, quarantining, etc.) defined for the mail policy.

Sending an Email to the Appliance to Test Anti-Virus Scanning

Procedure

Step 1 Enable virus scanning for a mail policy.

Use the **Security Services > Sophos/McAfee Anti-virus** page or the `antivirusconfig` command to set global settings, and then use the Email Security Manager pages (GUI) or the `antivirus` subcommand of `policyconfig` to configure the settings for a specific mail policy.

Step 2 Open a standard text editor, then type the following character string as *one line, with no spaces or line breaks:*

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Note The line shown above should appear as one line in your text editor window, so be sure to maximize your text editor window and delete any line breaks. Also, be sure to type the letter O, not the number 0, in the "X5O..." that begins the test message.

If you are reading this manual on your computer, you can copy the line directly from the PDF file or HTML file and paste it into your text editor. If you copy the line, be sure to delete any extra carriage returns or spaces.

Step 3 Save the file with the name **EICAR.COM**.

The file size will be 68 or 70 bytes.

Note This file is not a virus — it cannot spread or infect other files, or otherwise harm your computer. However, you should delete the file when you have finished testing your scanner to avoid alarming other users.

Step 4 Attach the file EICAR.COM to an email message, and send it to the listener that will match the mail policy you configured in step 1.

Ensure the that the recipient you specify in the test message will be accepted on the listener. (For more information, see Adding Domains and Users For Which to Accept Messages.)

Note that it may be difficult to email the file if you have virus scanning software is installed for outgoing mail on a gateway other than the Cisco (for example, a Microsoft Exchange server).

Note The test file always scans as unrepairable.

Step 5 Evaluate the actions you configured for virus scanning on the listener and ensure they are enabled and working as expected.

This is most easily accomplished by performing one of the following actions:

a. Configure the virus scanning settings to Scan and Repair mode or Scan only mode without dropping attachments.

- Send an email with the Eicar test file as an attachment. Confirm that the actions taken match your configuration for Virus Infected Message Handling (the settings in Virus Infected Message Handling, on page 9).

b. Configure the virus scanning settings to Scan and Repair mode or Scan only mode with dropping attachments.

- Send an email with the Eicar test file as an attachment.
- Confirm that the actions taken match your configuration for Repaired Message Handling (the settings in Repaired Message Handling, on page 8).

For more information obtaining virus files for testing anti-virus scanning, see:
http://www.eicar.org/anti_virus_test_file.htm

This page provides 4 files for downloading. Note that it may be difficult to download and extract these files if you have a client-side virus scanning software installed.

Updating Virus Definitions

Related Topics

- About Retrieving Anti-Virus Updates via HTTP , on page 17
- Configuring Update Server Settings , on page 17
- Monitoring and Manually Checking for Anti-Virus Updates, on page 17
- Verifying Anti-Virus Files Have Updated on the Appliance , on page 18

About Retrieving Anti-Virus Updates via HTTP

Sophos and McAfee frequently update their virus definitions with newly-identified viruses. These updates must be passed to your appliance .

By default, the appliance is configured to check for updates every 5 minutes. For the Sophos and McAfee anti-virus engines, the server updates from a dynamic website.

The system does not timeout on updates as long as the update is actively downloading to the appliance . If the update download pauses for too long, then the download times out.

The maximum amount of time that the system waits for an update to complete before timing out is a dynamic value that is defined as 1 minute less than the anti-virus update interval (defined on Security Services > Service Updates). This configuration value aids appliances on slower connections while downloading large updates that may take longer than 10 minutes to complete.

Configuring Update Server Settings

You can configure virus update settings via the Security Services > Service Updates page. For example, you can configure how the system receives anti-virus updates and how often it checks for updates. For more information about these additional settings, see Service Updates.

Monitoring and Manually Checking for Anti-Virus Updates

You can use the **Security Services > Sophos or McAfee** page or the `antivirusstatus` CLI command to verify the appliance has the latest anti-virus engine and identity files installed, and to confirm when the last update was performed.

You can also manually perform updates. See Manually Updating Anti-Virus Engines , on page 17

Manually Updating Anti-Virus Engines

Procedure

Step 1 Navigate to the Security Services > Sophos or McAfee Anti-Virus page.

Step 2 Click **Update Now** in the Current McAfee/Sophos Anti-Virus Files table.

The appliance checks for and downloads the latest updates.

What to do next

You can also configure this in the command-line interface using the antivirusstatus and antivirusupdate command

Verifying Anti-Virus Files Have Updated on the Appliance

You can view the Updater Logs to verify whether or not the antivirus files have been successfully downloaded, extracted, or updated. Use the tail command to show the final entries in the Updater log subscription to ensure that virus updates were obtained.