

OpenMail supports the use of the virus protection software product ScanMail for OpenMail, available from the third-party supplier Trend Micro.

When the virus scanning software is activated, the Service Router scans all messages for viruses and, optionally, attempts to clean those which contain infected parts.

The performance of your OpenMail system may be degraded slightly when you configure virus scanning. The level of performance degradation will depend on the number of viruses detected, and the action taken.

This chapter contains the following sections:

- “Overview”
- “Virus Scanning Rules”
- “Notification and Reporting”
- “Virus Scanning Files”

Overview

OpenMail uses the third-party product ScanMail for OpenMail, available from Trend Micro, to scan messages for viruses.

Configure OpenMail to use this virus protection software by setting up filters to check messages for viruses, and specifying the action to be taken when a virus is found.

To enable virus protection, carry out the following steps:

1. Buy and install the ScanMail for OpenMail product.

This is available from Trend Micro, at:

<http://www.antivirus.com>

2. Decide on the actions to be taken when a virus is discovered; for example, should an attempt be made to remove it, or should the message containing the virus be returned to the sender?
3. Create a ruleset to implement the above actions: see the *OpenMail Technical Reference Guide* for general information on rules and rulesets. See “Virus Scanning Rules” for how to create a virus protection ruleset.

Note: *Unlike other rulesets, you cannot associate the virus scanning ruleset with specific routes. When virus scanning is enabled, it applies to all routes.*

Updating the Virus Scanning Software

Note that when you update the Trend Micro virus scanning software, you must shut down and restart the Service Router (using `omoff` and `omon`) for the update to take effect. (See the ScanMail for OpenMail documentation for instructions on updating the software.)

Virus Scanning Rules

What is a Message Delivery Rule?

A message delivery rule causes the Service Router to test the value of a message attribute, and to carry out specific actions based on the result of the test. For example, you could create a rule to test if the Priority of a message is Low and, if true, defer its delivery until after normal office hours.

Rules are contained in rulesets, each of which can contain one or more rules. In this way, a ruleset can test for a number of different values of a message attribute, with a different action for each value it finds.

A ruleset is a text file, located in `/var/opt/openmail/rules`, that contains one or more rules. In general, each ruleset can be associated with one or more OpenMail routes. However, the virus scanning ruleset, once created, applies to all routes.

See the *OpenMail Technical Reference Guide* for more information on rules and rulesets.

Creating a Virus Scanning Ruleset

A virus scanning ruleset is a text file, `/var/opt/openmail/rules/ALL-ROUTES.VIR`, that contains rules that test for the presence of viruses and specify the actions to be taken as a result of those tests.

Virus Scanning Message Attributes

There are two message attributes that you can use in virus scanning rules:

- `VIRUS-FOUND`

Using this attribute in a rule causes the Service Router to test each message for the presence of viruses.

- `VIRUS-UNCLEANED`

Using this attribute in a rule causes the Service Router to test each message for the presence of viruses, and attempt to remove any that it finds.

33 Configuring Virus Protection

Virus Scanning Rules

Creating the Ruleset

Follow these steps to create the virus scanning ruleset:

1. Decide whether you wish the Service Router to attempt to clean the viruses that it finds, or simply to prevent the delivery of infected messages. This will determine which of the two virus scanning message attributes you use in your virus scanning ruleset.
2. Create a text file containing the virus scanning rules you wish to use. Each rule will be a single line of text of the form:

message-attribute=mvalue action-attribute=avalue action-attribute=avalue ...

message-attribute is either `VIRUS-FOUND` or `VIRUS-UNCLEANED`. *mvalue* is a numerical value specifying the number of viruses detected/uncleaned. Use a value of 0 to mean none, and a value of 1 to mean one or more.

action-attribute and *avalue* are pairs of action attributes and values as specified in the *OpenMail Technical Reference Guide*. For example, `ACTION=DISCARD`.

3. Save the text file with the name and path
`/var/opt/openmail/rules/ALL-ROUTES.VIR`.
4. Restart the Service Router by using the `omoff` and `omon` commands. For example:

```
omoff -s sr
omon -s sr
```

This causes the Service Router to test all messages, on all routes, for the conditions you specified in the rules, and take the specified action for each case.

Examples

Example 1: Detecting but not cleaning

The file `/var/opt/openmail/rules/ALL-ROUTES.VIR` is as follows:

```
VIRUS-FOUND=1 ACTION=DISCARD NOTIFY="Your message was rejected
because it contained a virus"
VIRUS-FOUND=0 ACTION=ALLOW
```

The Service Router will test all messages for viruses, but will not attempt to clean them. Messages that contain a virus will be discarded, and the sender will receive a notification saying "Your message was rejected because it contained a virus".

Example 2: Detecting and cleaning

The file `/var/opt/openmail/rules/ALL-ROUTES.VIR` is as follows:

```
VIRUS-UNCLEANED=1 ACTION=REJECT NDN-INFO=!ndninfo.txt
VIRUS-UNCLEANED=0 VIRUS-FOUND=1 ACTION=ALLOW
NOTIFY="Virus found and cleaned. Please ensure your
virus scanning software is up-to-date"
```

The Service Router will test all messages for viruses and attempt to clean those that it finds. Messages that are successfully cleaned will cause a notification message to be sent to the sender ("Virus found and cleaned. Please ensure your virus scanning software is up-to-date").

Infected messages that could not be cleaned are rejected, and the sender will receive a standard Non-Delivery Notification with additional text as contained in the file `/var/opt/openmail/rules/ndninfo.txt`.

Determining Which Filetypes to Scan

By default, when you configure virus scanning, all filetypes are scanned. However, you can prevent certain filetypes from being scanned by setting the `SR_VS_IGNORE_ITEM_TYPES` general configuration option to a colon-separated list of file codes you wish to exclude. For example, if you include the following line in the `general.cfg` file, then distribution lists (1166) and text files (1167) will not be scanned:

```
SR_VS_IGNORE_ITEM_TYPES=1166:1167
```

File codes are specified in the file `/var/opt/openmail/nls/language/filetype`, and described in Chapter 7, "Body Part Identification and Conversion".

See the *OpenMail Technical Reference Guide* for more information on configuration options.

Notification and Reporting

Note that not all non-delivery actions specified in a rule will result in a Non-Delivery Notification. `ACTION=DISCARD` will not cause a NDN to be sent, and in that case you should use the `NOTIFY` action attribute in your rule to cause a message to be returned to the sender.

If you use the `NOTIFY` action, the sender of this notification is the user `VIRUS-CHECKER`. The sender of a Non-Delivery Notification (NDN) is always shown as the user `MAIL-SYSTEM`.

Virus Scanning Files

The following files are used by the virus scanning software:

<code>libom_vs.sl</code>	The OpenMail virus scanning shared library. Its location is <code>/opt/openmail/version/lib</code> where <i>version</i> is the OpenMail version number.
<code>libvsapi.1</code>	The Trend Micro virus scanning shared library. Its default location is <code>/etc/iscan</code> . This file is only installed when you install Scanmail for Openmail.
<code>lpt\$vpn.n</code>	The Trend Micro virus signature, or pattern, file. <i>n</i> is a version number. Its default location is <code>/etc/iscan</code> . This file is only installed when you install Scanmail for Openmail.

Reference: Virus Protection Options

`SR_VS_DO_VIRUS_SCAN=FALSE`

In the absense of the `ALL-ROUTES.VIR` ruleset file, this option determines whether virus scanning is active. If the `ALL-ROUTES.VIR` file exists, then the rules within that file determine the virus scanning/cleaning action that will be taken. See the *OpenMail Overview* for more information on `ALL-ROUTES.VIR`.

Set the option to `TRUE` to cause the Service Router to check all message attachments for viruses. If a virus is found, the message is not routed, and OpenMail generates a non-delivery notification.

Set the option to `FALSE` to disable virus checking.

Note that the performance of your OpenMail system may be degraded if you enable virus checking and a large number of viruses are detected, since each virus detected will cause OpenMail to generate a non-delivery report.

`SR_VS_IGNORE_ITEM_TYPES=filetype-no ...`

Specifies the filetypes of items that will not be scanned for viruses.

By default, when virus scanning is enabled, either by setting the `SR_VS_DO_VIRUS_SCAN` option to `TRUE` or by creating the `ALL-ROUTES.VIR` ruleset file, all filetypes are scanned for viruses. Use this option to prevent certain filetypes from being scanned.

filetype-no ... is a colon-separated list of numerical file codes, as specified in

`/var/opt/openmail/nls/language/filetype`, and described in Chapter 7, “Body Part Identification and Conversion”.

For example, set `SR_VS_IGNORE_ITEM_TYPES` to `1167` to prevent text files from being scanned.

See the *OpenMail Overview* for more information on configuring virus protection.

`SR_VS_TEST_SCAN_SL=string`

Specifies the location of the test virus shared library. If this file is in its default location, you must set this option to `/opt/openmail/version/lib/libom_testvs.sl` if you want to test your virus scanning configuration (*version* is the OpenMail version number, for example B.06.00).

See the *OpenMail Overview* for more information on configuring virus protection.

`SR_VS_VIRUS_SCAN_TYPE=string`

Specifies whether virus checking is operating in test mode. Set this option to "Test Scan" to cause the Service Router to check messages and generate a non-delivery notification if the first five characters of any attachment is VIRUS. Note: if you set this option to "Test Scan", you must also set the `SR_VS_TEST_SCAN_SL` option to the location of the test virus shared library.

Set this option to "Trend Micro" to cause the Service Router to check messages for viruses.

Reference: Message Filter Attributes (for use in delivery rulesets)

The Service Router determines if any messages require special handling (for example, to be rejected or have their delivery deferred) by checking the settings of attributes in any *ruleset* specified for a given route. Each rule within a ruleset defines the conditions under which the Service Router should reject or defer the delivery of a message. Rules also specify how the Service Router should handle these messages and the time at which it should perform the specified action.

The contents of the message are compared against each rule within the ruleset to check for a match:

- If all the attributes for a rule are matched, the Service Router performs the action defined for the rule.

If the defined action is to defer the message, it submits the message to the Deferred Mail Manager queue DMM (see the section “Deferred Mail Manager”).

- If not all of the attributes in the ruleset are matched, by default the Service Router continues with its procedure to route the message (see the section “How the Service Router Handles Messages”).

The message attributes related to virus protection are as follows:

- **VIRUS-FOUND**

Specifies whether a message contains a virus. A value of 0 indicates that a virus was not found in the message; a value of 1 indicates that a virus was found.

Include this attribute in a rule to enable virus scanning, but not virus cleaning. See the *OpenMail Overview* for more information on virus protection.

This attribute can only be used in the ruleset **ALL-ROUTES.VIR**, and applies to all routes. It cannot be applied selectively to specified routes.

- **VIRUS-UNCLEANED**

Specifies whether a message that contains a virus could not be cleaned. A value of 0 indicates that the message was checked and was successfully cleaned of any viruses that were found. A value of 1 indicates that the message contained a virus that could not be cleaned.

Include this attribute in a rule to enable virus cleaning. See the *OpenMail Overview* for more information on virus protection.

Reference: Message Filter Attributes (for use in delivery rulesets)

This attribute can only be used in the ruleset `ALL-ROUTES.VIR`, and applies to all routes. It cannot be applied selectively to specified routes.

