

# **ESET Mail Security**

## **Installation Manual and User Guide**

Linux, BSD and Solaris



## ESET Mail Security

Copyright ©2011 by ESET, spol. s r. o.

ESET Mail Security was developed by ESET, spol. s r. o.

For more information visit [www.eset.com](http://www.eset.com).

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r. o. reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: [www.eset.eu/support](http://www.eset.eu/support)

Customer Care North America: [www.eset.com/support](http://www.eset.com/support)

REV. 2011-02-08

## Contents

<b>1. Introduction.....</b>	<b>3</b>
1.1 Main functionality.....	3
1.2 Key features of the system.....	3
<b>2. Terminology and abbreviations.....</b>	<b>5</b>
<b>3. Installation.....</b>	<b>7</b>
<b>4. Architecture Overview.....</b>	<b>8</b>
<b>5. Integration with Email Messaging System...10</b>	
5.1 Bi-directional email message scanning in MTA.....	11
5.2 Scanning of inbound email messages .....	11
5.3 Scanning of outbound email messages.....	11
5.4 Scanning of email messages downloaded from POP3/IMAP server .....	11
5.5 Alternative methods of content filtering.....	12
5.5.1 Scanning email messages in CommuniGate Pro using esets_cgp.....	12
5.5.2 Scanning email messages using AMaViS.....	13
<b>6. Important ESET Mail Security mechanisms.14</b>	
6.1 Handle Object Policy.....	14
6.2 User Specific Configuration.....	14
6.3 Blacklist and Whitelist.....	15
6.4 Anti-Spam Control.....	15
6.5 Samples Submission System.....	16
6.6 Web Interface.....	17
6.6.1 License management .....	17
6.6.2 SMTP+Postfix configuration example.....	18
6.6.3 Statistics .....	19
6.7 Remote Administration.....	19
6.7.1 Remote Administration usage example .....	20
6.8 Logging.....	22
<b>7. ESET Security system update.....23</b>	
7.1 ESETS update utility .....	23
7.2 ESETS update process description.....	23
7.3 ESETS mirror http daemon.....	23
<b>8. Let us know.....24</b>	
<b>9. Appendix A. ESETS setup and configuration.....25</b>	
9.1 Setting ESETS for MTA Postfix.....	25
9.2 Setting ESETS for MTA Sendmail .....	26
9.3 Setting ESETS for MTA Qmail.....	26
9.4 Setting ESETS for MTA Exim version 3.....	27
9.5 Setting ESETS for MTA Exim version 4.....	28
9.6 Setting ESETS for MTA ZMailer.....	28
9.7 Setting ESETS for outbound email message scanning....	29
9.8 Setting ESETS for scanning of POP3 communication .....	29
9.9 Setting ESETS for scanning of IMAP communication.....	29
<b>10. Appendix B. PHP License.....31</b>	

# 1. Introduction

Dear user, you have acquired ESET Mail Security - the premier security system running under the Linux, BSD and Solaris OS. As you will soon find out, ESET's state-of-the-art scanning engine has unsurpassed scanning speed and detection rates combined with a very small footprint that makes it the ideal choice for any Linux, BSD and Solaris OS server.

## 1.1 Main functionality

### Post Office Protocol filter (POP3)

The POP3 filter scans communication between POP3 clients and servers for viruses.

### Simple Mail Transfer Protocol filter (SMTP)

The SMTP filter scans communication between SMTP clients and servers for viruses. In addition it can also serve as a content filter for the Postfix MTA.

### Internet Message Access Protocol filter (IMAP)

The IMAP filter scans communication between IMAP clients and servers for viruses.

### Sendmail content filter

Sendmail content filter accesses mail messages processed by MTA Sendmail and scans them for viruses. It examines and modifies content and meta-information of messages. If an infection cannot be removed from an email message, the message will be rejected.

### External filter plugin for CommuniGate Pro

The CGP module is an external filter plugin for CommuniGate Pro. It reads email filenames from stdin, then requests a scan by ESETS daemon and finally returns a status. It examines (but does not modify) email content and blocks messages with infiltrations in the email body.

### PIPE module

The PIPE is a simple email scanner, that reads email from the standard (stdin) input, then requests an ESETS daemon scan. In case content is accepted, it is submitted to the standard (stdout) output.

## 1.2 Key features of the system

### Advanced engine algorithms

The ESET antivirus scanning engine algorithms provide the highest detection rate and the fastest scanning times.

### Multi-processing

ESET Mail Security is developed to run on single- as well as multi-processor units.

### Advanced Heuristics

ESET Mail Security includes unique advanced heuristics for Win32 worms, backdoor infections and other forms of malware.

### Built-In features

Built-in archivers unpack archived objects without the need for any external programs.

### Speed and efficiency

To increase the speed and efficiency of the system, its architecture is based on the running daemon (resident program) where all scanning requests are sent.

### Enhanced security

All executive daemons (except esets\_dac) run under non-privileged user account to enhance security.

### Selective configuration

The system supports selective configuration based on the user or client/server.

### Multiple logging levels

Multiple logging levels can be configured to get information about system activity and infiltrations.

**Web interface**

Configuration, administration and license management are offered through an intuitive and user-friendly Web interface.

**Remote administration**

The system supports ESET Remote Administration for management in large computer networks.

**No external libraries**

The ESET Mail Security installation does not require external libraries or programs except for LIBC.

**User-specified notification**

The system can be configured to notify specific users in the event of a detected infiltration or other important events.

**Low system requirements**

To run efficiently, ESET Mail Security requires just 16MB of hard-disk space and 32MB of RAM. It runs smoothly under the 2.2.x, 2.4.x and 2.6.x Linux OS kernel versions as well as under 5.x, 6.x FreeBSD OS kernel versions.

**Performance and scalability**

From lower-powered, small office servers to enterprise-class ISP servers with thousands of users, ESET Mail Security delivers the performance and scalability you expect from a UNIX based solution, in addition to the unequalled security of ESET products.

## 2. Terminology and abbreviations

In this section we will review the terms and abbreviations used in this document. Note that a boldface font is reserved for product component names and also for newly defined terms and abbreviations. Terms and abbreviations defined in this chapter are expanded upon later in this document.

### ESETS

*ESET Security* is a standard acronym for all security products developed by ESET, spol. s r. o. for Linux, BSD and Solaris operating systems. It is also the name (or its part) of the software package containing the products.

### RSR

Abbreviation for 'RedHat/Novell(SuSE) Ready'. Note that we also support RedHat Ready and Novell(SuSE) Ready variations of the product. The RSR package differs from the 'standard' Linux version in that it meets the FHS (File-system Hierarchy Standard defined as a part of Linux Standard Base) criteria required by the RedHat Ready and Novell(SuSE) Ready certificate. This means that the RSR package is installed as an add-on application - the primary installation directory is '/opt/eset/esets'.

### ESETS daemon

The main ESETS system control and scanning daemon: *esets\_daemon*.

### ESETS base directory

The directory where ESETS loadable modules containing the virus signature database are stored. The abbreviation *@BASEDIR@* will be used for future references to this directory. The *@BASEDIR@* value for the following Operating Systems is listed below:

```
Linux: /var/lib/esets
Linux RSR: /var/opt/eset/esets/lib
FreeBSD: /var/lib/esets
NetBSD: /var/lib/esets
Solaris: /var/opt/esets/lib
```

### ESETS configuration directory

The directory where all files related to the ESET Mail Security configuration are stored. The abbreviation *@ETCDIR@* will be used for future references to this directory. The *@ETCDIR@* value for the following Operating Systems is listed below:

```
Linux: /etc/esets
Linux RSR: /etc/opt/eset/esets
FreeBSD: /usr/local/etc/esets
NetBSD: /usr/pkg/etc/esets
Solaris: /etc/opt/esets
```

### ESETS configuration file

Main ESET Mail Security configuration file. The absolute path of the file is as follows:

*@ETCDIR@/esets.cfg*

### ESETS binary files directory

The directory where the relevant ESET Mail Security binary files are stored. The abbreviation *@BINDIR@* will be used for future references to this directory. The *@BINDIR@* value for the following Operating Systems is listed below:

```
Linux: /usr/bin
Linux RSR: /opt/eset/esets/bin
FreeBSD: /usr/local/bin
NetBSD: /usr/pkg/bin
Solaris: /opt/esets/bin
```

### ESETS system binary files directory

The directory where the relevant ESET Mail Security system binary files are stored. The abbreviation *@SBINDIR@* will be used for future references to this directory. The *@SBINDIR@* value for the following Operating Systems is listed below:

```
Linux: /usr/sbin
Linux RSR: /opt/eset/esets/sbin
FreeBSD: /usr/local/sbin
NetBSD: /usr/pkg/sbin
Solaris: /opt/esets/sbin
```

## **ESETS object files directory**

The directory where the relevant ESET Mail Security object files and libraries are stored. The abbreviation *@LIBDIR@* will be used for future references to this directory. The *@LIBDIR@* value for the following Operating Systems is listed below:

```
Linux: /usr/lib/esets  
Linux RSR: /opt/eset/esets/lib  
FreeBSD: /usr/local/lib/esets  
NetBSD: /usr/pkg/lib/esets  
Solaris: /opt/esets/lib
```

## 3. Installation

After purchasing ESET Mail Security, you will receive your authorization data (username, password and license key). This data is necessary for both identifying you as our customer and allowing you to download updates for ESET Mail Security. The username/password data is also required for downloading the initial installation package from our web site. ESET Mail Security is distributed as a binary file:

```
esets.i386.ext.bin
```

In the binary file shown above, 'ext' is a Linux, BSD and Solaris OS distribution dependent suffix, i.e., 'deb' for Debian, 'rpm' for RedHat and SuSE, 'tgz' for other Linux OS distributions, 'fbs5.tgz' for FreeBSD 5.x, 'fbs6.tgz' for FreeBSD 6.x, 'nbs4.tgz' for NetBSD 4.x and 'sol10.pkg.gz' for Solaris 10.

Note that the Linux RSR binary file format is:

```
esets-rsr.i386.rpm.bin
```

To install or upgrade the product, use the following command:

```
sh ./esets.i386.ext.bin
```

For the Linux RSR variation of the product, use the command:

```
sh ./esets-rsr.i386.rpm.bin
```

to display the product's User License Acceptance Agreement. Once you have confirmed the Acceptance Agreement, the installation package is placed into the current working directory and relevant information regarding the package's installation, un-installation or upgrade is displayed onscreen.

Once the package is installed, you can verify that the main ESETS service is running by using the following command:

Linux OS:

```
ps -C esets_daemon
```

BSD OS:

```
ps -ax | grep esets_daemon
```

Solaris:

```
ps -A | grep esets_daemon
```

After pressing ENTER, you should see the following (or similar) message:

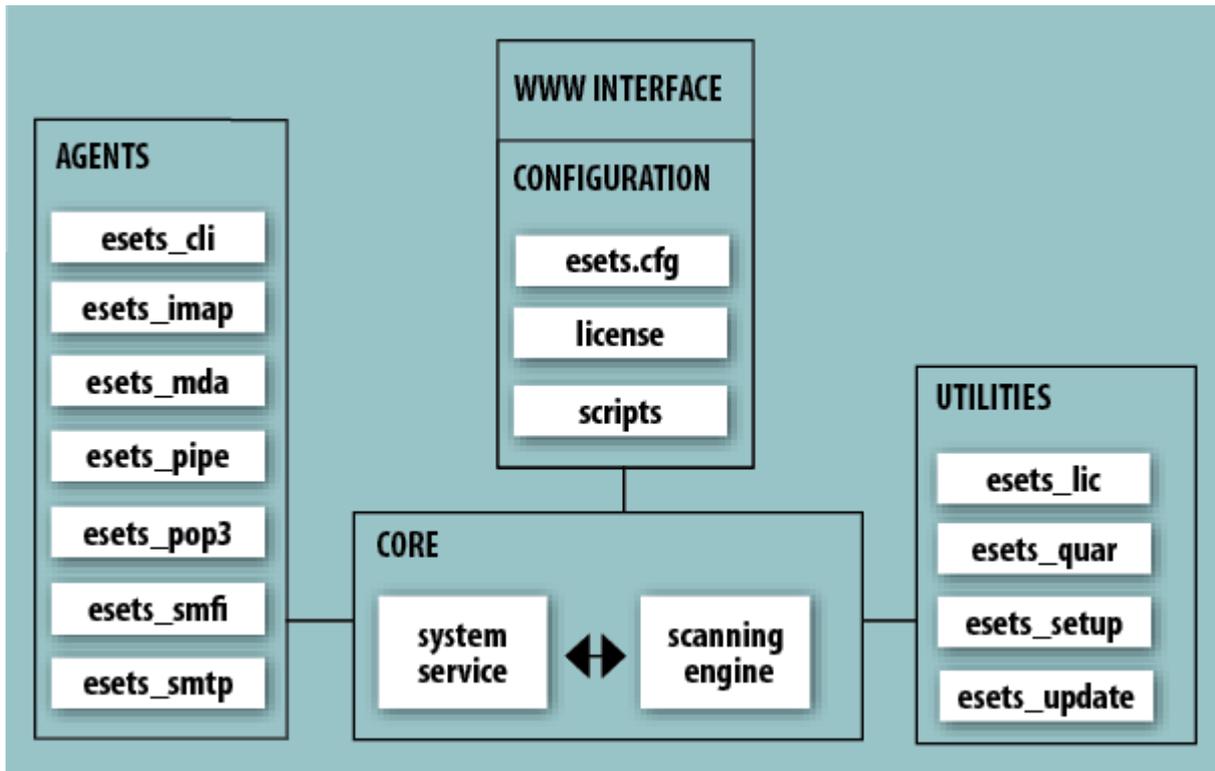
```
PID TTY          TIME CMD
2226 ?             00:00:00 esets_daemon
2229 ?             00:00:00 esets_daemon
```

At least two ESETS daemon processes are running in the background. The first PID represents the process and threads manager of the system. The other represents the ESETS scanning process.

## 4. Architecture Overview

Once ESET Mail Security is successfully installed, you should become familiar with its architecture.

Figure 4-1. Structure of ESET Mail Security.



The structure of ESET Mail Security is shown in Figure 4-1. The system is comprised of the following parts:

### CORE

The Core of ESET Mail Security is the ESETS daemon (`esets_daemon`). The daemon uses ESETS API library `libesets.so` and ESETS loading modules `em00X_xx.dat` to provide base system tasks such as scanning, maintenance of the agent daemon processes, maintenance of the samples submission system, logging, notification, etc. Please refer to the `esets_daemon(8)` man page for details.

### AGENTS

The purpose of ESETS agent modules is to integrate ESETS with the Linux, BSD and Solaris Server environment.

### UTILITIES

The utility modules provide simple and effective management of the system. They are responsible for relevant system tasks such as license management, quarantine management, system setup and update.

### CONFIGURATION

Proper configuration is the most important aspect of a smooth-running security system - the remainder of this chapter is dedicated to explaining all related components. A thorough understanding of the `esets.cfg` file is also highly recommended, as this file contains information essential to the configuration of ESET Mail Security.

After the product is successfully installed, all its configuration components are stored in the ESETS configuration directory. The directory consists of the following files:

#### @ETCDIR@/esets.cfg

This is the most important configuration file, as it controls all major aspects of the product's functionality. The `esets.cfg` file is made up of several sections, each of which contains various parameters. The file contains one global and several "agent" sections, with all section names enclosed in square brackets. Parameters in the global section are used to define configuration options for the ESETS daemon as well as default values for the ESETS scanning engine configuration. Parameters in agent sections are used to define configuration options of modules used to intercept various data flow types in the computer and/or its neighborhood, and prepare it for scanning. Note that in addition to the various parameters used for system configuration, there are also rules governing the organization of the file. For detailed information on the most effective way to organize this file,

please refer to the *esets.cfg(5)* and *esets\_daemon(8)* man pages, as well as relevant agents' man pages.

#### **@ETCDIR@/certs**

This directory is used to store the certificates used by the ESETS web interface for authentication. Please see the *esets\_wwwi(8)* man page for details.

#### **@ETCDIR@/license**

This directory is used to store the product(s) license key(s) you have acquired from your vendor. Note that the ESETS daemon will check only this directory for a valid license key, unless the *'license\_dir'* parameter in the ESETS configuration file is redefined.

#### **@ETCDIR@/scripts/license\_warning\_script**

If enabled by the ESETS configuration file parameter *'license\_warn\_enabled'*, this script will be executed 30 days (once per day) before product license expiration, sending an email notification about the expiration status to the system administrator.

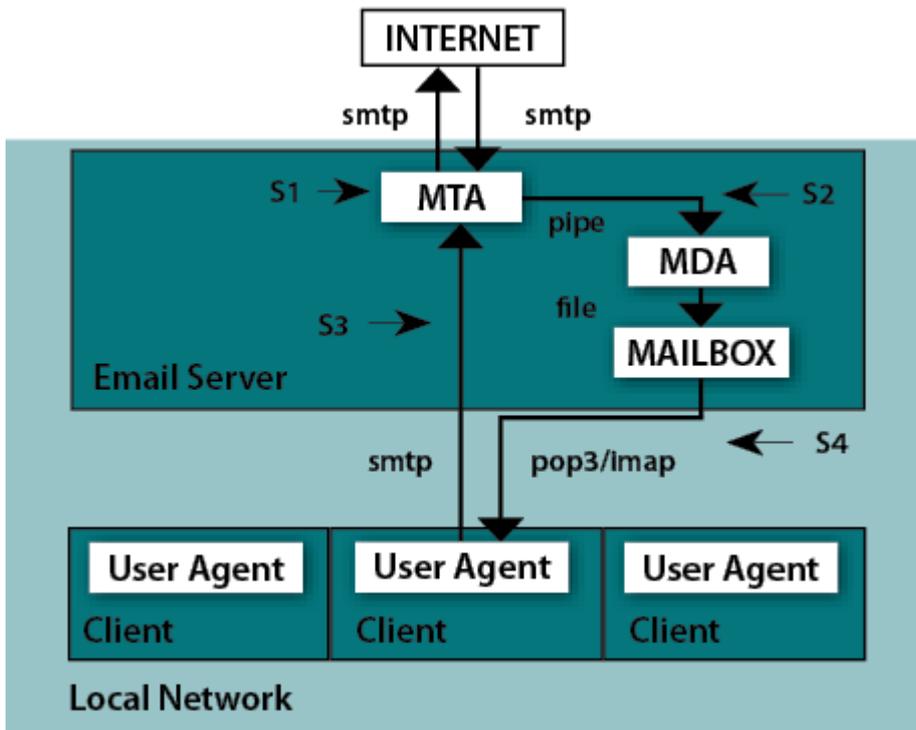
#### **@ETCDIR@/scripts/daemon\_notification\_script**

If enabled by the ESETS configuration file parameter *'exec\_script'*, this script is executed in the event of a detected infiltration by the antivirus system. It is used to send email notification about the event to the system administrator.

## 5. Integration with Email Messaging System

This chapter describes the integration of ESET Mail Security with a variety of known email messaging systems. It is extremely important to understand the basic principles of an email messaging system (see figure 5-1) and how ESET Mail Security integrates with it.

Figure 5-1. Scheme of UNIX OS email messaging system.



### MTA - Mail Transport Agent

A program (e.g., sendmail, postfix, qmail, exim, etc.) that enables the transfer of email messages between local and remote domains.

### MDA - Mail Delivery Agent

A program (e.g., maildrop, procmail, deliver, local.mail, etc.) that enables the delivery of locally addressed email messages into particular mailboxes.

### MUA - Mail User Agent

A program (e.g., Microsoft Outlook, Mozilla Thunderbird, Eudora, etc.) that provides access to and management of email messages, such as reading, composing, printing, etc.

### MAILBOX

A file or file structure on a disk serving as the storage space for email messages.

The email server receives data communication using SMTP (Simple Mail Transfer Protocol) communication. The received message is transferred by MTA either to another remote email messaging system or is delivered using local MDA into a particular MAILBOX. In most cases, each local network user owns a MAILBOX located on the server. Note that it is the responsibility of the user's local MUA to provide the function of downloading and correctly interpreting the message at the user's computer. When retrieving data from MAILBOX, the MUA typically uses POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) to communicate with the MTA. The SMTP protocol is used to send data to the Internet.

The ESETS operating principle is based on data communication interception and scanning at the various phases of its transfer. The interception locations are marked in figure 5-1 by symbols S1, S2, S3 and S4.

- S1 - Bi-directional email message scanning, i.e. content filtering in MTA.
- S2 - Scanning of inbound email messages, i.e. messages with a target address which is located inside the local domain.
- S3 - Scanning of outbound email messages, i.e. messages bound to a remote Internet domain.
- S4 - Scanning of email messages being downloaded from POP3/IMAP server.

The remainder of this chapter reviews methods for integrating ESETS with a variety of supported messaging systems.

## 5.1 Bi-directional email message scanning in MTA

Bi-directional email message scanning mode allows the user to scan inbound email messages as well as outbound, using the same implementation algorithm. The bi-directional content filter method is MTA dependent. ESET Mail Security comes with five content filters that are built for the most common MTA programs, such as MTA Sendmail, Postfix, Exim, QMail and ZMailer.

Check that your MTA is properly configured and running. Then, configure ESET Mail Security for bi-directional email message scanning by running the following script:

```
/usr/sbin/esets_setup
```

Select MTA and content filter install options. The ESETS module being used is also displayed.

Note that the installer backs up all modified configuration files and can display every command that it will execute after your approval. It can also be used for uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

## 5.2 Scanning of inbound email messages

Inbound email message scanning is performed during message transfer between MTA and MDA. Incoming emails are intercepted by the *esets\_mda* module, scanned by the ESETS daemon and delivered to MAILBOX using the original MDA. As shown in figure 5-1, virus scanning can be enabled by setting the proper configuration of MTA and the *esets\_mda* module. ESET Mail Security supports most common MTA programs, such as MTA Sendmail, Postfix, Exim, QMail and ZMailer. ESETS supports any MDA. In particular, the following MDAs were tested: procmail, maildrop, deliver and local.mail.

Check that your MTA is properly configured using the original MDA and that the MTA is running. Then configure ESET Mail Security for inbound email message scanning by running the following script:

```
/usr/sbin/esets_setup
```

Select MDA and inbound install options. The ESETS module used is also displayed.

Note that the installer backs up all modified configuration files and can display every command that it will execute after your approval. Also use it for uninstall. Detailed steps for all possible scenarios are described in the appendix A of this documentation.

## 5.3 Scanning of outbound email messages

Outbound email message scanning is performed during transfer of email messages between the local MUA and the MTA.

Configure ESET Mail Security for outbound email message scanning by running the following script:

```
/usr/sbin/esets_setup
```

Select the SMTP install option. This will set the *esets\_smtp* module to listen on a predefined port and redirect applicable IP packets. Check the newly added firewall rule to see if any changes are necessary.

Note that the installer backs up all modified configuration files and can display every command that it will execute after your approval. It can also be used for uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

## 5.4 Scanning of email messages downloaded from POP3/IMAP server

POP3/IMAP messages scanning is performed during message transfer between MAILBOX and MUA. All emails requested by POP3/IMAP clients are intercepted by the *esets\_pop3* (or *esets\_imap*) agent module and scanned by the ESETS daemon for infiltrations. ESET Mail Security supports most common MUA programs, such as Microsoft Outlook, Evolution, Mozilla Thunderbird and others. Note that there is restriction in ESET Mail Security functionality when emails downloaded by Mozilla Thunderbird using IMAP communication protocol. An email in this case is requested and downloaded part by part and built directly by Mozilla Thunderbird. For this reason it is not possible to write proper information about the infiltrations found into the header and body of the email and thus the functionality is deactivated for this MUA.

To configure ESET Mail Security for scanning of email messages downloaded from POP3 or IMAP server, run the following script:

```
/usr/sbin/esets_setup
```

Select the POP3 or IMAP install option. This will set the given ESETS module to listen on a predefined port and redirect applicable IP packets. Check the newly added firewall rule to see if any changes are necessary.

Note that the installer backs up all modified configuration files and can display every command that it will execute after your

approval. It can also be used for uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

## 5.5 Alternative methods of content filtering

### 5.5.1 Scanning email messages in CommuniGate Pro using esets\_cgp

CommuniGate Pro is the powerful and reliable Unified Communications server and *esets\_cgp* is used for content filtering (anti-virus and anti-spam filtering).

*Esets\_cgp* only allows scanning of incoming email messages. *Esets\_cgp* does not allow modification of scanned email messages and denies ESETS access to clean or delete infected email attachments. As a result, the ESETS footnote with log and status dependent header fields will not be written into the email message. Also, *esets\_cgp* does not provide mail sender/recipient information. Thus, user specific configurations are unavailable and advanced mail handling features (accept, defer, discard, reject) are limited.

#### Integrating the antivirus Plugin with CommuniGate Pro

Please see the VirusScan section of the CommuniGate Pro manual.

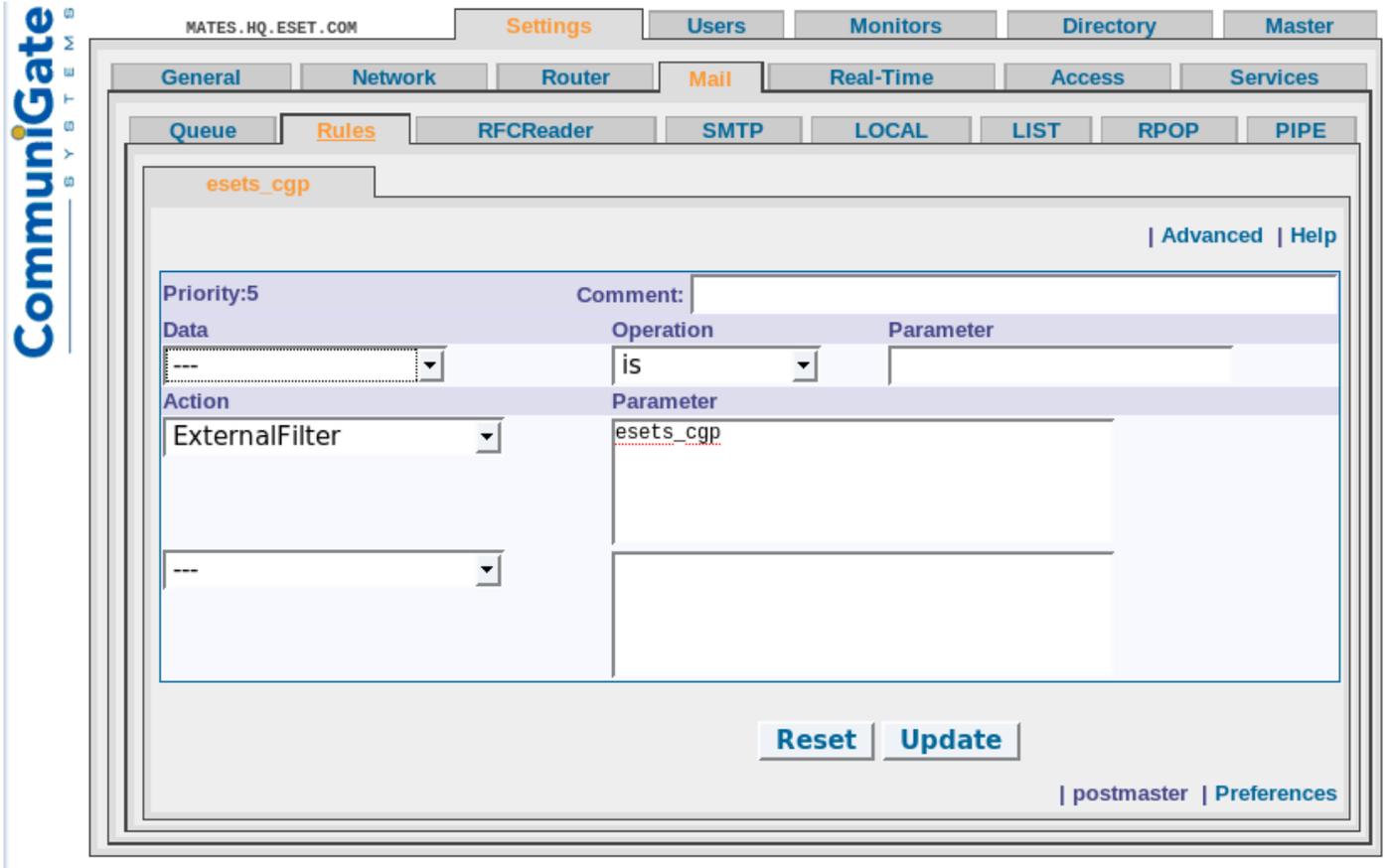
Open the **General** page in the **Settings** section of the WebAdmin Interface and click the **Helpers** link. In panel **Content Filtering** create new filter with followed values:

Figure 5-2. Setting of Content Filtering.

Content Filtering		Help
Enabled	esets_cgp	
Log Level:	Problems	Program Path: /usr/bin/esets_cgp
Time-out:	30 sec	Auto-Restart: 15 sec
Disabled		
Log Level:	Problems	Program Path:
Time-out:	Never	Auto-Restart: Never

Next, open the Mail page in the **Settings** section of the WebAdmin Interface, click the **Rules** link and add a new rule as follows:

Figure 5-3. Rule Settings.



## 5.5.2 Scanning email messages using AMaViS

AMaViS (A Mail Virus Scanner) is a tool that interfaces your MTA with several antivirus scanners. It supports various MTAs and comes in three branches: *amavis*, *amavisd* and *amavisd-new*. Only the *amavisd-new* branch is supported. AMaViS cooperates with ESET Mail Security by using *esets\_cli*. Before explaining the AMaViS configurations, the impact of the ESET Mail Security functionality method is described. AMaViS does not allow modification of scanned email messages and denies ESETS access to clean or delete infected email attachments. As a result, the ESETS footnote with log and status dependent header fields will not be written into the email message. Also, AMaViS does not provide mail sender/recipient information. Thus, user specific configurations are unavailable and advanced mail handling features (accept, defer, discard, reject) are limited for *esets\_cli*. Lastly, AMaViS only scans files, it cannot use the ESETS anti-spam engine.

Taking into account these drawbacks, content filtering using AMaViS is recommended only if the system administrator does not require the features discussed above.

### amavisd-new configuration

To install the product with *amavisd-new*, unpack and install the source *amavisd-new-2.x.y.tgz* in your installation directory. Next, configure the product with the newly installed *amavisd-new*. To do this, delete the clause for 'ESET Software ESETS' and then replace the clause for 'ESET Software ESETS - Client/Server Version' in the file 'amavisd.conf' with the following one:

```
### http://www.eset.com/
['ESET Software ESETS Command Line Interface',
 '@BINDIR@/esets_cli', '--subdir {}',
 [0], [1, 2, 3], qr/virus="([\^"]+)/ ],
```

You may need to install additional Perl modules Archive-Tar, Archive-Zip, BerkeleyDB, Compress-Zlib, Convert-TNEF, Convert-UUlib, IO-stringy, MailTools, MIME-Base64, MIME-tools, Net-Server and Unix-Syslog from:

[www.cpan.org/modules](http://www.cpan.org/modules)

The procedure to install is as follows:

```
perl Makefile.PL; make; make install
```

After configuration, please follow the recommendations for configuring *amavisd-new* in the README.mta located in the Amavisd-new directory according your mail server.

## 6. Important ESET Mail Security mechanisms

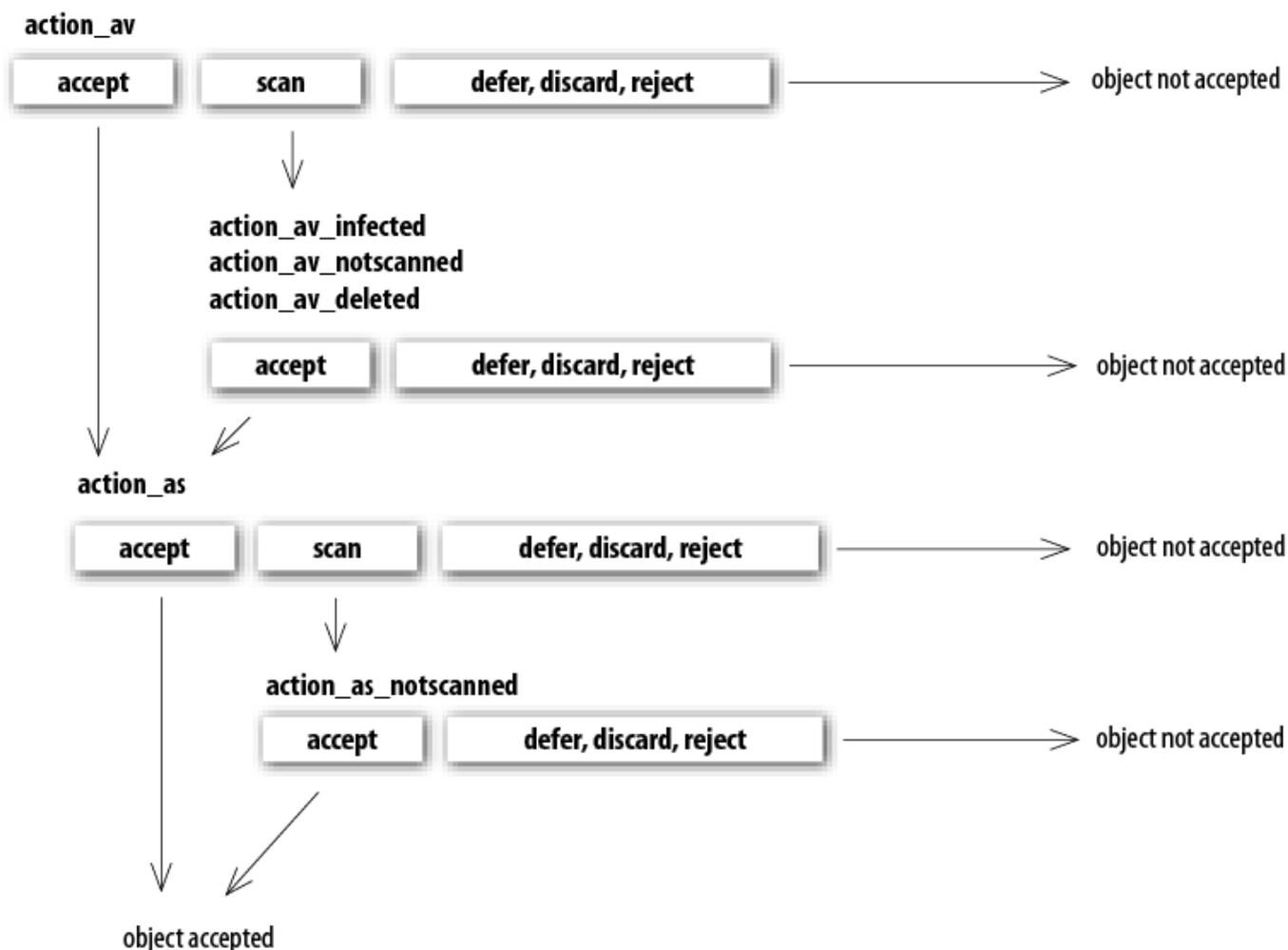
### 6.1 Handle Object Policy

The Handle Object Policy (see figure 6-1) mechanism provides filtering of scanned objects based on their status. This functionality is based on the following configuration options:

- `action_av`
- `action_av_infected`
- `action_av_notscanned`
- `action_av_deleted`

For detailed information on these options, please refer to the `esets.cfg(5)` man page.

Figure 6-1. Scheme of Handle Object Policy mechanism.



Every object processed is first handled according to the configuration of the `'action_av'` option. If this option is set to `'accept'` (or `'defer'`, `'discard'`, `'reject'`) the object is accepted (or deferred, discarded, rejected). If the option is set to `'scan'` the object is scanned for virus infiltrations, and if the `'av_clean_mode'` option is set to `'yes'`, the object is also cleaned. In addition, the configuration options `'action_av_infected'`, `'action_av_notscanned'` and `'action_av_deleted'` are taken into account to further evaluate handling of the object. If an `'accept'` action has been taken as a result of these three action options, the object is accepted. Otherwise, the object is blocked.

### 6.2 User Specific Configuration

The purpose of the User Specific Configuration mechanism is to provide a higher degree of customization and functionality. It allows the system administrator to define ESETS antivirus scanner parameters based on the user who is accessing file system objects.

A detailed description of this functionality can be found in the `esets.cfg(5)` man page; in this section we will provide only a short example of a user-specific configuration.

Here, the *esets\_smtp* module is used as a content filter for MTA Postfix. The functionality of this module is based on the **[smtp]** section in the ESETS configuration file (*esets.cfg*). See below:

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
action_av = "scan"
```

To provide individual parameter settings, define a *'user\_config'* parameter with the path to the special configuration file where the individual setting will be stored. In the example below, we create a reference to the special configuration file *'esets\_smtp\_spec.cfg'*, which is located in the ESETS configuration directory. See below:

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
action_av = "scan"
user_config = "esets_smtp_spec.cfg"
```

Once the special configuration file is referenced from within the **[smtp]** section, create the *'esets\_smtp\_spec.cfg'* file in the ESETS configuration directory and add the appropriate individual settings. The *'esets\_smtp\_spec.cfg'* file should look like this:

```
[rcptuser@rcptdomain.com]
action_av = "reject"
```

Note that the section header identifies the recipient for which the individual settings have been created, and the section body contains individual parameters for this recipient. This configuration will allow all other users attempting to access the file-system to be processed normally. All file system objects accessed by other users will be scanned for infiltrations, except for the user *rcptuser@rcptdomain.com*, whose access will be rejected (blocked).

## 6.3 Blacklist and Whitelist

In the following example we demonstrate blacklist and whitelist creation for the *esets\_smtp* content filter for MTA Postfix configuration. Note that the configuration described in the previous section is used for this purpose.

To create a blacklist used by *esets\_smtp*, create the following group section within the special configuration file *'esets\_smtp\_spec.cfg'*, introduced in the previous section. See below:

```
[black-list]
action_av = "reject"
```

Next, add the SMTP server to the *'black-list'* group. To do this, the following special section must be created:

```
[|sndrname1@sndrdomain1.com]
parent_id = "black-list"
```

In the example above, *'sndrname1@sndrdomain1.com'* is the email address of the sender added to the *'black-list'*. All email messages sent from this address will now be rejected. When creating the *'white-list'* used by *esets\_smtp*, it is necessary to create the following group section in the special configuration file *'esets\_smtp\_spec.cfg'*. See below:

```
[white-list]
action_av = "accept"
action_as = "accept"
```

Adding the sender's email address to the list is self-explanatory.

The *'|'* character is placed in front of the header name of the special section for the sender address and is not placed there for the recipient address. For information regarding the special header name syntax, refer to the man page of the appropriate ESETS agent module. For *esets\_smtp*, refer to the *esets\_smtp(1)* man page.

## 6.4 Anti-Spam Control

The anti-spam system filters spam messages, using dynamic evaluation of the data flow of the email delivery process.

To eliminate spam, ESET Mail Security uses the anti-spam control mechanism. This mechanism can be enabled using the *'action\_as'* parameter. For a full description of the parameter refer to the *esets.cfg(5)* man page. Note that anti-spam scanning can be used only for email objects. Thus, this functionality is relevant only for the following modules: *esets\_imap*, *esets\_mda*, *esets\_pipe*, *esets\_pop3*, *esets\_smtp* and *esets\_smfi*.

Once anti-spam is enabled in any of the configuration sections, the anti-spam scanning engine initializes during the main scanning daemon start-up. During this process, appropriate anti-spam support modules are loaded from the anti-spam cache directory.

To define the period (in minutes), after which ESETS will check for available anti-spam module updates, edit the entry shown below in the ESETS configuration file. If you do not set the value for this parameter, ESETS will not regularly update its anti-spam database:

```
as_update_period = 60
```

Anti-spam functionality can also be configured using the following configuration file:

```
@ETCDIR@/anti-spam/spamcatcher.conf
```

**NOTE:** *SpamCatcher* is a tool for spam detection. It tracks all email communication on its own server and monitors messages rejected by users. It evaluates this and various other data to determine which email is likely to contain spam and sends users a probability score for every message they receive. It allows you to create your own rules for identifying and blacklisting spam. Hundreds of rules can be used to evaluate spam score and block the incoming spam.

The `@ETCDIR@/anti-spam/` directory contains a number of different configurations stored in files, that can be used to customize the anti-spam engine. If you wish to start using a particular configuration, replace the default anti-spam configuration stored in `'spamcatcher.conf'` with any of the available configuration files and reload the ESETS daemon.

### spamcatcher.conf

Is a default configuration file, that contains optimal configuration recommended for typical server environment.

To display differences between any of the files in the anti-spam directory, use the `diff` command. For example, if you wish to compare the `spamcatcher.conf` and the `spamcatcher.conf.accurate` files use the following command:

```
diff spamcatcher.conf spamcatcher.conf.accurate
```

### spamcatcher.conf.accurate

- Bayesian Word Token analysis (i.e. spam filtering using Bayesian Analysis) is enabled. It improves accuracy, but uses more memory and can therefore take slightly more time to finish than other methods.
- The limit of the number of domains queried against the DNS Block List server (DNSBL) is increased (the `'dnsbl_max_domains'` option). DNSBLs are most often used to publish addresses of computers or networks linked to spamming.
- *Sender Policy Framework (SDK)* with live DNS queries will be performed.
- The value of the `'spam_threshold'` parameter is increased. Messages with spam scores equal to or higher than this value will be rejected.
- The *SpamCompiler* version 4 is enabled.

### spamcatcher.conf.fast

- The number of domains queried against the DNS Block List server is reduced.
- The option `'target_throughput'` allowing you to specify throughput in messages per second is enabled.
- Cpu usage during rule file updates is reduced by increasing the size of on-disk cache files.
- TTL's (Time to live) for internal DNS and LiveFeed caches are enabled.

### spamcatcher.conf.no\_livefeed

- The `'livefeed'` option specifies which server is queried for LiveFeed requests. This option is disabled in this configuration file.
- The internal cache for DNS requests is disabled.

## 6.5 Samples Submission System

The Samples submission system is an intelligent *ThreatSense.Net* technology that collects infected objects which have been detected by advanced heuristics and delivers them to the samples submission system server. All virus samples collected by the sample submission system will be processed by the ESET virus laboratory and if necessary, added to the ESET virus signature database.

**NOTE:** According to our license agreement, by enabling sample submission system you are agreeing to allow the computer and/or platform on which the `esets_daemon` is installed to collect data (which may include personal information about you and/or the user of the computer) and samples of newly detected viruses or other threats and send them to our virus lab. This feature is turned off by default. All information collected will be used only to analyze new threats and will not be used for any other purpose.

In order to activate the Samples Submission System, the samples submission system cache must be initialized. This can be achieved by enabling the `'samples_enabled'` option in the **[global]** section of the ESETS configuration file. To allow for the actual delivery of samples to the ESET virus laboratory servers, the parameter `'samples_send_period'` must also be specified in the same

section.

In addition, users can choose to provide the ESET virus laboratory team with supplementary information using the `'samples_provider_mail'` and/or `'samples_provider_country'` configuration options. The information collected using these options will assist in providing the ESET team with an overview about a given infiltration which may be spreading over the Internet.

For more information on the Samples Submission System, refer to the `esets_daemon(8)` man page.

## 6.6 Web Interface

The Web Interface allows user-friendly configuration, administration and license management of ESET Security systems. This module is a separate agent and must be explicitly enabled. To quickly configure the *Web Interface*, set the following options in the ESETS configuration file and restart the ESETS daemon:

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Replace the text in italics with your own values and direct your browser to `'https://address:port'` (note the https). Login with `'username/password'`. Basic usage instructions can be found on the help page and technical details about `esets_wwwi` can be found on the `esets_wwwi(1)` man page.

The web interface allows you to remotely access the ESETS daemon and deploy it easily. This powerful utility makes it easy to read and write configuration values.

Figure 6-1. ESET Security for Linux - Home screen.



The web interface window of ESET Mail Security is divided into two main sections. The primary window, that serves to display the contents of the selected menu option and the main menu. This horizontal bar on the top lets you navigate between the following main options:

- **Home** - provides basic system and ESET product information
- **Licenses** - is a license management utility, see the following chapter for more details
- **Configuration** - you can change the ESET Mail Security system configuration here
- **Control** - allows you to run simple tasks and view global statistics about objects processed by `esets_daemon`
- **Help** - provides detailed usage instructions for the ESET Mail Security web interface
- **Logout** - use to end your current session

### 6.6.1 License management

You can upload a new license using the Web interface, as shown in Figure 6-2.

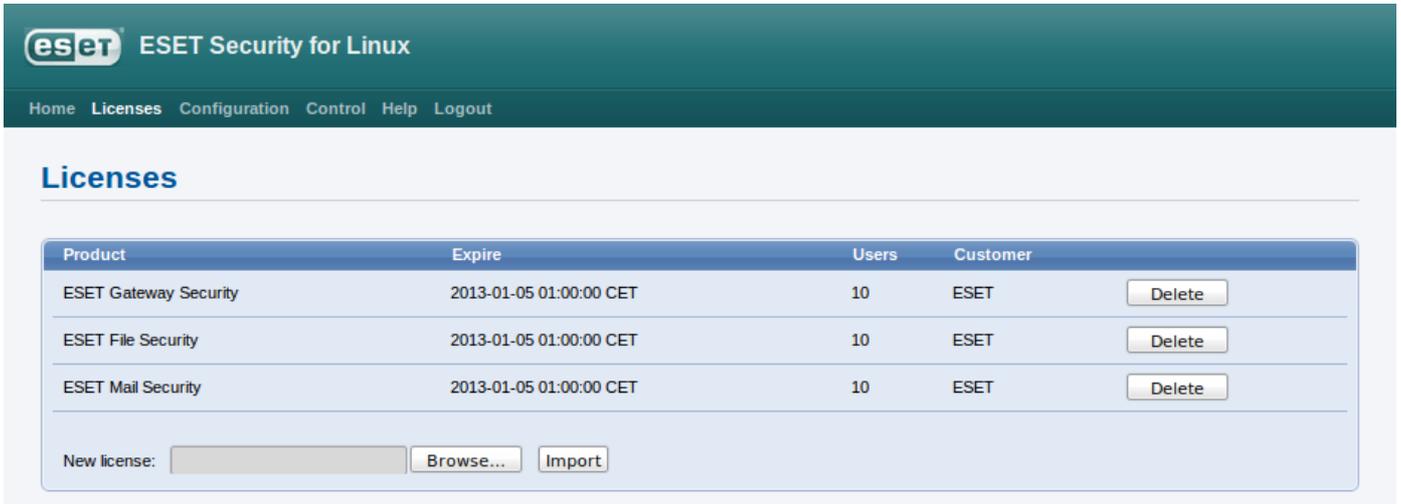
If you want to display licenses in the console, use the following command:

```
/usr/sbin/esets_lic --list
```

If you want to import new license files, use the following command:

```
/usr/sbin/esets_lic --import *.lic
```

Figure 6-2. ESET Licenses.



You can enable the license notification option in the *Global* section options. If enabled, this functionality will notify you 30 days prior to your license expiration.

**NOTE:** If you have a fully functional ESET File/Gateway Security for Linux, BSD and Solaris installation and you wish to expand it by adding ESET Mail Security, you will need to set your new username and password for ESET Mail Security either in the ESETS configuration file, or in the Web interface. This will prevent possible issues with updates in ESETS.

## 6.6.2 SMTP+Postfix configuration example

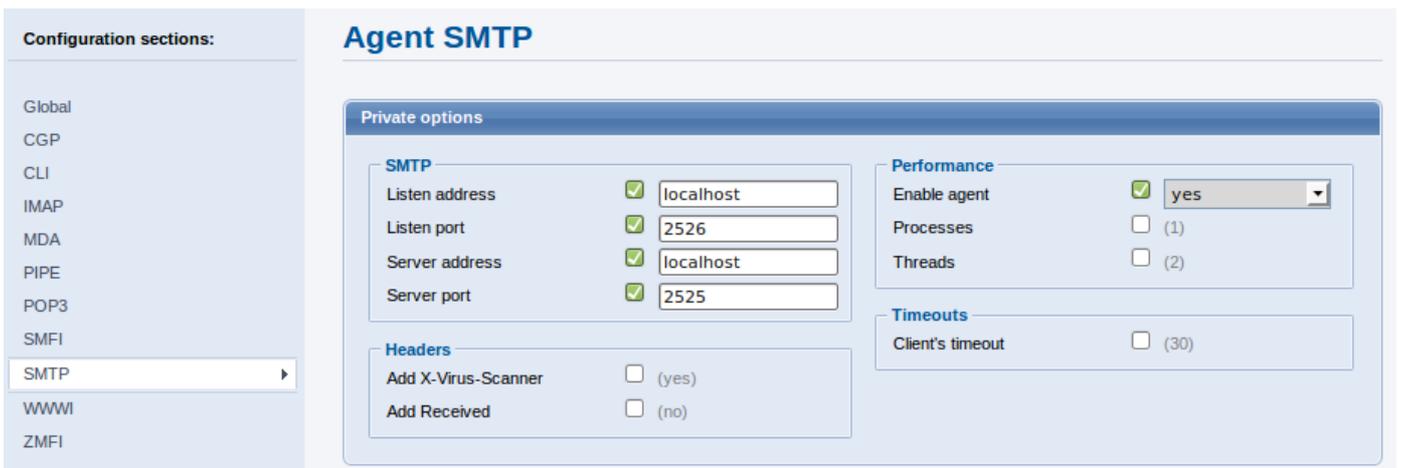
ESETS can be configured in two ways. In this example we will demonstrate how to use both when configuring the SMTP module, leaving you the choice of your preferred configuration method:

- Using the ESETS configuration file:

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
```

- Using the web interface:

Figure 6-3. ESETS - Configuration > SMTP Agent.



Always remember to save your new configuration by clicking **Save changes**. To apply your new changes click the **Apply changes** button in the **Configuration sections** panel.

There are various scanner options you can use to customize the scanning environment: actions, limits, modification masks, targets. Here is an example of a two-way filter based on a spam subject prefix:

```
[smtp]
action_as = "defer"
as_eml_subject_prefix = "[SPAM]"
```

Figure 6-4. SMTP Scanner options.

### 6.6.3 Statistics

You can view statistics for all of active ESETS agents here. *Statistics* summary refreshes every 10 seconds.

Figure 6-5. ESETS - Control > Statistics.

	On demand	On access	Mail	Mail part	Internet	Total
Scanned:	493	2	-	-	21	516
Error:	-	-	-	-	-	-
Infected:	-	-	-	-	2	2
Cleaned:	-	-	-	-	-	-
Spam:	-	-	-	-	-	-
Accepted:	493	1	-	-	19	513
Deferred:	-	-	-	-	-	-
Discarded:	-	-	-	-	-	-
Rejected:	-	1	-	-	2	3

## 6.7 Remote Administration

ESETS supports ESET Remote Administration for mail security management in large computer networks. The ESETS Remote Administration Client is part of the main ESETS daemon and performs the following functions:

- Communicates with ERA Server and provides you with system information, configuration, protection statuses and several other features
- Allows client configurations to be viewed/modified using the ESET Configuration Editor and implemented with the help of configuration tasks
- Can perform *Update Now* tasks
- Performs On-demand scans as requested, and submits the resulting back to ERA Server **Scan Log**
- **NOTE:** For this option to be available you must have a valid license for ESET File Security.
- Adds logs of notable scans performed by the ESETS daemon to **Threat Log**
- Sends all non-debug messages to **Event Log**

These functionalities are not supported:

- Firewall Log
- Remote Install

Figure 6-6. ERA Console tabs.



For more information, please read the ESET Remote Administrator manual. This manual is located on our web site at the following link:

<http://www.eset.com/documentation>

### 6.7.1 Remote Administration usage example

Before commencing any remote administration process ensure your system fulfills the three following prerequisites:

- Running ERA Server
- Running ERA Console
- Enable RA Client in the ESETS daemon. Ensure that firewall settings do not block traffic to ERA Server or vice versa.

To setup the basics, specify the address of your ERA Server in the `'racl_server_addr'` parameter first. If you are using a password to access the ERA Console password, you must edit the value of the `'racl_password'` parameter accordingly. Change the value of the `'racl_interval'` parameter to adjust the frequency of connections to ERA Server (in minutes).

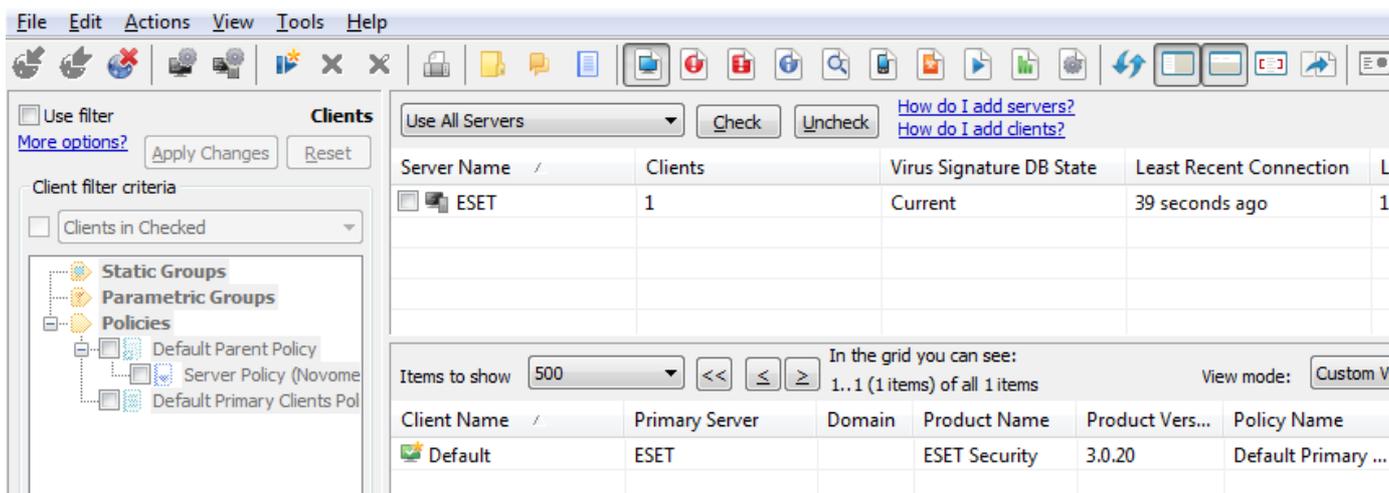
You can either use the web interface (see also previous chapter) to apply the new configuration, or you can adjust these parameters in the `[global]` section of the ESETS configuration file as follows:

```
racl_server_addr = "yourServerAddress"
racl_server_port = 2222
racl_password = "yourPassword"
racl_interval = 1
```

**NOTE:** All applicable ESET Remote Administration Client variables are listed on the `esets_daemon(8)` man page.

The ESETS daemon configuration will be reloaded and RACL will connect to ERA Server. You will be able to see a newly connected client in your ERA Console. Press the F5 button (or **Menu > View > Refresh**) to manually refresh the list of connected clients.

Figure 6-7. ERA Console.

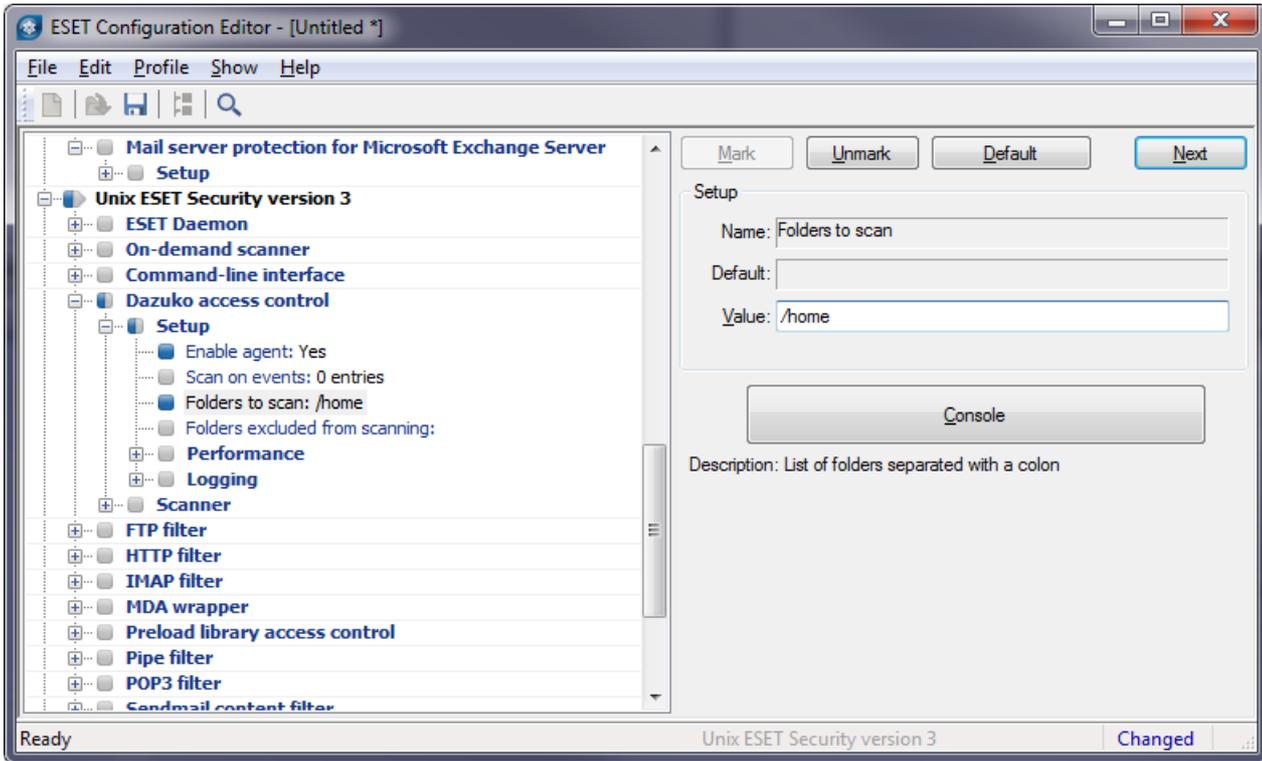


By using ERA Console you can create a configuration task to ESETS daemon from ERA Console:

- Right click the connected **Client Name**
- Navigate to **New Task > Configuration Task > Create...**
- Expand **Unix ESET Security tree**

For an example of a configuration task by the DAC agent, see below:

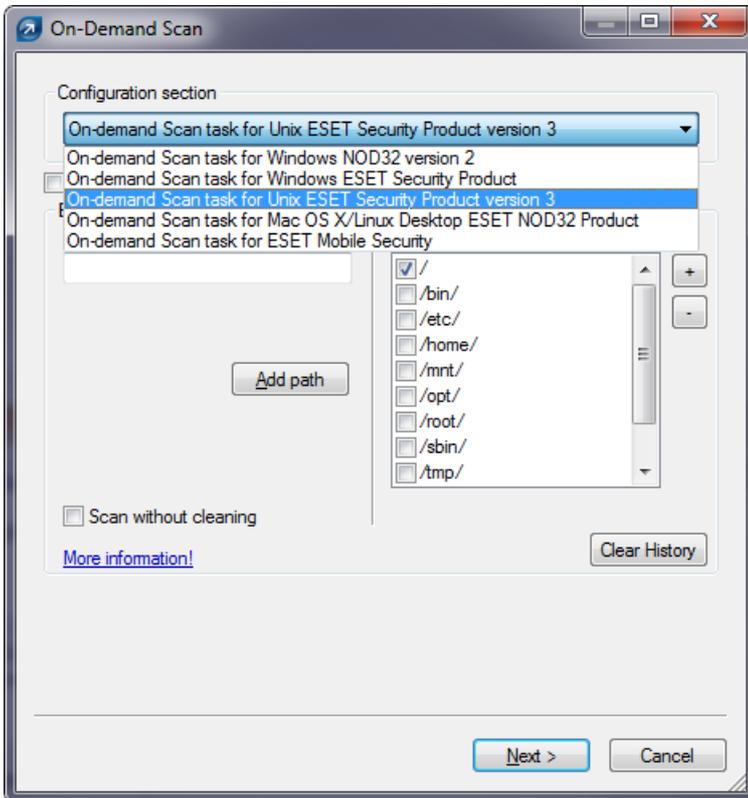
Figure 6-8. ERA Configuration Editor.



The **New Task** context menu contains On-demand scanning options (enabled/disabled cleaning).

You can select the desired product, that you wish to set the task for, in the **On-Demand Scan** pop-up window in the **Configuration Section** drop-down menu. Make sure that you select the **On-demand Scan task for Unix ESET Security Product** option (i.e. the product that is installed on your target workstation).

Figure 6-9. ERA On-demand scan.



## 6.8 Logging

ESETS provides system daemon logging via syslog. *Syslog* is a standard for logging program messages and can be used to log system events such as network and security events.

Messages refer to a facility:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

Messages are assigned a priority/level by the sender of the message:

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

This section describes how to configure and read the logging output of syslog. The `'syslog_facility'` option (default value `'daemon'`) defines the syslog facility used for logging. To modify syslog settings edit the ESETS configuration file or use the web interface. Modify the value of the `'syslog_class'` parameter to change the logging class. We recommend you modify these settings only if you are familiar with syslog. For an example of syslog configuration see below:

```
syslog_facility = "daemon"  
syslog_class = "error:warning:summall"
```

The name and location of the log file depend on your syslog installation and configuration (e.g. rsyslog, syslog-ng, etc.). Standard filenames for syslog output files are for example `'syslog'`, `'daemon.log'`, etc. To follow syslog activity, run one of the following commands from the console:

```
tail -f /var/log/syslog  
tail -100 /var/log/syslog | less  
cat /var/log/syslog | grep eset | less
```

If you enable ESET Remote Administration, ERA log entries older than given days by the option `'rac_logs_lifetime'` will be automatically deleted.

## 7. ESET Security system update

### 7.1 ESETS update utility

To maintain the effectiveness of ESET Mail Security, the virus signature database must be kept up to date. The `esets_update` utility has been developed for this purpose. See the `esets_update(8)` man page for details. To launch an update, the configuration options `'av_update_username'` and `'av_update_password'` must be defined in the **[global]** section of the ESETS configuration file. In the event that your server accesses the Internet via HTTP proxy, the additional configuration options `'proxy_addr'`, `'proxy_port'` must be defined. If access to the HTTP proxy requires a username and password, the `'proxy_username'` and `'proxy_password'` options must also be defined in this section. To initiate an update, enter the following command:

```
@SBINDIR@/esets_update
```

**NOTE:** If you have a fully functional ESET File/Gateway Security for Linux, BSD and Solaris installation and you wish to expand it by adding ESET Mail Security, you will need to set your new username and password for ESET Mail Security either in the ESETS configuration file, or in the Web interface. This will prevent possible issues with updates in ESETS.

To provide the highest possible security for the end user, the ESET team continuously collects virus definitions from all over the world - new patterns are added to the virus signature database in very short intervals. For this reason, we recommend that updates be initiated on a regular basis. To specify the update frequency, the `'av_update_period'` option must be defined in the **[global]** section of the ESETS configuration file. The ESETS daemon must be up and running in order to successfully update the virus signature database.

### 7.2 ESETS update process description

The update process consists of two stages: First, the precompiled update modules are downloaded from the ESET server. If the option `'av_mirror_enabled'` is set to `'yes'` in the **[global]** section of the ESETS configuration file, copies (or mirror) of these update modules are created in the following directory:

```
@BASEDIR@/mirror
```

If desired, the Mirror directory path can be redefined using the `'av_mirror_dir'` option in the **[global]** section of the ESETS configuration file. The newly created Mirror can then serve as a fully functional update server and can be used to create lower (child) Mirror servers. See section 7.3 for details.

The option `'av_mirror_pcu'` allows you to download Program Component Update (PCU) modules for Windows-based ESET security products. These modules can be mirrored from the ESET server.

**NOTE:** Once you set your username, password and license for ESET Mail Security to download PCU's for ESET NOD32 Antivirus / ESET Smart Security, please contact our Technical Support and request a change, that will enable your ESET Mail Security to download PCU's for our Windows-based products.

The second stage of the update process is the compilation of modules loadable by the ESET Mail Security scanner from those stored in the local mirror. Typically, the following ESETS loading modules are created: loader module (`em000.dat`), scanner module (`em001.dat`), virus signature database module (`em002.dat`), archives support module (`em003.dat`), advanced heuristics module (`em004.dat`), etc. The modules are created in the following directory:

```
@BASEDIR@
```

This is the directory where the ESETS daemon loads modules from and thus can be redefined using the `'base_dir'` option in the **[global]** section of the ESETS configuration file.

### 7.3 ESETS mirror http daemon

ESETS mirror http daemon is installed automatically with ESET Mail Security. The http mirror daemon starts if the option `'av_mirror_httpd_enabled'` in the **[global]** section of the ESETS configuration file is set to `'yes'` and the Mirror is enabled.

Options `'av_mirror_httpd_port'` and `'av_mirror_httpd_addr'` define the port (default 2221) and address (default: all local tcp addresses) where the http server listens.

The option `'av_mirror_httpd_auth_mode'` allows access authentication (default: none) to be changed to basic. The options `'av_mirror_httpd_username'` and `'av_mirror_httpd_password'` allow an administrator to define the login and password used to access the Mirror.

## 8. Let us know

Dear user, we hope this Guide has provided you with a thorough understanding of the requirements for ESET Mail Security installation, configuration and maintenance. However, our goal is to continually improve the quality and effectiveness of our documentation. If you feel that any sections in this Guide are unclear or incomplete, please let us know by contacting Customer Care:

<http://www.eset.com/support>

or use directly the support form:

<http://www.eset.eu/support/form>

We are dedicated to provide the highest level of support and look forward to helping you should you experience any problems concerning this product.

# 9. Appendix A. ESETS setup and configuration

## 9.1 Setting ESETS for MTA Postfix

### Inbound email message scanning

**Warning:** This installation is not compatible with SELinux. Either disable SELinux or proceed to the next section.

The objective of this installation is to insert *esets\_mda* before the original Postfix MDA. The MDA to be used (with arguments) is set in the Postfix parameter *'mailbox\_command'*.

**NOTE:** If the *'mailbox\_command'* value is empty, Postfix alone is delivering mail. You must install and configure a real MDA (e.g. procmail) and use that first for the *'mailbox\_command'* and arguments (e.g. */usr/bin/procmail -d "\$USER"*). Reload Postfix and make sure it is delivering mail according to your needs. You may then continue with the ESETS installation.

Take the full path to the current Postfix MDA and set the parameter *'mda\_path'* in the **[mda]** section of the ESETS configuration file to:

```
mda_path = "/usr/bin/procmail"
```

Restart the ESETS daemon. Then, replace the path to the current Postfix MDA with *esets\_mda* path and add *--recipient="\$RECIPIENT" --sender="\$SENDER"* to the arguments, as in the following example:

```
mailbox_command = @BINDIR@/esets_mda -d "$USER" -- --recipient="$RECIPIENT" --sender="$SENDER"
```

To re-read the newly created configuration, reload Postfix.

### Bi-directional email message scanning

The objective of this installation is to divert all mail from Postfix to *esets\_smtp* and get them back to Postfix. In the **[smtp]** section of the ESETS configuration file, set the following parameters:

```
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
```

Restart the ESETS daemon; *esets\_smtp* will be started and will scan all SMTP communication accepted on *'listen\_addr:listen\_port'* and forward it to *'server\_addr:server\_port'*. To divert all mail to *esets\_smtp* set the following in Postfix:

```
content_filter = smtp:[127.0.0.1]:2526
```

**NOTE:** If the *'content\_filter'* parameter already has a value, do not follow these instructions. Instead, you must insert *esets\_smtp* (or other ESETS mail scanning module) before or after your current *'content\_filter'*.

Lastly, set Postfix to accept mail on port 2525 and continue processing it. To do this, add the following entry to the Postfix *master.cf* file:

```
localhost:2525 inet  n  -  n  -  -  smtpd
-o content_filter=
-o myhostname=esets.yourdomain.com
-o local_recipient_maps=
-o relay_recipient_maps=
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
```

Replace *yourdomain.com* with your hostname. Make sure all but the first line is indented. To re-read the newly created configuration, reload Postfix.

**NOTE:** If you have SELinux enabled, it will prevent Postfix from listening on 2525 (e.g. Fedora Core >= 5), In this case, run the following command:

```
semanage -a -t smtp_port_t -p tcp 2525
```

## 9.2 Setting ESETS for MTA Sendmail

### Inbound email message scanning

**Warning:** This installation is not compatible with SELinux. Either disable SELinux or proceed to the next section.

The objective of this installation is to insert *esets\_mda* before Sendmail's original MDA.

**NOTE:** On FreeBSD, Sendmail may be communicating with MDA using LMTP. However, *esets\_mda* does not understand LMTP. If you have `FEATURE(local_lmtp)` in `'hostname'.mc`, comment it out now and recreate `sendmail.cf`.

The currently used MDA can be found in the file `sendmail.cf` in section `Mlocal: parameters 'P'` (executable) and `'A'` (its name and arguments).

First, set the `'mda_path'` in the `[mda]` section of the ESETS configuration file to the currently used MDA executable (Sendmail's `'P'` parameter). Then restart the ESETS daemon.

Next, add the lines below to the `sendmail.mc` file (or `'hostname'.mc` on FreeBSD and Solaris) before all MAILER definitions:

```
define('LOCAL_MAILER_PATH', '@BINDIR@/esets_mda')dnl
define('LOCAL_MAILER_ARGS', 'esets_mda original_arguments -- --sender $f --recipient $u@$j')dnl
```

In the example above, `original_arguments` is Sendmail's `'A'` parameter without the name (first word).

Lastly, recreate `sendmail.cf` and restart Sendmail.

### Bi-directional email message scanning

The objective of this installation is to scan all mail in Sendmail using the *esets\_smfi* filter. In the `[smfi]` section of the ESETS configuration file, set the following parameters:

```
agent_enabled = yes
smfi_sock_path = "/var/run/esets_smfi.sock"
```

Restart the ESETS daemon. Then, add the lines below to the `sendmail.mc` file (or `'hostname'.mc` on FreeBSD) before all MAILER definitions:

```
INPUT_MAIL_FILTER('esets_smfi', 'S=local:/var/run/esets_smfi.sock, F=T, T=S:2m;R:2m;E:5m')dnl
```

With these settings, Sendmail will communicate with *esets\_smfi* via unix socket `'/var/run/esets_smfi.sock'`. Flag `'F=T'` will result in a temporary failed connection if the filter is unavailable. `'S:2m'` defines a 2 minute timeout for sending information from MTA to the filter, `'R:2m'` defines a 2 minute timeout for reading replies from the filter and `'E:5m'` sets an overall 5 minute timeout between sending end-of-message to the filter and waiting for final acknowledgment.

If the timeouts for the *esets\_smfi* filter are too short, Sendmail can temporarily defer the message to the queue and attempt to pass it through later. However, this may lead to continuous deferral of the same messages. To avoid this problem, the timeouts should be set properly. You can experiment with Sendmail's `'confMAX_MESSAGE_SIZE'` parameter, which is the maximum accepted message size in bytes. Taking into account this value and the approximate maximum time for MTA to process a message of that size (this can be measured), you can determine the most effective timeout settings for the *esets\_smfi* filter.

Lastly, recreate `sendmail.cf` and restart Sendmail.

## 9.3 Setting ESETS for MTA Qmail

### Inbound email message scanning

The objective of this installation is to insert *esets\_mda* before Qmail's local delivery agent. Assuming Qmail is installed in the `/var/qmail` directory, in the `[mda]` section of the ESETS configuration file, set the following parameter:

```
mda_path = "/var/qmail/bin/qmail-esets_mda"
```

Restart the ESETS daemon. Create the file `/var/qmail/bin/qmail-esets_mda` with the following content and run `'chmod a+x'` on it:

```
#!/bin/sh
exec qmail-local -- "$USER" "$HOME" "$LOCAL" "" "$EXT" "$HOST" "$SENDER" "$1"
```

This will cause *esets\_mda* to call Qmail's local delivery agent. Next, create the file `/var/qmail/bin/qmail-start.esets` with the following content and also run `'chmod a+x'` on it:

```
#!/bin/sh
A="$1"; shift
exec qmail-start.orig "|@BINDIR@/esets_mda '$A'" -- --sender="$SENDER" --recipient="$RECIPIENT" "$@"
```

This will start Qmail using `esets_mda` for local deliveries. However, the original delivery specification is passed to `qmail-local` through `esets_mda`. Note that in this configuration `esets_mda` will use Qmail's recognized exit codes (see the `qmail-command(8)` man page). Lastly, replace `qmail-start` using commands:

```
mv /var/qmail/bin/qmail-start /var/qmail/bin/qmail-start.orig
ln -s qmail-start.esets /var/qmail/bin/qmail-start
```

Restart Qmail.

### Bi-directional email messages scanning

The objective of this installation is to insert `esets_mda` before `qmail-queue`, which queues all mails before delivery. Assuming Qmail is installed in the `/var/qmail` directory, in the `[mda]` section of the ESETS configuration file, set the following parameter:

```
mda_path = "/var/qmail/bin/qmail-queue.esets"
```

Restart the ESETS daemon. Lastly, replace `qmail-queue` using these commands:

```
mv /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.esets
ln -s @BINDIR@/esets_mda /var/qmail/bin/qmail-queue
```

Restarting Qmail is unnecessary. All messages enqueued from now will be scanned by ESETS. Note that in this configuration `esets_mda` will use `qmail-queue`'s exit codes (see the `qmail-queue(8)` man page).

## 9.4 Setting ESETS for MTA Exim version 3

### Inbound email messages scanning

The objective of this installation is to create an Exim transport from `esets_mda` for local users. In the `[mda]` section of the ESETS configuration file set the following parameter:

```
mda_path = "/usr/sbin/exim"
```

In the above, `/usr/sbin/exim` is the full path to Exim binary. Restart the ESETS daemon. Next, add the following transport (on any line) to the list of Exim transports:

```
esets_transport:
  driver = pipe
  command = @BINDIR@/esets_mda -oi -oMr esets-scanned $local_part@$domain \
  -- --sender=$sender_address --recipient=$local_part@$domain
  user = mail
```

In the above example, `'mail'` is one of Exim's `'trusted_users'`. Now add the following director to the top of the list of Exim directors:

```
esets_director:
  driver = smartuser
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

This will send all unscanned mails for local users to `esets_mda`; `esets_mda` will then send them back to Exim for further processing. To re-read the newly created configuration, restart Exim.

### Bi-directional email message scanning

The goal of this installation is to create an Exim transport from `esets_mda` for all mail. Perform all steps from the previous section, but also add this router to the top of the Exim router list:

```
esets_router:
  driver = domainlist
  route_list = "* localhost byname"
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

## 9.5 Setting ESETS for MTA Exim version 4

### Inbound email message scanning

The goal of this installation is to create an Exim transport from *esets\_mda* for local users. In the *[mda]* section of the ESETS configuration file, set this parameter:

```
mda_path = "/usr/sbin/exim"
```

or, if you are using FreeBSD, this parameter:

```
mda_path = "/usr/local/sbin/exim"
```

where */usr/sbin/exim* (or */usr/local/sbin/exim*) is the full path to the Exim binary. Then restart the ESETS daemon. Add this router to the top of the Exim router list:

```
esets_router:
  driver = accept
  domains = +local_domains
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

and this transport (at whatever location) to the list of Exim transports:

```
esets_transport:
  driver = pipe
  command = @BINDIR@/esets_mda -oi -oMr esets-scanned $local_part@$domain \
  -- --sender=$sender_address --recipient=$local_part@$domain
```

This will send all unscanned mails for local users to *esets\_mda*; *esets\_mda* will then send them back to Exim for further processing. To re-read the newly created configuration, restart Exim.

### Bi-directional email message scanning

The goal of this installation is to create an Exim transport from *esets\_mda* for all mail. Perform all steps from the previous section, but omit this line in *esets\_router*:

```
domains = +local_domains
```

## 9.6 Setting ESETS for MTA ZMailer

### Inbound email message scanning

The goal of this installation is to use *esets\_mda* as ZMailer's local delivery agent. However, you must have a real MDA installed, such as *procmail*. In the *[mda]* section of the ESETS configuration file, set this parameter:

```
mda_path = "/path/to/procmail"
```

and restart the ESETS daemon. *Procmail* doesn't support the full email address as a recipient, so comment out this line in ZMailer's *router.cf* prepending a '#':

```
localdoesdomain=1
```

Next, in the *'local/\*'* clause of *scheduler.conf*, replace your current delivery command with:

```
command="sm -c $channel esets"
```

and append this line to *sm.conf* (replace *your.hostname.com* with your FQDN):

```
esets sSPfn @BINDIR@/esets_mda esets_mda -a $h -d $u -- --sender $g --recipient $u@your.hostname.com
```

Finally, restart ZMailer.

### Bi-directional email messages scanning

The goal of this installation is to use *esets\_zmfi* as ZMailer's SMTP contentfilter. First start the ESETS daemon. Then add this line to *smtpserver.conf*:

```
PARAM contentfilter @BINDIR@/esets_zmfi
```

and restart ZMailer.

Please note that this will scan only the email messages coming through the *smtpserver*. Also, make sure that your *smtp-policy* is filtering all email according to your needs.

## 9.7 Setting ESETS for outbound email message scanning

Outbound email message scanning is performed using the *esets\_smtp* daemon. In the *[smtp]* section of the ESETS configuration file, set these parameters:

```
agent_enabled = yes
listen_addr = "192.168.1.0"
listen_port = 2525
```

where *'listen\_addr'* is the address of the local network interface named *if0*. Then, restart the ESETS daemon. The next step is to redirect all SMTP requests to *esets\_smtp*. If IP-filtering is being performed by the *ipchains* administration tool, an appropriate rule would be:

```
ipchains -A INPUT -p tcp -i if0 --dport 25 -j REDIRECT 2525
```

If IP-filtering is being performed by the *iptables* administration tool, the rule is:

```
iptables -t nat -A PREROUTING -p tcp -i if0 --dport 25 -j REDIRECT --to-ports 2525
```

On FreeBSD, the rule is as follows:

```
ipfw add fwd 192.168.1.10,2525 tcp from any to any 25 via if0 in
```

On NetBSD and Solaris:

```
echo 'rdr if0 0.0.0.0/0 port 25 -> 192.168.1.10 port 2525 tcp' | ipnat -f -
```

**Warning:** Your MTA may accept all connections without extensive checking from *esets\_smtp* because those connections are local. By using your own firewall rules, make sure you do not create an open relay, i.e., allow someone from the outside to connect to *esets\_smtp* and use it as a relay SMTP server.

## 9.8 Setting ESETS for scanning of POP3 communication

The POP3 communication scanning is performed using *esets\_pop3* daemon. In the *[pop3]* section of the ESETS configuration file, set these parameters:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8110
```

where *'listen\_addr'* is the address of the local network interface named *if0*. Then restart the ESETS daemon. The next step is to redirect all POP3 requests to *esets\_pop3*. If IP-filtering is being performed by the *ipchains* administration tool, an appropriate rule is:

```
ipchains -A INPUT -p tcp -i if0 --dport 110 -j REDIRECT 8110
```

If IP-filtering is being performed by the *iptables* administration tool, the rule would be:

```
iptables -t nat -A PREROUTING -p tcp -i if0 --dport 110 -j REDIRECT --to-ports 8110
```

On FreeBSD, the rule is as follows:

```
ipfw add fwd 192.168.1.10,8110 tcp from any to any 110 via if0 in
```

On NetBSD and Solaris:

```
echo 'rdr if0 0.0.0.0/0 port 110 -> 192.168.1.10 port 8110 tcp' | ipnat -f -
```

## 9.9 Setting ESETS for scanning of IMAP communication

The IMAP communication scanning is performed using the *esets\_imap* daemon. In the *[imap]* section of the ESETS configuration file, set these parameters:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8143
```

where *'listen\_addr'* is the address of the local network interface named *if0*. Then restart the ESETS daemon. The next step is to redirect all IMAP requests to *esets\_imap*. If IP-filtering is being performed by the *ipchains* administration tool an appropriate rule would be:

```
ipchains -A INPUT -p tcp -i if0 --dport 143 -j REDIRECT 8143
```

If IP-filtering is being performed by the *iptables* administration tool, the rule is:

```
iptables -t nat -A PREROUTING -p tcp -i if0 --dport 143 -j REDIRECT --to-ports 8143
```

On FreeBSD, the rule is as follows:

```
ipfw add fwd 192.168.1.10,8143 tcp from any to any 143 via if0 in
```

On NetBSD and Solaris:

```
echo 'rdr if0 0.0.0.0/0 port 143 -> 192.168.1.10 port 8143 tcp' | ipnat -f -
```

## 10. Appendix B. PHP License

The PHP License, version 3.01 Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [group@php.net](mailto:group@php.net).
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from [group@php.net](mailto:group@php.net). You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.