ESET MAIL SECURITY

Installation Manual and User Guide

(intended for product version 4.5 and higher)

Linux and FreeBSD

Click here to download the most recent version of this document

ESET **MAIL SECURITY**

Copyright ©2015 by ESET, spol. s r. o.
ESET Mail Security was developed by ESET, spol. s r. o.
For more information visit 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.

Worldwide Customer Support: www.eset.com/support

REV. 11/13/2015

Contents

1. Introduction to ESET Mail Security ... 3
1.1 Main functionality ... 3
1.2 Key features of the system ... 3
1.3 What's new ... 4
2. Terminology and abbreviations ... 5
3. System requirements ... 6
4. Installation ... 7
4.1 Upgrading to a more recent version ... 8
5. Architecture Overview ... 9
6. Integration with Email Messaging System ... 11
6.1 Bi-directional email message scanning in MTA ... 12
6.2 Scanning of inbound email messages ... 12
6.3 Scanning of outbound email messages ... 12
6.4 Scanning of email messages downloaded from POP3/IMAP server ... 12
6.5 Alternative methods of content filtering ... 13
6.5.1 Scanning email messages in CommuniGate Pro ... 13
6.5.2 Scanning email messages using AMaViS ... 14
6.5.3 Scanning email messages using Novell GroupWise ... 15
7. Important ESET Mail Security mechanisms ... 16
7.1 Handle Object Policy ... 16
7.2 User Specific Configuration ... 16
7.3 Blacklist and Whitelist ... 17
7.4 Anti-Spam control ... 17
7.5 Samples Submission System ... 18
7.6 Scheduler ... 18
7.7 Web Interface ... 19
7.7.1 License management ... 20
7.7.2 SMTP+Postfix configuration example ... 20
7.7.3 Scheduler ... 22
7.7.4 Statistics ... 23
7.8 Remote Administration ... 23
7.8.1 Connecting with ESET Remote Administrator ... 23
7.8.2 ESET Remote Administrator usage example (6.x) ... 24
7.8.3 ESET Remote Administrator usage example (5.x) ... 26
7.9 Logging ... 27
7.10 Command-line programs ... 28
8. ESET Security system update ... 29
8.1 ESETS update utility ... 29
8.2 ESETS update process description ... 29
8.3 ESETS mirror http daemon ... 29
9. Let us know ... 30
10. Appendix A. ESETS setup and configuration ... 31
10.1 Setting ESETS $PATH environment variable ... 31
10.2 Setting ESETS for MTA Postfix ... 31
10.3 Setting ESETS for MTA Sendmail ... 32
10.4 Setting ESETS for MTA Qmail ... 33
10.5 Setting ESETS for MTA Exim version 3 ... 33
10.6 Setting ESETS for MTA Exim version 4 ... 34
10.7 Setting ESETS for MTA ZMailer ... 34
10.8 Setting ESETS for MTA Novell GroupWise ... 35
10.9 Setting ESETS for outbound email message scanning ... 35
10.10 Setting ESETS for scanning of POP3 communication ... 35
10.11 Setting ESETS for scanning of IMAP communication ... 36
10.12 Setting ESETS to enable Mail reporting functionality ... 36
10.13 Setting ESETS to send email notifications on virus detection ... 37
11. Appendix B. PHP License ... 38

1. Introduction to ESET Mail Security

Thank you for using ESET Mail Security (ESETS) - the premier security system for Linux and FreeBSD.

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 server on Linux and FreeBSD.

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. Additionally, 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

The 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.

Antispam

Unsolicited email, called spam, ranks among the greatest problems of electronic communication. Spam represents up to 80 percent of all email communication. Antispam protection serves to protect against this problem. Combining several email security principles, the Antispam module provides superior filtering to keep users and their inbox clean.

E**mail reporting**

Email reporting records statistics for each domain group over a specific period or automatically by setting a schedule. In addition, it allows you to send completed reports to specific email address(es).

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 requiring any external programs.

Speed and efficiency

To increase the speed and efficiency of the system, ESET Mail Security's 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 a 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 Administrator for management in large computer networks.

No external libraries

The ESET Mail Security installation does not require external libraries or programs except for LIBC and several core utilities (ED, etc.).

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 250MB of hard-disk space and 256MB of RAM. It runs smoothly under the 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 unequaled security of ESET security products.

1.3 What's new

We strongly recommend that you upgrade to the most recent version of ESET Mail Security.

ESET Mail Security 4.5.2

- Support for ESET Remote Administrator 6.x
- Enhanced email statistics reporting
- New built-in anti-spam module
- Threat notifications enhancements
- Bugfixes and compatibility issues resolved

ESET Mail Security 4.0.10

- Installation/upgrade method is easier and improved
- Samples submission system based on the *ThreatSense.Net* technology

ESET Mail Security 4.0.8

- Support for multi-license keys
- Web interface
- Support for Novell GroupWise
- Support for FreeBSD 8
- New design of Web interface with extended functions
- Scheduler functionality added

2. Terminology and abbreviations

In this section, we will review the terms and abbreviations used in this document. Note that 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 on later in this document.

ESETS

ESET Security is a standard acronym for all security products developed by ESET, spol. s r. o. for Linux and FreeBSD operating systems. It is also the name of the software package containing the products.

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 (depending on the operating system) is listed below:

```
Linux: /var/opt/eset/esets/lib
FreeBSD: /var/lib/esets
```

ESETS cache directory

The directory where ESETS cache and temporary files (such as quarantine files or reports) are stored. The *@CACHEDIR@* value (depending on the operating system) is listed below:

```
Linux: /var/opt/eset/esets/cache
FreeBSD: /var/cache/esets
```

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 (depending on the operating system) is listed below:

```
Linux: /etc/opt/eset/esets
FreeBSD: /usr/local/etc/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 (depending on the operating system) is listed below:

```
Linux: /opt/eset/esets/bin
FreeBSD: /usr/local/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 (depending on the operating system) is listed below:

```
Linux: /opt/eset/esets/sbin
FreeBSD: /usr/local/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 (depending on the operating system) is listed below:

```
Linux: /opt/eset/esets/lib
FreeBSD: /usr/local/lib/esets
```

Note: In a 64-bit Linux operating system environment there are some 32-bit libraries available in the following directory (for example, the *libesets_pac.so* preload library to scan 32-bit binary files):

```
Linux: /opt/eset/esets/lib32
```

3. System requirements

The following hardware requirements must be met before the installation process in order to run ESET Mail Security properly:

- 250MB of hard-disk space
- 256MB of RAM
- glibc 2.3.6 or later
- 2.6.x and later Linux OS kernel versions

ESET Mail Security should work on most recent and frequently used open-source Linux distributions if the above criteria are met. The following operating systems are officially supported:

Operating system	**x86**	**x64**
Ubuntu 12.04 LTS	Yes	Yes
Red Hat Enterprise Linux 6	Yes	Yes
Red Hat Enterprise Linux 7	No	Yes
FreeBSD 9	Yes	No

Remote management via ESET Remote Administrator:

ESET Remote Administrator 5.x	ESET Mail Security 3.0.x ESET Mail Security 4.0.x ESET Mail Security 4.5.x (it is not possible to set anti-spam parameters using ERA 5.x)
ESET Remote Administrator 6.x	ESET Mail Security 4.0.x (it is not possible to set anti-spam parameters using ERA 6.x) ESET Mail Security 4.5.x (recommended, fully functional)

4. Installation

After purchasing ESET Mail Security, you will receive your authorization data (Username, Password and License Key). These credentials identify you as an ESET customer, and are required to download updates for ESET Mail Security. Your license information is also required for downloading the initial installation package from ESET.com. ESET Mail Security is distributed as a binary file:

```
esets.arch.ext.bin
```

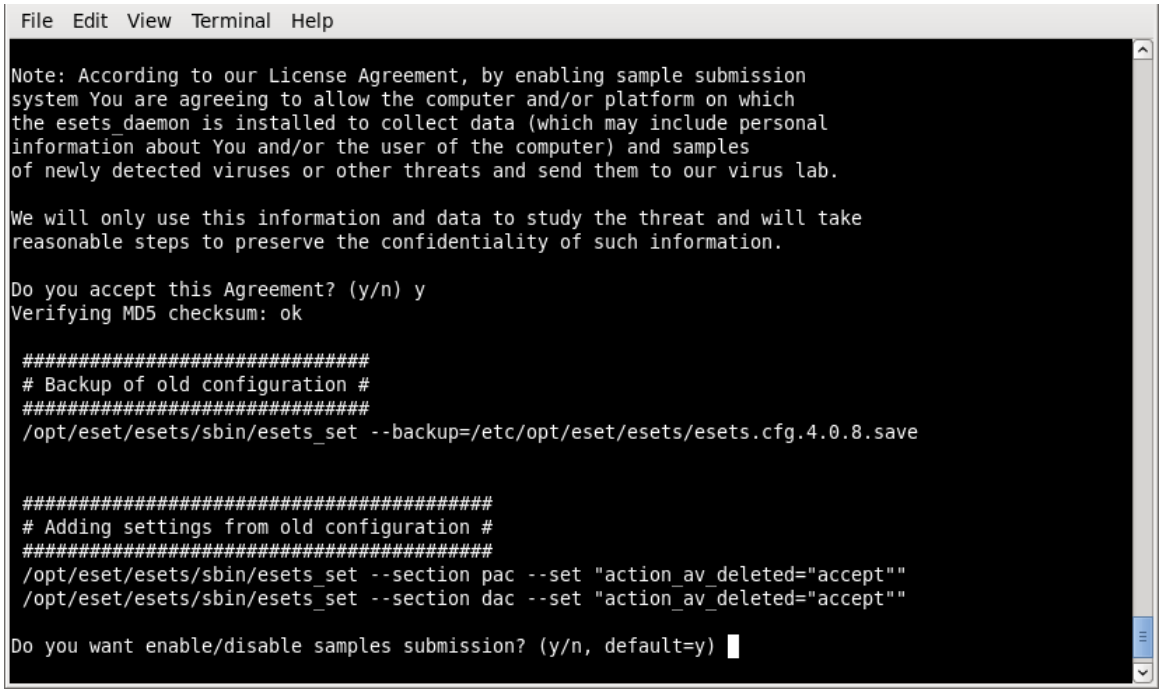
In the binary file shown above, *'ext'* is an Linux and FreeBSD OS distribution dependent suffix (for example, 'deb' for Debian, 'rpm' for RedHat, SuSE, 'tgz' for other Linux OS distributions and 'fbs9.tgz' for FreeBSD 9.x.)
The *'arch'* value represents a computer architecture, either 'i386' for 32-bit OS distributions or 'amd64', 'x86_64' for 64-bit.

To install or upgrade your product, run the ESET distribution script appropriate for the OS distribution and architecture that you have:

```
sh ./esets.i386.deb.bin
sh ./esets.i386.fbs9.tgz.bin
sh ./esets.amd64.deb.bin
sh ./esets.x86_64.rpm.bin
```

Once you accept the product License Agreement, you will be prompted to enable or disable the Samples submission system during the installation.

Figure 4-1. Installation of ESET Mail Security via Terminal.



Always import a license file before you start the ESETS daemon:

```
@SBINDIR@/esets_lic --import file.lic
```

To enable regular updates of virus signature database, enter your Username and Password into the global section of the ESET configuration file using a text editor:

```
vi @ETCDIR@/esets.cfg
```

Edit the **Update options** section of the ESETS configuration file.

```
av_update_username = "EAV-12345678"
av_update_password = "yourpassword"
```

Start the main daemon service:

Linux OS:
`/etc/init.d/esets start`
Systemd distributions:
`systemctl start esets`
	BSD OS:
	`/usr/local/etc/rc.d/esets.sh start`

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

Linux OS:	BSD OS:
`ps -C esets_daemon`	`ps -ax | 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.

To help you easily integrate ESET Security with your system, you can also use the ESET Security interactive automated install script. . A list of available ESET Mail Security installations/uninstallations according to imported licenses will be displayed.

```
@SBINDIR@/esets_setup
```

4.1 Upgrading to a more recent version

New versions of ESET Mail Security are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules.

Which product version is currently installed?

To determine the product version of ESET Mail Security, you have two options:

1. In Web interface, navigate to **Home** > **Product version**. To determine whether a new version of ESET Mail Security is available, click **Check for new version**.
2. Run an ESET command-line program with the `--version` parameter.

How to upgrade?

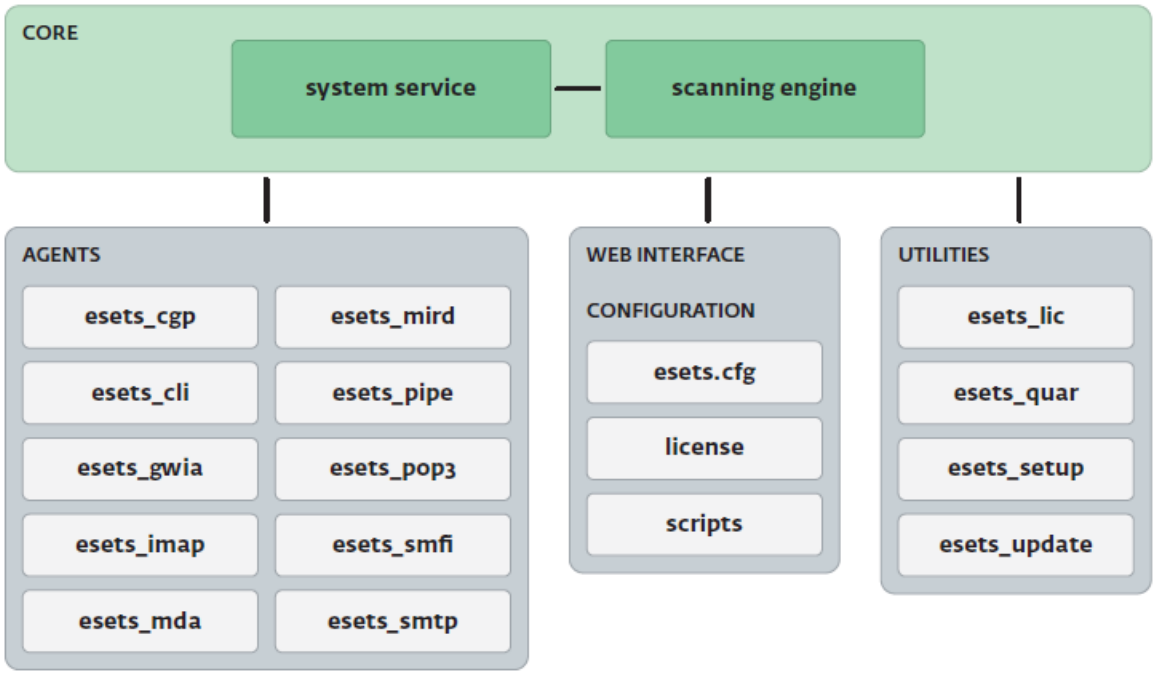
To upgrade to a more recent version, run an OS-related installation package as described in the Installation section. All parameters from the ESETS configuration file are set automatically under normal circumstances during the upgrade.

Important: ESET Mail Security 4.5.x uses a new anti-spam engine that cannot accept anti-spam settings from versions 4.0.x and earlier; attempts to merge settings will fail. We recommend that you make a backup of spamcatcher.conf and then migrate the settings into the ESETS configuration file manually.

5. 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 and FreeBSD server environment.

UTILITIES

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

CONFIGURATION

Proper configuration is the most important aspect of your 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 page.

@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.

@ETCDIR@/scripts/license_warning_script

If enabled by the Scheduler task named *Threat notification*, 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.

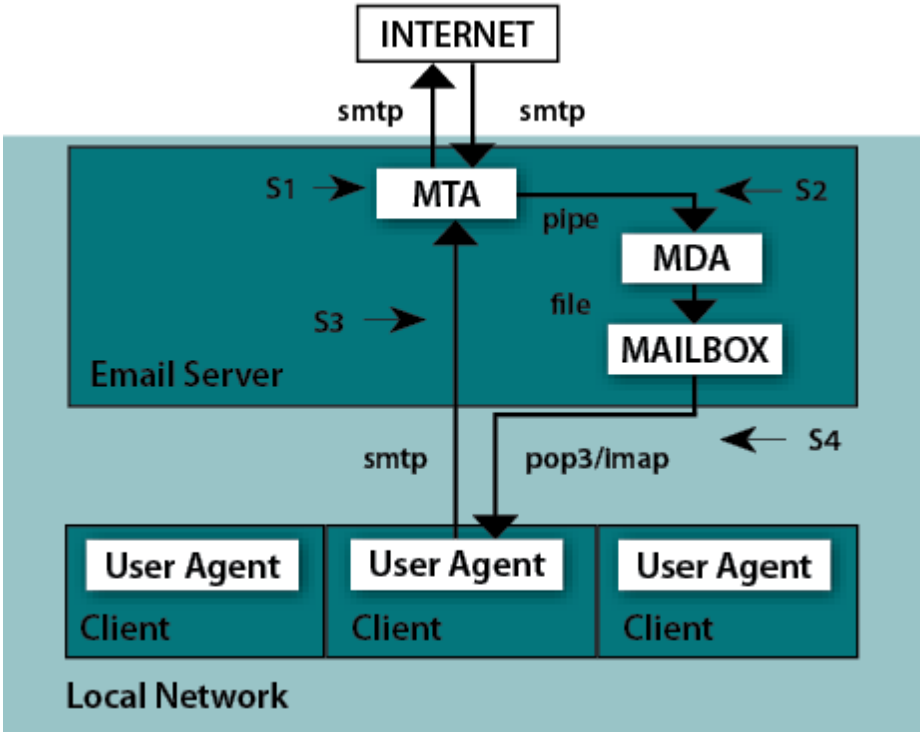
@ETCDIR@/scripts/daemon_notification_script

If enabled by the Scheduler task named *License expiration*, 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.

6. 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.

6.1 Bi-directional email message scanning in MTA

Bi-directional email message scanning mode allows the user to scan inbound and outbound email messages with 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 and GroupWise Internet Agent (GWIA).

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:

```
@SBINDIR@/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. The backup configuration files should be reimplemented after uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

6.2 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:

```
@SBINDIR@/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. The backup configuration files should be reimplemented after uninstalling. Detailed steps for all possible scenarios are described in the appendix A of this documentation.

6.3 Scanning of outbound email messages

Outbound email message scanning is performed during the 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:

```
@SBINDIR@/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. The backup configuration files should be reimplemented after uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

6.4 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 are 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 to scan email messages downloaded from POP3 or IMAP server, run the following script:

```
@SBINDIR@/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. The backup configuration files should be reimplemented after uninstalling. Detailed steps for all possible scenarios are described in appendix A of this documentation.

6.5 Alternative methods of content filtering

6.5.1 Scanning email messages in CommuniGate Pro

CommuniGate Pro is the powerful and reliable Unified Communications server and *esets_cgp* is used for content filtering (antivirus and antispam filtering).

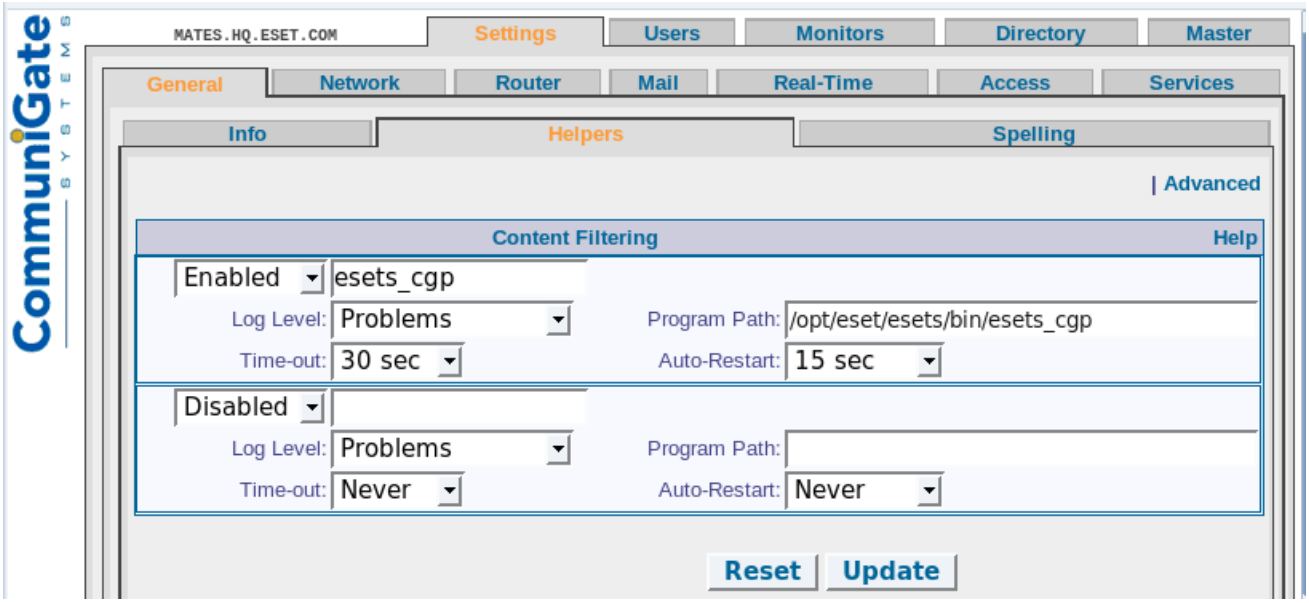
Esets_cgp only allows incoming email message scanning. *Esets_cgp* does not allow scanned email message modification and denies ESETS access to clean or delete infected email attachments. As a result, the ESETS footnote with log and status dependent header fields will not be written into the email message. Also, *esets_cgp* does not provide mail sender/recipient information. Due to this, 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.

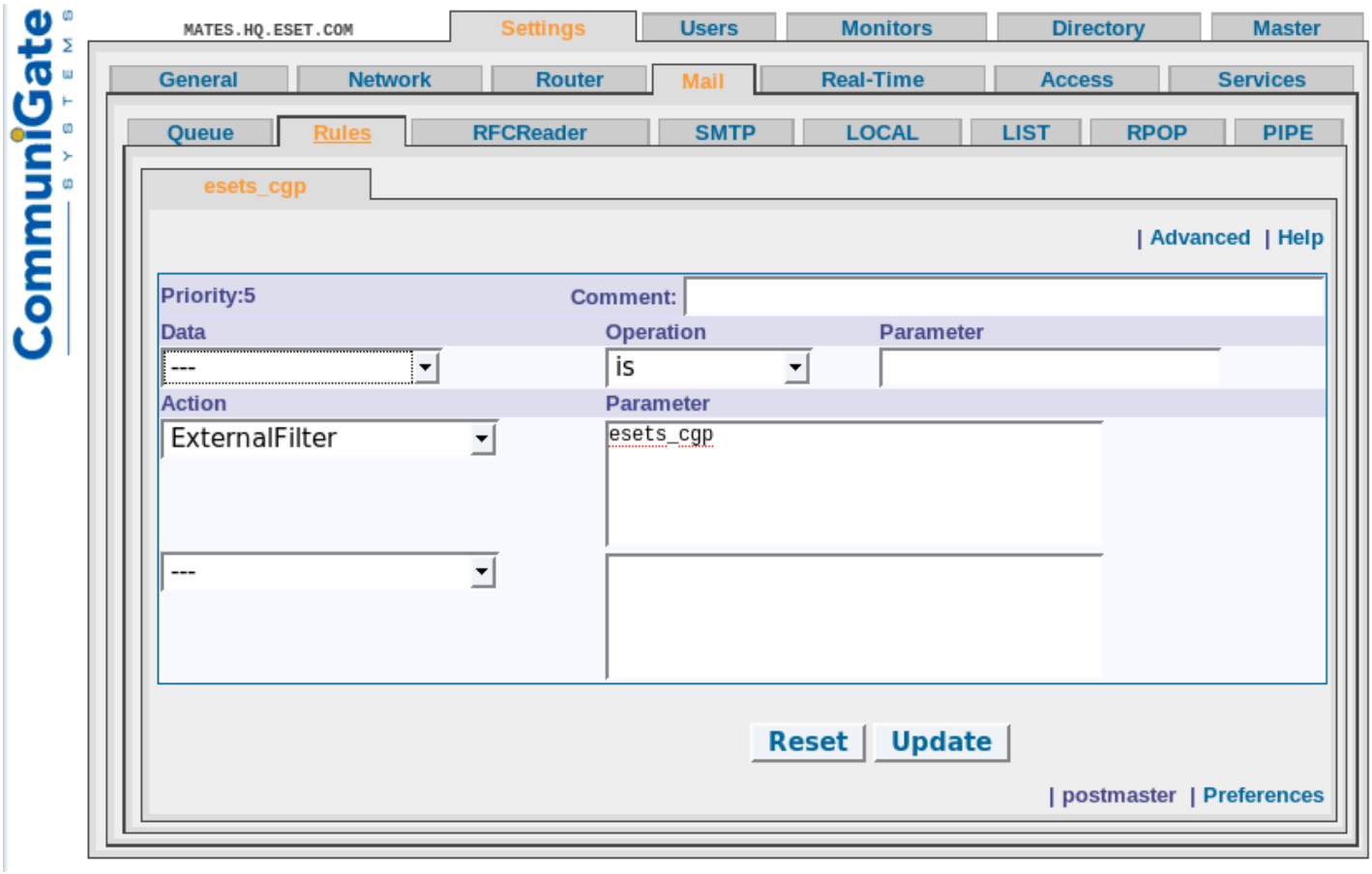
Open the **General** page in the **Settings** section of the WebAdmin Interface and click the **Helpers** link. In panel **Content Filtering** create new filter with followed values:

Figure 5-2. Setting of Content Filtering.



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.



6.5.2 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 scanned email message modification 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. Due to this, 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 antispam 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', '{}',
[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

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.

6.5.3 Scanning email messages using Novell GroupWise

Novell GroupWise is a messaging and collaborative software platform that also supports email management. The platform consists of the client and server software, available for various platforms (i.e. Linux).

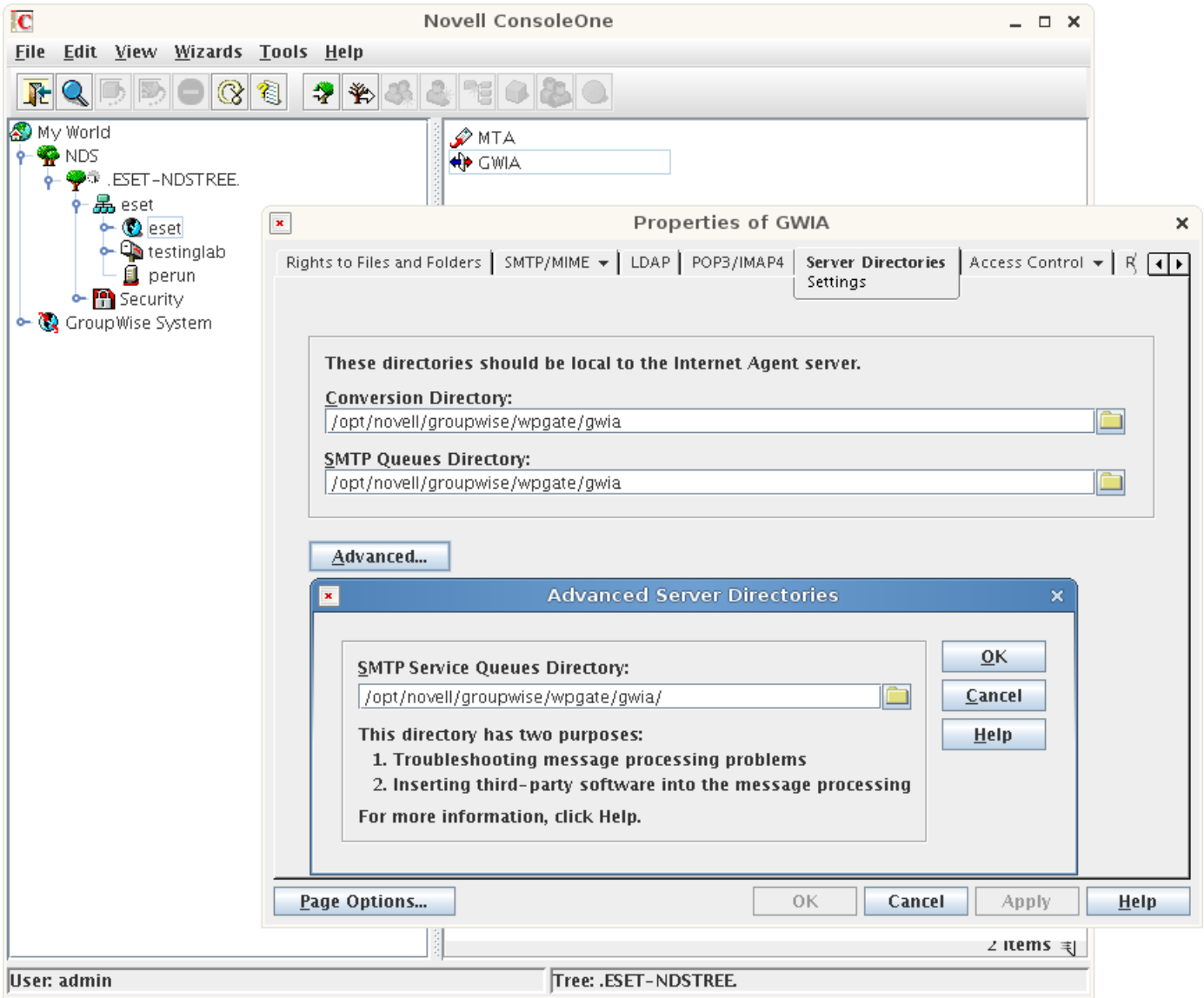
The module *esets_gwia* only allows the scanning of incoming email messages. For delivering email messages to clients immediately, the following GroupWise agent directories must have set the same paths:

- Conversion Directory
- SMTP Queues Directory
- SMTP Service Queues Directory

To perform this, open the **Novell ConsoleOne**, navigate to **NDS** > **ESET-NDSTREE** > **eset** > **domain** > **GWIA** > **Propertiers** > **Server Directories Settings** and set the particular parameters. There is an example domain called **eset** featured in our case. Then restart the GroupWise agent:

```
/etc/init.d/grpwise restart
```

Figure 5-4. Novell ConcoleOne module settings.



To configure ESET Mail Security to scan email messages downloaded from Novell GroupWise server, run the following script:

```
@SBINDIR@/esets_setup
```

Select the **MTA** install option. This will configure the GWIA (Novell GroupWise Internet Agent) and the *esets_gwia* module parameters and directories, where email queues (files) are being scanned and watched.

Note that the installer is performing a backup of all modified configuration files and can display every command that it will execute after your approval. The backup configuration files should be reimplemented after uninstalling. Detailed configuration is described in appendix A of this documentation.

7. Important ESET Mail Security mechanisms

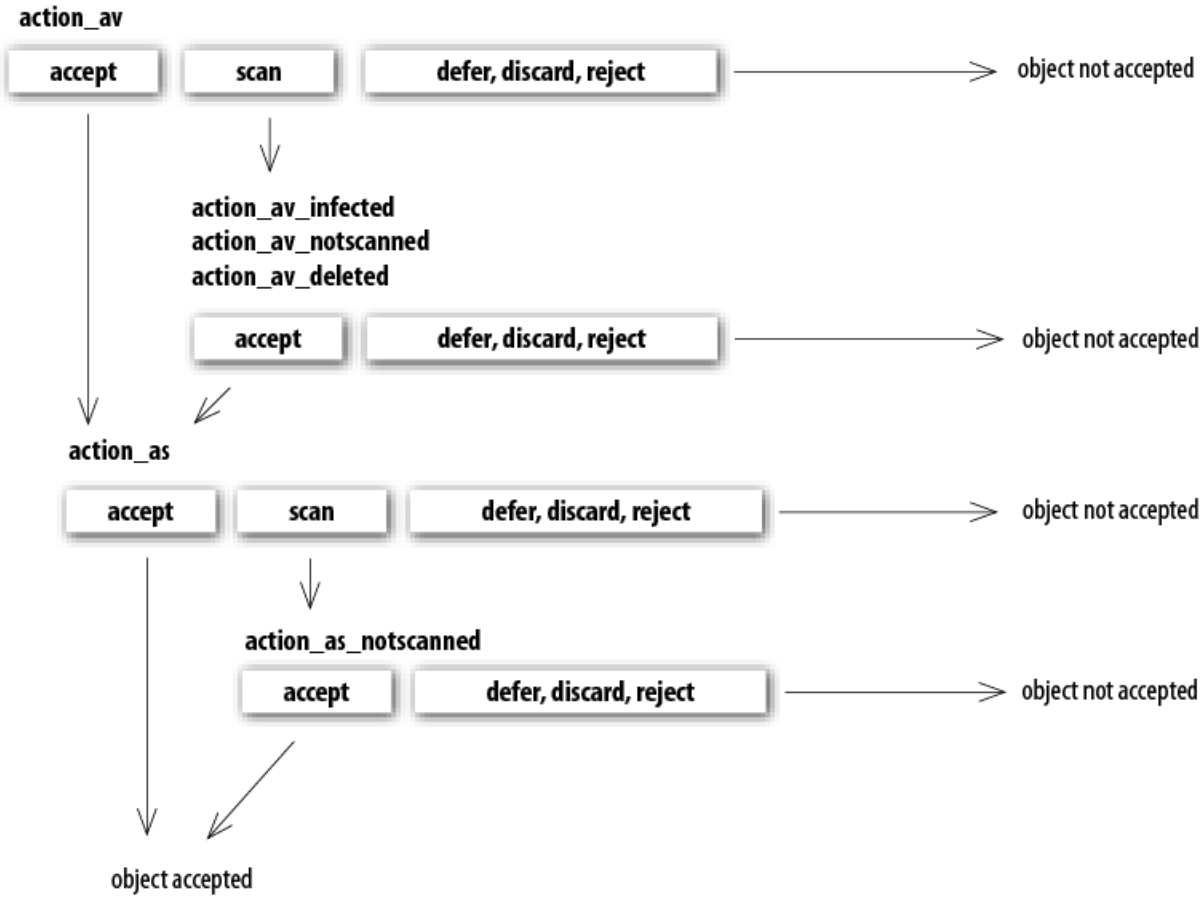
7.1 Handle Object Policy

The Handle Object Policy (see figure 6-1) mechanism provides filtering for 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 processed object 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 object handling. If an *'accept'* action has been taken as a result of these three action options, the object is accepted. Otherwise, the object is blocked.

7.2 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).

7.3 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.

7.4 Anti-Spam control

The anti-spam system filters spam messages using dynamic evaluation email data during email reception.

Important: ESET Mail Security 4.0.x and below uses a different anti-spam module than version 4.5.x and later. We strongly recommend that you upgrade to the most recent version of ESET Mail Security for the best anti-spam protection.

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 this parameter, refer to the *esets.cfg(5)* man page. Note that anti-spam scanning can only be used for email. For this reason, this functionality is only relevant for the following modules: esets_imap, esets_mda, esets_pipe, esets_pop3, esets_smtp, esets_smfi and esets_cgp.

Regular updates of the anti-spam database included in ESET Mail Security updates.

To configure anti-spam settings in ESET Mail Security:

- navigate to the **[global]** section of the ESETS configuration file, which also contains detailed description of all available parameters
  OR
- navigate to **Configuration > Global > Antispam options** of in the ESET Mail Security web interface.

We recommend that you customize the following parameters:

`as_approved_ip_list`	Several IP addresses, especially from your company, can be excluded from anti-spam scanning. This is useful to conserve system resources on the ESETS server, or eliminate false spam reports triggered by company emails. IP addresses can be specified in the following formats: IP (e.g. 1.2.3.4) IP/netmask (e.g. 1.2.3.4/8) StartingIP-EndingIP (e.g. 1.2.3.4-.1.2.3.8) Default value: empty
`as_rbl_service`	To extend analysis of email messages for spam, you can query for other anti-spam services. For example, you can query the Spamhaus server: `as_rbl_service = "zen.spamhaus.org:127.0.0.2"`
`as_message_scan_size`	Allows you to specify a document size; documents smaller than this size will not be scanned by anti-spam. We do not recommend setting this value below 100kB, as it may negatively affect classification and performance of the ESETS server. Default value: unlimited

7.5 Samples Submission System

The Samples submission system is an intelligent *ThreatSense.Net* technology that collects infected objects that 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 the 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 other users of the computer) and samples of newly detected viruses or other threats and send them to ESET virus laboratory. This feature is disabled 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 enable sampling, the samples submission system cache must be initialized. This can be achieved by selecting *'samples_enabled'* in the **[global]** section of the ESETS configuration file.

For more information on the Samples Submission System and its options, please refer to the *esets_daemon(8)* mane page.

7.6 Scheduler

The Scheduler's functionality includes running scheduled tasks at a specified time or on a specific event, managing and launching tasks with predefined configuration and properties and more. Task configuration and properties can be used to influence launch dates and times, but also to expand the application of tasks by introducing the use of custom profiles during task execution.

The *'scheduler_tasks'* option is commented by default, causing the default scheduler configuration to be applied. In the ESETS configuration file all parameters and tasks are semicolon-separated. Any other semicolons (and backslashes) must be backslash escaped. Each task has 6 parameters and the syntax is as follows:

- id – Unique number.
- name – Task description.
- flags – Special flags to disable the specified scheduler task can be set here.
- failstart – Instructs what to do if task could not be run on scheduled date.
- datespec – A regular date specification with 6 (crontab like year-extended) fields, recurrent date or an event name option.
- command – Can be an absolute path to a command followed by its arguments or a special command name with the '@' prefix (e.g. anti-virus update: *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

The following event names can be used in place of the datespec option:

- start – Daemon startup.
- startonce – Daemon startup but at most once a day.
- engine – Successful engine update.
- login – Web interface logon startup.
- threat – Threat detected.
- notscanned – Not scanned email or file.
- licexp – 30 days before license expiration.

To display the current scheduler configuration, use the Web interface or run the following command:

```
cat @ETCDIR@/esets.cfg | grep scheduler_tasks
```

For a full description of Scheduler and its parameters refer to the Scheduler section of the *esets_daemon(8)* man page.

7.7 Web Interface

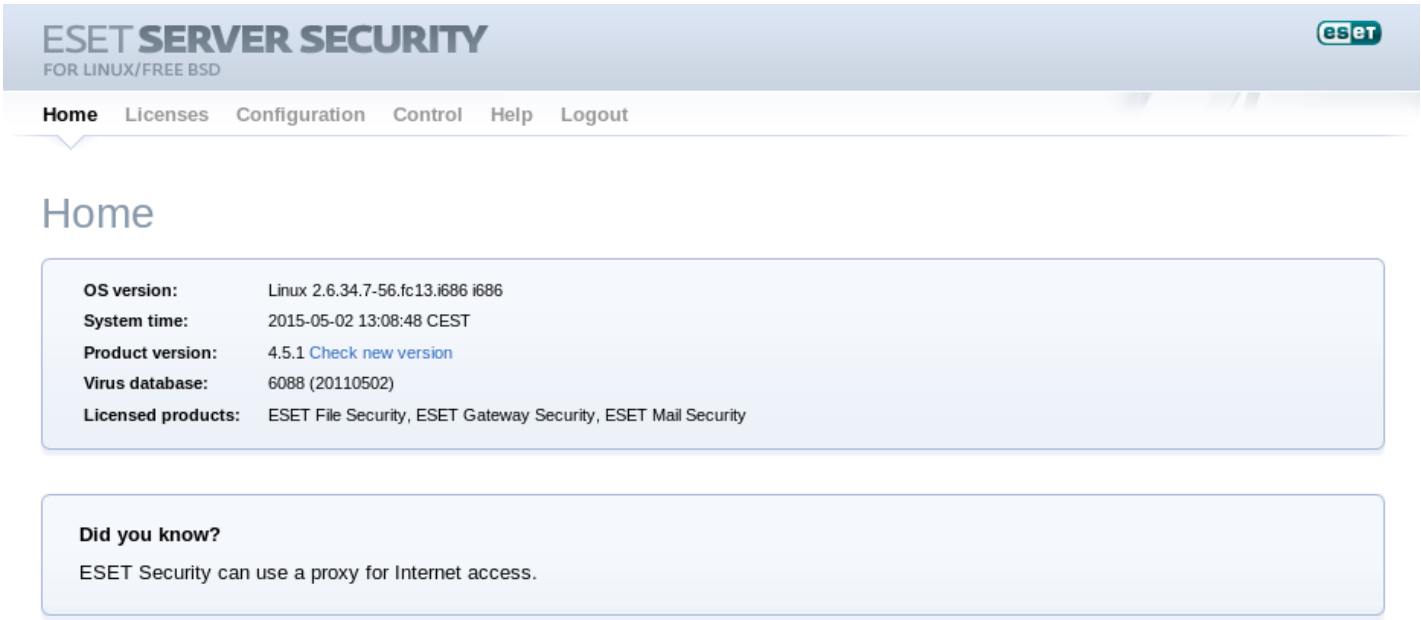
The web interface allows user-friendly configuration, administration and license management of ESET Security systems. This module is a standalone component and must be enabled before it can be accessed. To quickly configure the web interface, configure the following options in the ESETS configuration file as shown below 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 in the **Help** section of the web interface and technical details about *esets_wwwi* can be found in 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, which displays the contents of the selected menu option, and the main menu. A horizontal bar on the top lets you navigate between the following main options:

- **Home** – provides basic system and ESET product information
- **Licenses** – a license management utility, see the following chapter for mode 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

Important: Make sure you click **Save changes** after making any changes in the **Configuration** section of the web interface to save your new settings. To apply your settings, restart the ESETS daemon by clicking **Apply changes** on the left pane.

We recommend that you limit access to this interface for a specific range of IP addresses. This can be done two ways:

1. By adding only one interface under the `listen_addr` parameter (not using 0.0.0.0)
2. Using a firewall rule (such as *iptables*).

7.7.1 License management

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

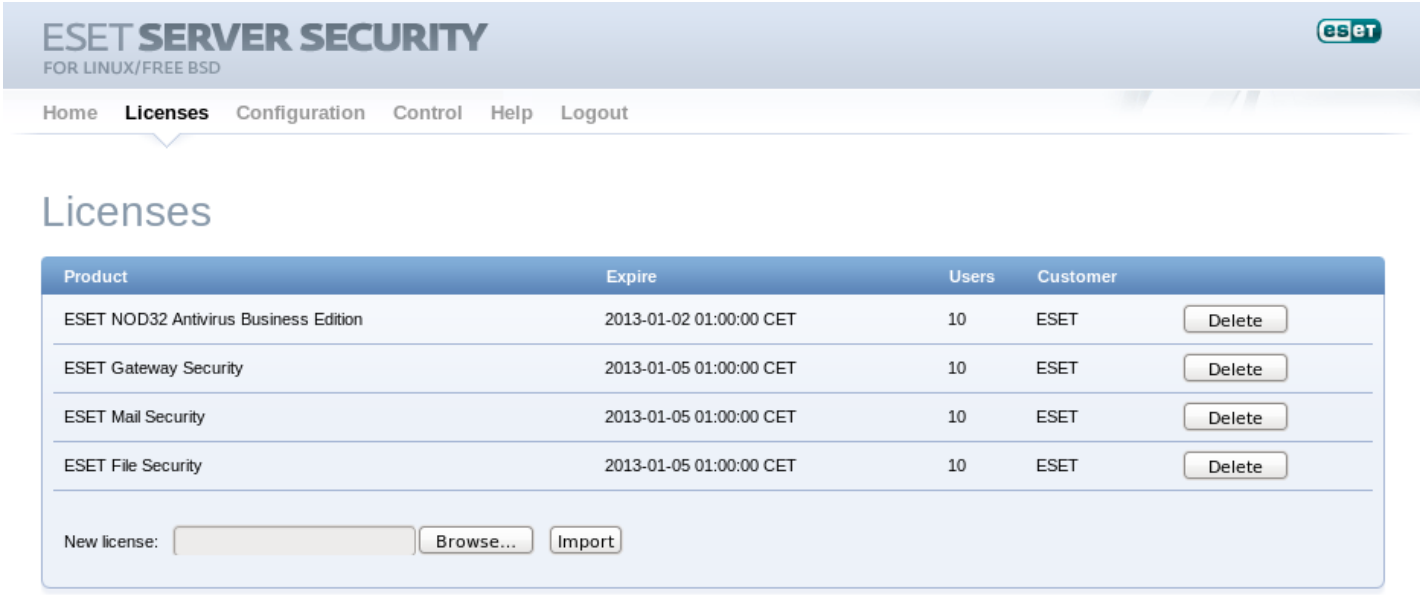
If you want to display licenses in the console, use the following command:

```
@SBINDIR@/esets_lic --list
```

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

```
@SBINDIR@/esets_lic --import *.lic
```

Figure 6-2. ESET Licenses.



You can enable the license notification option in the Scheduler 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 and FreeBSD 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.

7.7.2 SMTP+Postfix configuration example

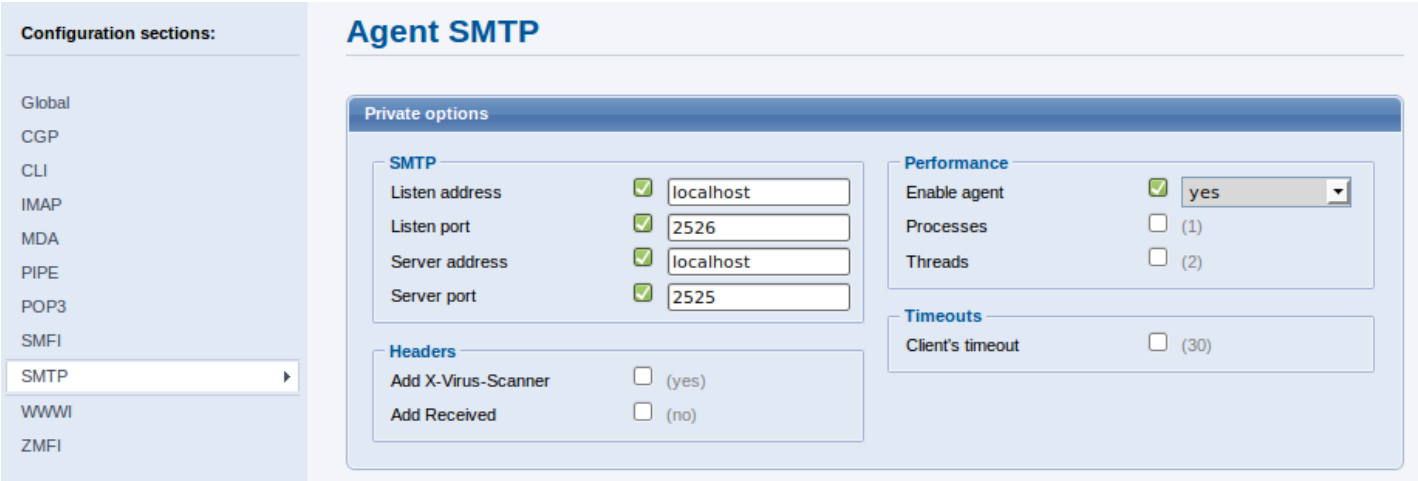
ESETS can be configured in two ways. In this example, we will demonstrate how to use both when configuring the SMTP module, leaving you the choice of your preferred configuration method:

- 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.

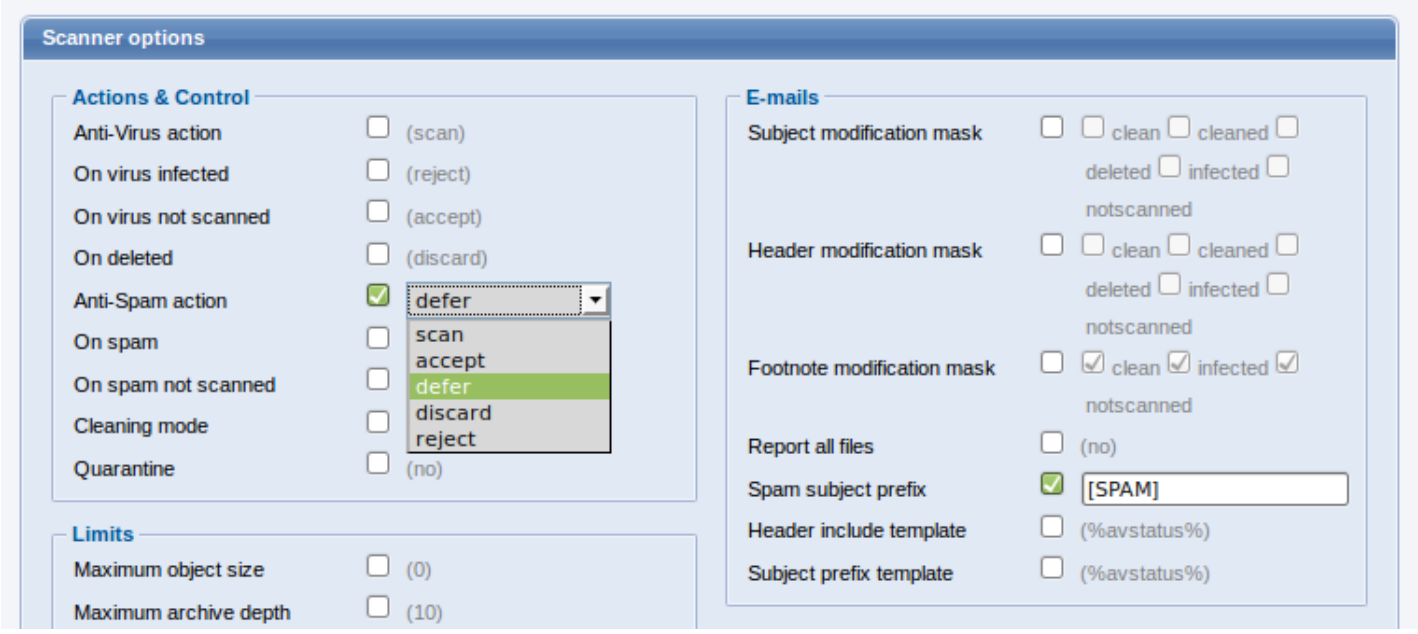


Always remember to save your new configuration by clicking **Save changes**. To apply your new changes, click the **Apply changes** button in the **Configuration sections** panel.

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]"
```

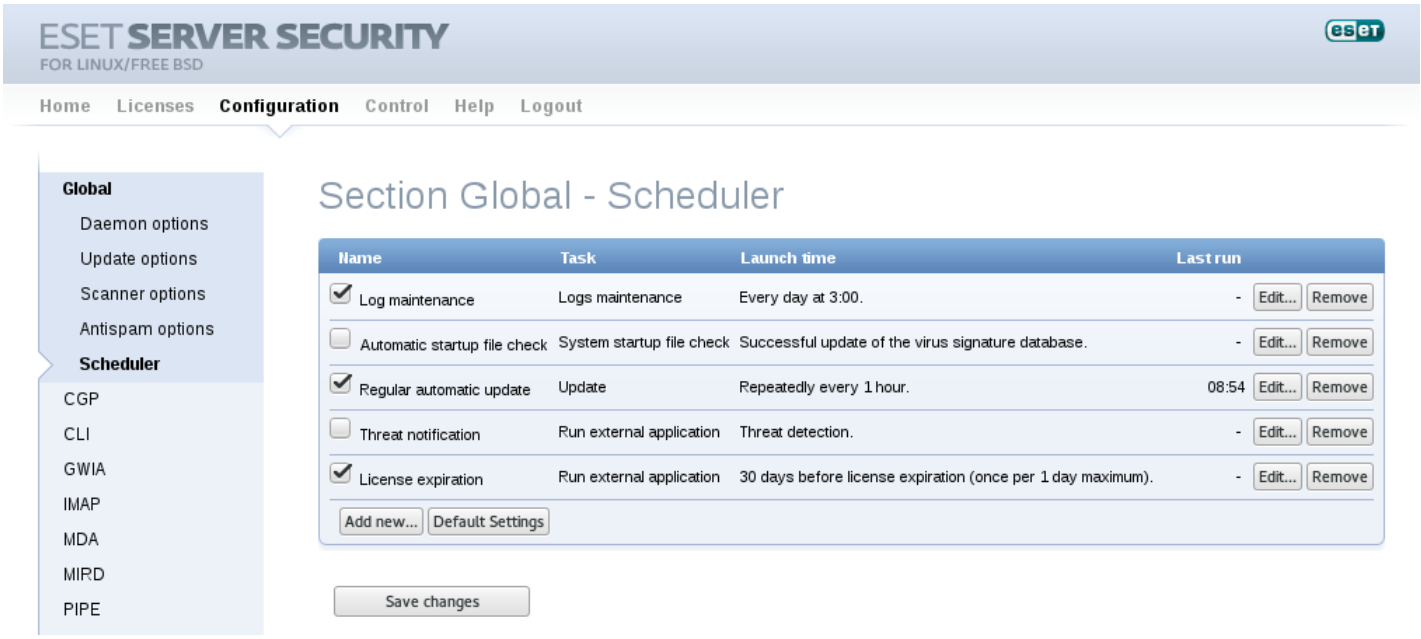
Figure 6-4. SMTP Scanner options.



7.7.3 Scheduler

You can manage the scheduler tasks either via ESET configuration file (see chapter Scheduler) or using the web interface.

Figure 6-5. ESETS - Global > Scheduler.



Click the checkbox to enable/disable a scheduled task. By default, the following scheduled tasks are displayed:

Log maintenance – The program automatically deletes older logs in order to save hard disk space. The Scheduler will start defragmenting logs. All empty log entries will be removed during this process. This will improve the speed when working with logs. The improvement will be more noticeable if the logs contain a large number of entries.

Automatic startup file check – Scans memory and running services after a successful update of the virus signature database.

Regular automatic update – Regularly updating ESET Mail Security's virus signature database and antispam modules is the best method of keeping the maximum level of security on your computer. See ESETS update utility for more information.

Threat notification – By default, each threat will be logged into syslog. In addition, ESETS can be configured to run an external (notification) script to notify a system administrator via email about threat detection.

License expiration – If enabled, this functionality will notify you 30 days prior to your license expiration. This task will run the *@ETCDIR@/scripts/license_warning_script* shell script, which sends an email to the email address of the root user account. The script can be customized to reflect specific server needs.

7.7.4 Statistics

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

Figure 6-6. ESETS - Control > Statistics.



7.8 Remote Administration

ESETS supports remote administration for server security management in large computer networks. The ESETS Remote Administration Client (RACL) 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 Remote Administrator policies and configuration tasks
- Can perform *Update Now* tasks
- Performs computer scans as requested, and submits the results back to the 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 logs
- Sends all non-debug messages to event logs

These functionalities are not supported:

- Firewall logging
- Remote installation

For more specific information, please read the ESET Remote Administrator manual or visit our Online help.

7.8.1 Connecting with ESET Remote Administrator

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

- Running ERA Server
- Running ERA Console
- Installed and running ERA Agent (ESET Remote Administrator version 6.x and higher)
- 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).

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

7.8.2 ESET Remote Administrator usage example (6.x)

Installing ERA Agent

ERA Agent must be installed to allow communication with the ERA Server. ESET Mail Security communicates with the ERA Agent through the *localhost* connection, and then ERA Agent relays information to ESET Remote Administrator via Internet or LAN.

Username/Password data is not required to download the ERA Agent installation package from ESET.com.

- To install ERA Agent please refer to:
  Agent installation - Linux (ESET Remote Administrator 6.x manual)

Enabling RACL

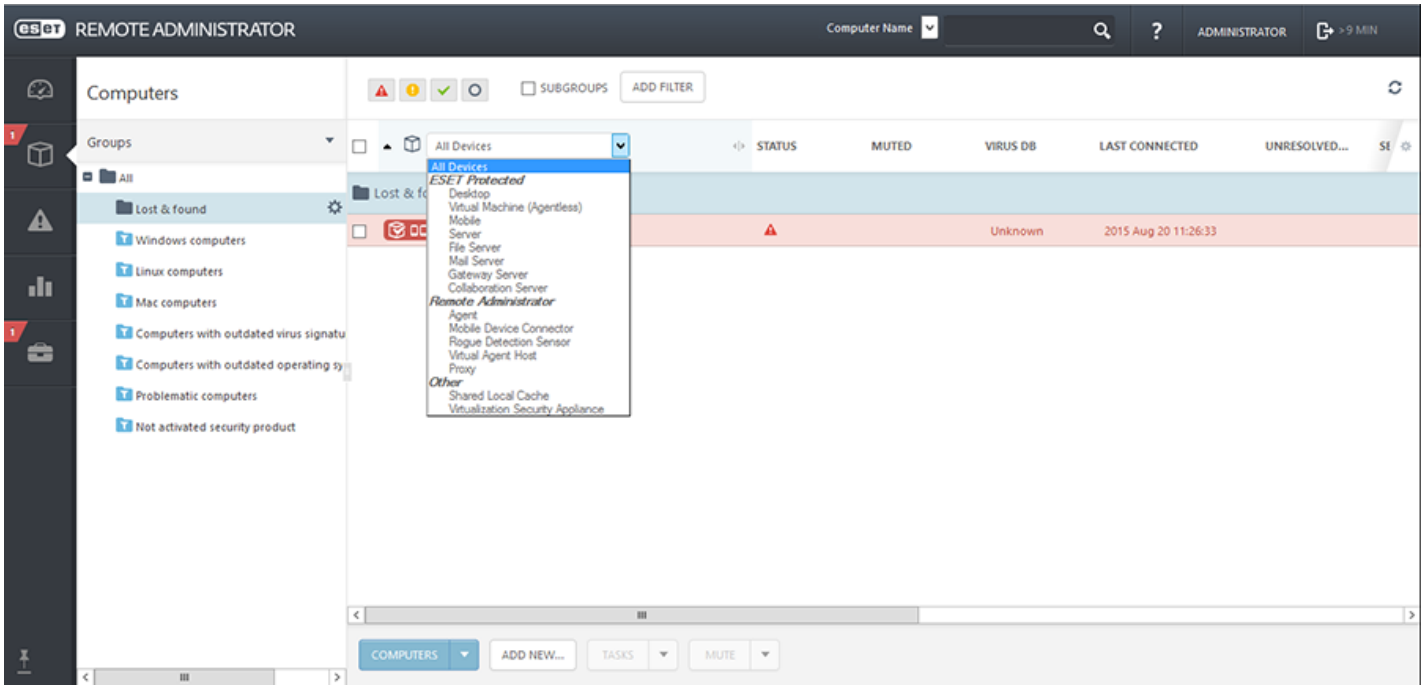
You can either use the web interface (see the previous chapter) to apply the new configuration, or you can adjust these parameters in the **[global]** section of the ESETS configuration file as follows:

```
racl_server_addr = "localhost"
racl_server_port = 2225
racl_password = "yourPassword"
racl_interval = 1
```

ERA Web Console

After the ESETS daemon configuration is be reloaded, ERA Agent is installed, and RACL can connect to ERA Server (or ERA Proxy) through ERA Agent, you should see a newly connected client in the **Computers** > **Lost & found** section of the ERA Web Console.

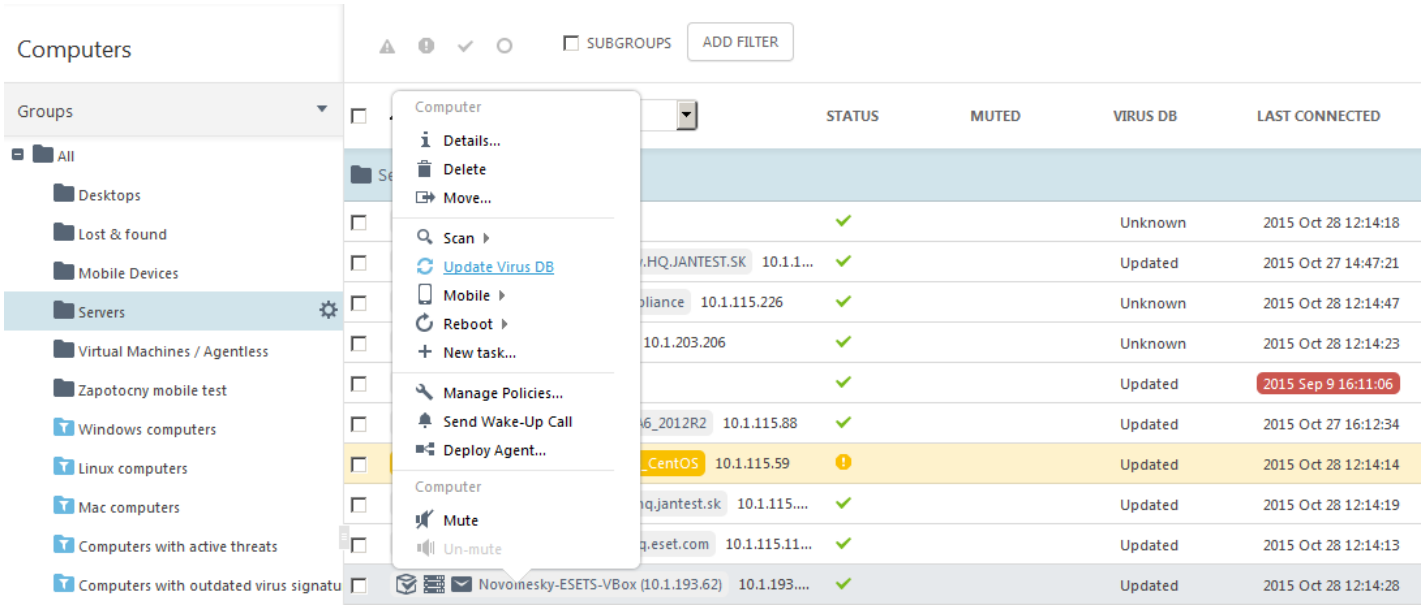
Figure 6-7. ERA Web Console.



Using the Web Console, you can create a client task to ESETS daemon by:

- Clicking the connected client.
- Selecting a task from **Admin** > **Client tasks**, for example **Update virus DB**.

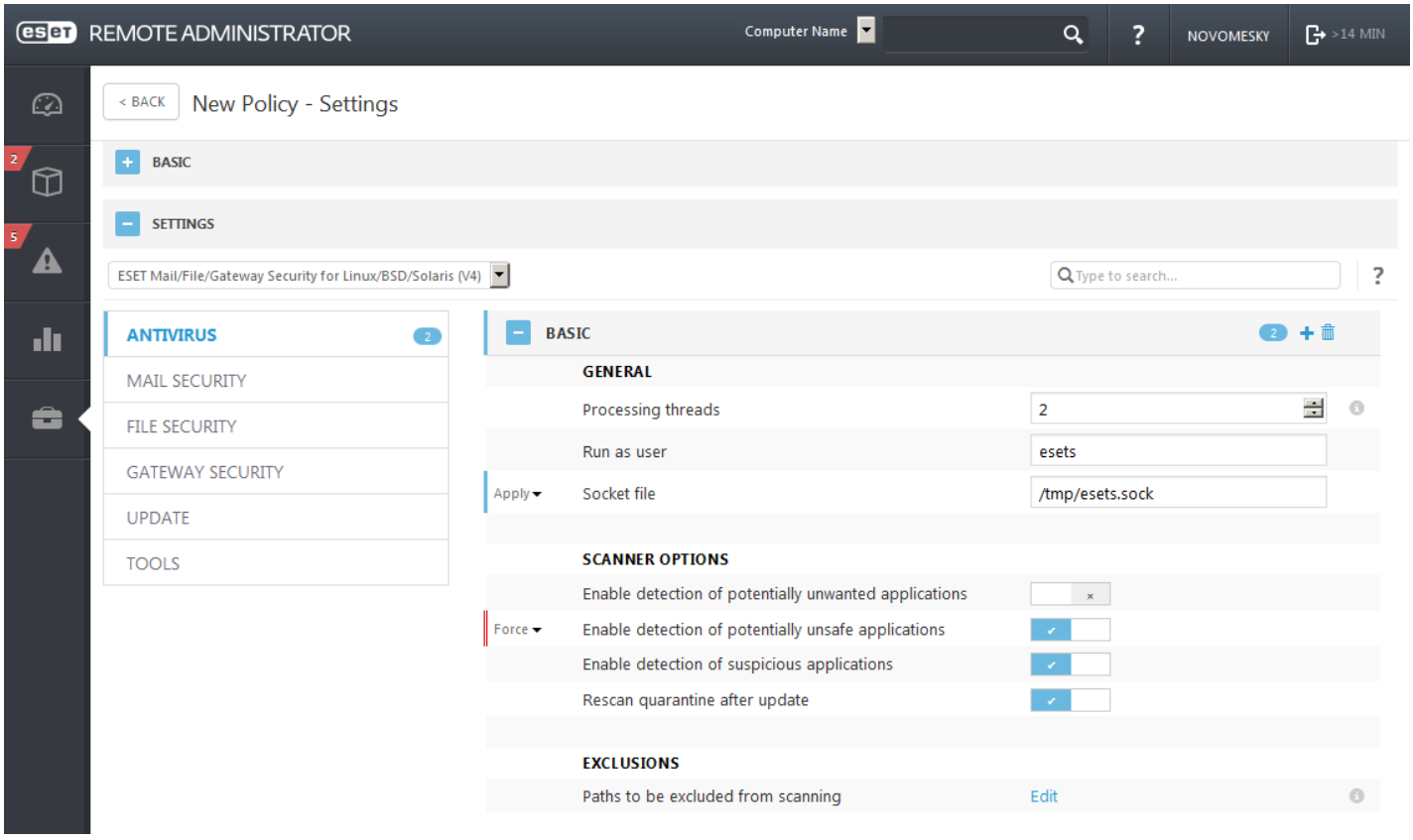
Figure 6-8. ERA Client task from ERA Web Console.



An ERA policy can be used to push and enforce specific configurations to ESET Mail Security. For example, you can enforce detection of potentially unsafe applications so that it cannot be overridden locally on ESET Mail Security. To do so,

1. From the ERA Web Console navigate to **Admin** > **Policies** > **New**
2. In the **Settings** section select **ESET Mail/File/Gateway Security for Linux (V4)**
3. Under **Antivirus,** select the check box next to **Enable detection of potentially unsafe applications** and select the check box next to **Force**
4. Select your ESET Mail Security server as the policy target and click **Finish**.

Figure 6-9. Enforcing a policy in ERA Web Console.



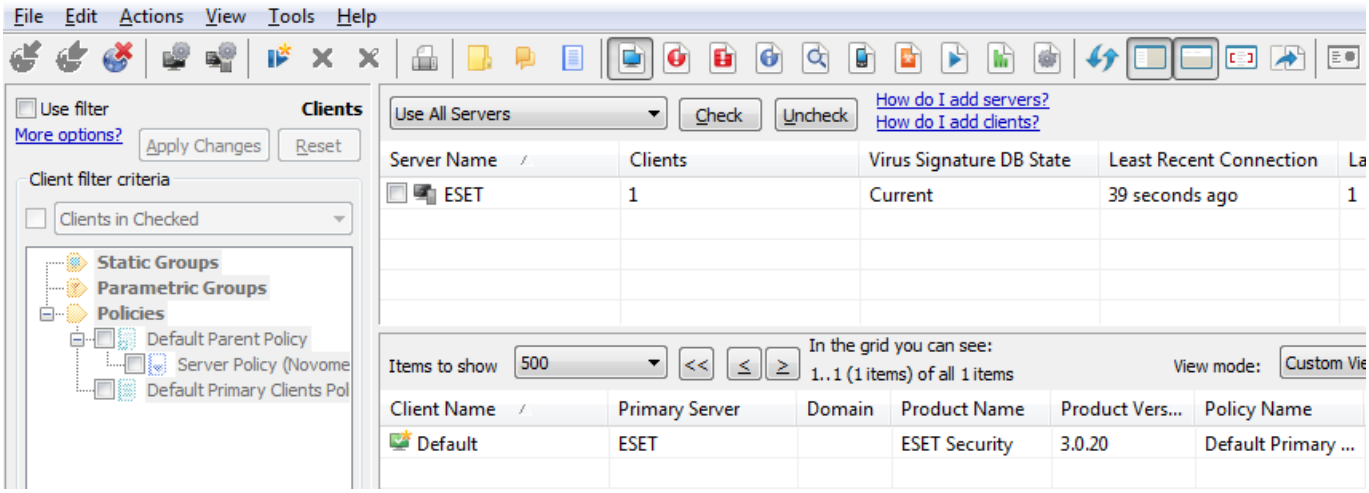
7.8.3 ESET Remote Administrator usage example (5.x)

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 = "your_ERA5_Server_IP_Address_or_Hostname"
racl_server_port = 2222
racl_password = "yourPassword"
racl_interval = 1
```

After 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 6-10. ERA Console.

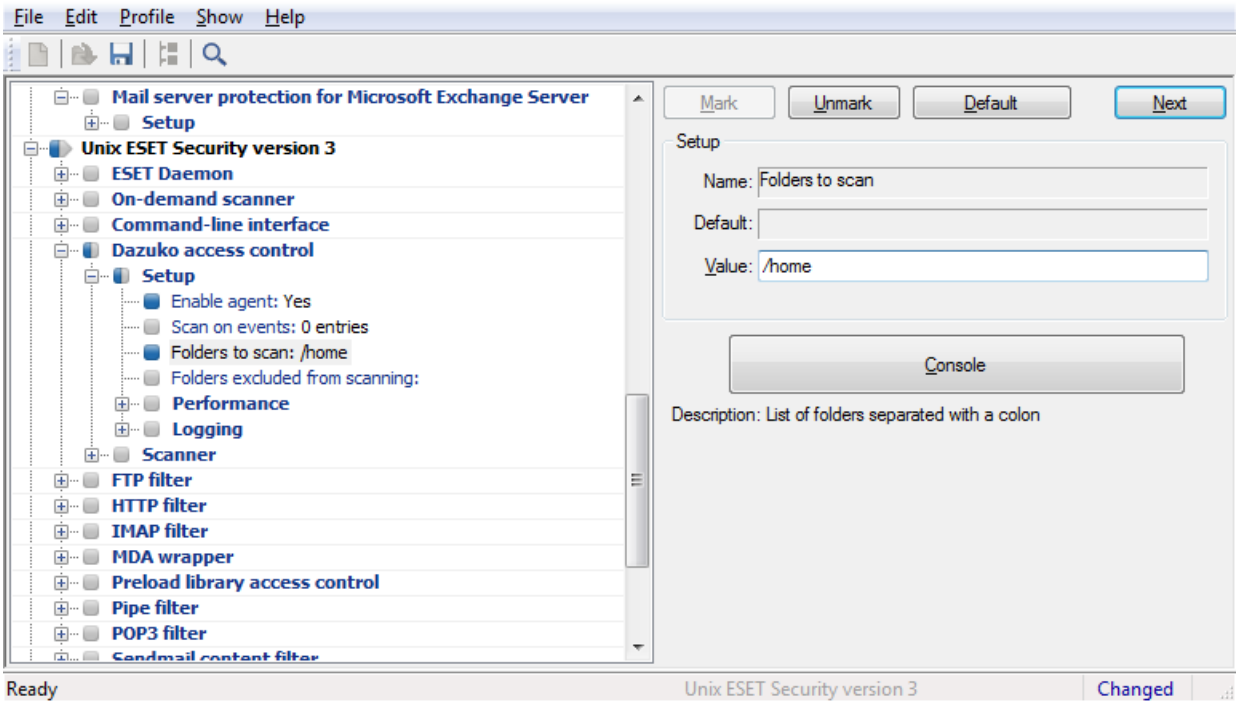


By using ERA Console you can create a configuration task to ESETS daemon from ERA Console:

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

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

Figure 6-11. ERA Configuration Editor.

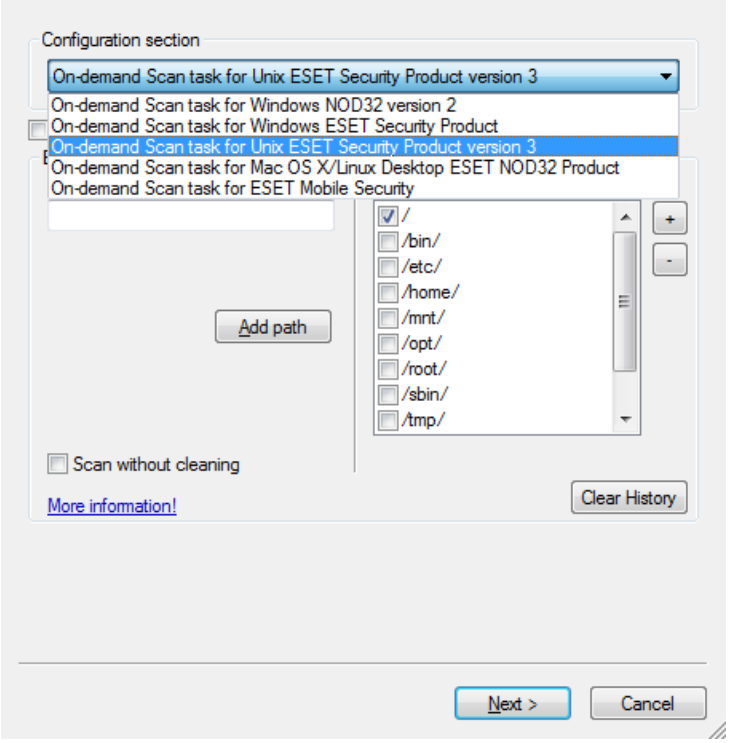


The **New Task** context menu contains On-demand scanning options (enabled/disabled cleaning).

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 6-12. ERA On-demand scan.



7.9 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 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 esets | less
```

Systemd uses a different logging approach. To display activity run one of the following command:

```
journalctl --since today
journalctl | grep esets | less
```

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

7.10 Command-line programs

ESETS commands can be launched using the command line – manually (@SBINDIR@/esets_*) or with a batch (".sh") script. ESETS command-line usage:

esets_daemon	ESET Security Daemon is the main ESET'S system control and scanning Daemon module. It reads all the ESET'S scanner configuration from the main ESET'S configuration file and provides all the main tasks. Usage: `@SBINDIR@/esets_daemon [OPTIONS..]`
esets_inst	ESET system integrator can be used to display and optionally execute commands that integrate ESET'S with your system. This module features installation for mta, pop3, imap and smtp. Usage: `@SBINDIR@/esets_inst [OPTIONS..] [COMMAND]`
esets_lic	ESET'S license management utility features management options, which allow you to display information about your licenses, import license files to the license directory or remove expired licenses. Usage: `@SBINDIR@/esets_lic [OPTIONS..] [COMMAND] [FILES..]`
esets_quar	ESET'S quarantine management utility module allows you to import any file system object into the quarantine storage area. Usage: `@SBINDIR@/esets_quar ACTIONS [RULES] [OBJECTS..]`
esets_scan	ESET Command-line scanner is an on-demand anti-virus scanning module, which provides scanning of the file system objects upon user request using command line interface. Usage: `@SBINDIR@/esets_scan [OPTIONS..] FILES..`
esets_set	ESETS configuration file SET-up utility allows you to modify the ESET'S configuration file as requested by given command. Usage: `@SBINDIR@/esets_set [OPTIONS..] [COMMAND]`
esets_setup	ESET'S setup utility is an interactive automated install script to help you easily integrate ESET Security with your system. Usage: `@SBINDIR@/esets_setup [OPTIONS..] [COMMAND]`
esets_update	ESET'S update utility is a system utility for the creation, update and maintenance of the ESET'S modules storage mirrors as well as for update of ESET'S system. Usage: `@BINDIR@/esets_update [OPTIONS..]`

The following commands are available only for ESET Mail Security.

esets_cgp	External filter plug-in for CommuniGate Pro, which reads e-mail filenames from standard input, requests esets_daemon to scan it and responds with status. Usage: `@BINDIR@/esets_cgp [OPTIONS..]`
esets_cli	ESET'S Command Line Interface module, the role of which is to scan all file system objects that are defined as a command line argument(s). Usage: `@BINDIR@/esets_cli [OPTIONS..] FILES..`
esets_mda	ESET'S Mail Delivery Agent wrapper module, the role of whichis to receive e-mail, request esets_daemon to scan it, and forward the scanned e-mail to the original MDA, since this module is not a full-featured MDA.
esets_pipe	A simple e-mail scanner, which reads the mail from stdin, requests eset_daemon to scan it and if accepted, writes it scanned to standard output. Usage: `@BINDIR@/esets_pipe [OPTIONS..]`
esets_zmfi	ZMailer's contentfilter, which scans e-mail filenames read from stdin, requests esets_daemon to scan it and responds with the status. Usage: `@BINDIR@/esets_zmfi [OPTIONS..]`

8. ESET Security system update

8.1 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 specifically 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 and FreeBSD 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 be able to specify the frequency of updates, you need to configure the *'@update'* task in the *'scheduler_tasks'* option in the **[global]** section of the ESETS configuration file. You can also use the Scheduler to set the update frequency. The ESETS daemon must be up and running in order to successfully update the virus signature database.

8.2 ESETS update process description

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

@BASEDIR@/mirror

'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: To enable the mirror and download PCUs for ESET NOD32 Antivirus, ESET Smart Security, ESET Endpoint Antivirus or ESET Endpoint Security, you have to:

- set your Username and Password for update purposes (as described in the topic above),
- import a license for your specific ESET product.

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.

8.3 ESETS mirror http daemon

The http mirror daemon in ESET Mail Security allows you to create copies of update files which can be used to update other workstations located in the network. Creation of the "mirror" – a copy of the update files in the LAN environment is convenient, since the update files need not be downloaded from the vendor update server repeatedly and by each workstation. They are downloaded centrally to the local mirror server and then distributed to all workstations, therefore avoiding the potential risk of network traffic overload. This is also a typical feature of ESET Remote Administrator.

The http mirror daemon needs to be properly configured to start and enable the mirror. In the example below *esets_mird* is configured to listen on port 2221 of a computer with the local network IP address 192.168.1.10. The following parameters in the **[mird]** section of the ESETS configuration file need to be specified:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 2221
```

Options *'listen_port'* and *'listen_addr'* define the port (default 2221) and address (default: all local tcp addresses) where the http server listens. If you set the value of the *'auth_mode'* switch from 'none' to 'basic', the mirror will require authentication. The options *'username'* and *'password'* allow the administrator to define the login and password required to access the Mirror.

9. Let us know

We hope this guide has provided you with a thorough understanding of the requirements for ESET Mail Security installation, configuration and maintenance. It is our goal to continually improve the quality and effectiveness of our documentation.

For additional assistance with your ESET product, please visit our online Knowledgebase at the following URL:

- http://support.eset.com

If you feel that any sections in this guide are unclear or incomplete or you are unable to resolve your issue, please let us know by using the support form directly:

- http://www.eset.com/int/support/contact

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

10. Appendix A. ESETS setup and configuration

10.1 Setting ESETS $PATH environment variable

To access ESETS command-line programs without typing a full @BINDIR@ or @SBINDIR@ path, you can export the *$PATH* variable directly from a Unix command line using the following command:

```
export PATH=$PATH:/opt/eset/esets/bin:/opt/eset/esets/sbin
```

After performing this command, typing a full path to ESETS command-line programs is not be required:

Before:	After:
`/opt/eset/esets/bin/esets_update`	`esets_update`

Note that this command will be active only for a current shell session. You have to save this command to the *~/.bashrc* file, or somewhere to */etc*, depending on a type of a Unix operating system you use.

10.2 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
```

10.3 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) 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.

10.4 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).

10.5 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
```

10.6 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
```

10.7 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.

10.8 Setting ESETS for MTA Novell GroupWise

ESETS GroupWise Internet Agent contentfilter module scanning is performed using the *esets_gwia* daemon. The ESETS configuration file In the **[gwia]** section should look like this:

```
agent_enabled = yes
gwia_smtphome = "/var/spool/gwia/esets"
gwia_dhome = "/var/spool/gwia/queues"
```

Note: According to the Handle Object Policy, configuration options in **[gwia]** section such as *'action_av', 'action_av_infected', 'action_as'* and their actions *'defer'* and *'reject'* will be changed to *'discard'*. These events will be logged into syslog.

Ensure that these parameters were set using *esets_setup* installer in *gwia.cfg* (located in */opt/novell/groupwise/agents/share/*) configuration file:

```
--home /opt/novell/groupwise/wpgate/gwia
--dhome /var/spool/gwia/queues
--smtphome /var/spool/gwia/esets
```

10.9 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
```

'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
```

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.

10.10 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
```

10.11 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
```

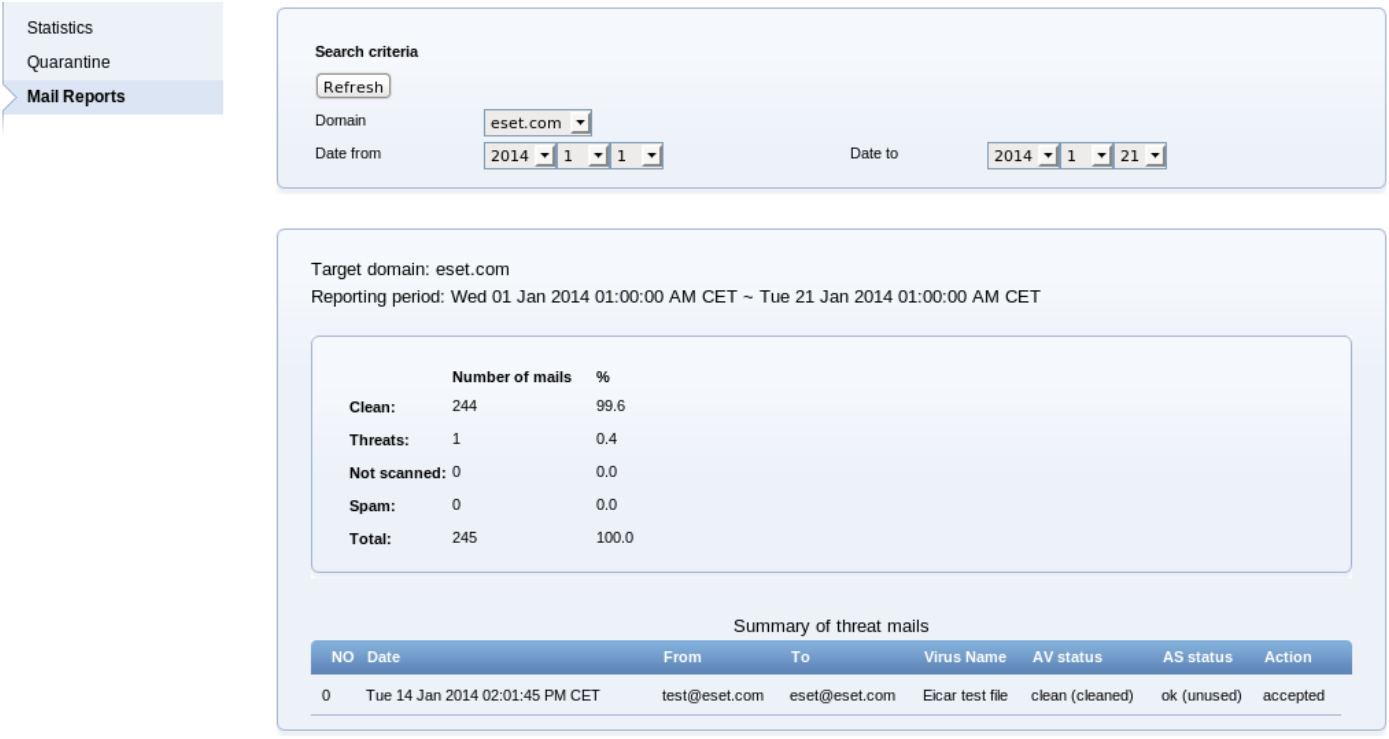
10.12 Setting ESETS to enable Mail reporting functionality

Important: This feature is available in ESETS 4.0.21 and later.

The reporting function of mail statistics can be enabled using the *'report_enabled'* and *'report_domains'* options in the ESETS configuration file.

Reporting options in Web interface can be found in **Configuration** > **Global** > **Daemon options** > **Reports**.
Reports generated for a specified domain can be found in **Control** > **Mail reports** and can be filtered by a domain or date. A sample generated report is displayed in the image below.

Figure 8-1. Example of a generated report for domain eset.com.



Important information

- There is no report displayed in the **Mail Reports** section of the Web interface by default. A report will be displayed when all search criteria are matched.
- The reporting period is displayed in UTC time standard.
- Reports can be created for e-mails older than 1 day. Same-day reporting is not available.
- Add a *'.com'* domain to the 'report_domains' option of the ESETS configuration file if you want to create reports from all .com domains.

Report files are stored in:
`@CACHEDIR@/reports/`

Reports lifetime affects the **Log maintenance** scheduler task, which is responsible for cleaning up reporting data as well.

10.13 Setting ESETS to send email notifications on virus detection

Important: This feature is available in ESETS 4.0.21 and later.

Notification email of virus detection can be enabled using the 'av_mail_notified_users' option in the **[global]** section of the ESETS configuration file. Threat notifications are not handled by Scheduler.

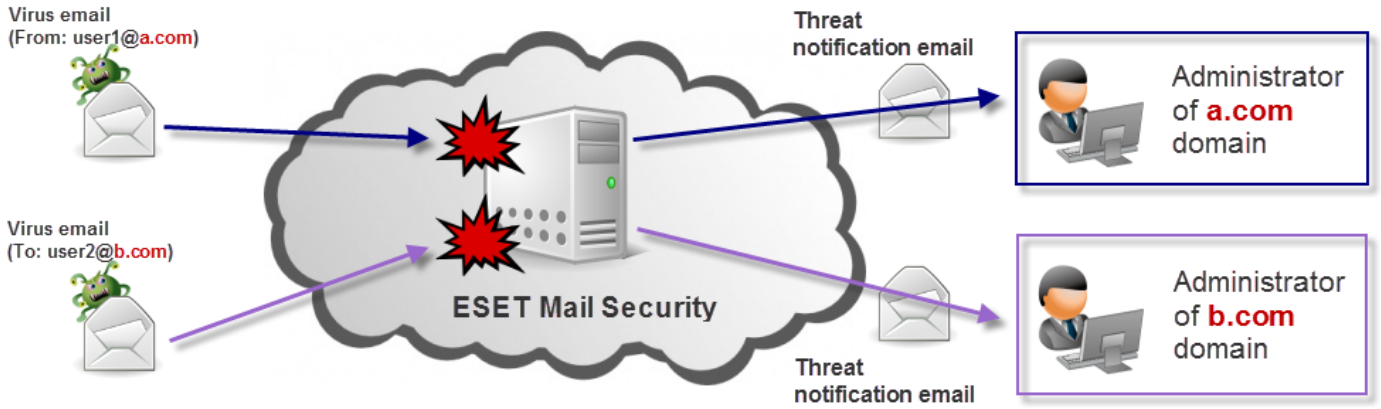
For more information please refer to the *esets_daemon(8)* man page.

Important: The mail notification script is located in:
`@ETCDIR@/scripts/mail_notification_script`

Use the following syntax to simulate a scenario, if a.com is specified in the sender address or recipient address of a detected virus mail, ESETS sends threat notifications to the administrator of the a.com domain (the same for b.com):

```
av_mail_notified_users = "a.com:admin@a.com:b.com:admin@b.com"
```

Figure 8-2. Two domains, two domain administrators.



11. Appendix B. PHP License

The PHP License, version 3.01 Copyright (c) 1999 - 2010 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.
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. 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.