ESET MAIL SECURITY

Installation Manual and User Guide

(intended for product version 4.0 and higher)

Linux, BSD and Solaris

Click here to download the most recent version of this document

ESET **MAIL SECURITY**

Worldwide Customer Support: www.eset.com/support

REV. 6/16/2015

Contents

1. Introduction

Thank you for using ESET Mail Security - the premier security system for Linux, BSD and Solaris. 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, BSD and Solaris.

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.

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.

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.

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, BSD and Solaris 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
NetBSD: /var/lib/esets
Solaris: /var/opt/esets/lib
```

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
NetBSD: /var/cache/esets
Solaris: /var/opt/esets/cache
```

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
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 (depending on the operating system) is listed below:

```
Linux: /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 (depending on the operating system) is listed below:

```
Linux: /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 (depending on the operating system) is listed below:

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

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 Linux distributions (x86/x64) are officially supported:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise

ESET Mail Security will also run on the following operating systems (but only x86, 32-bit):

- NetBSD 4
- FreeBSD 6.x, 7.x, 8.x and 9.x
- SUN Solaris 10

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. The Username/ Password data 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
```

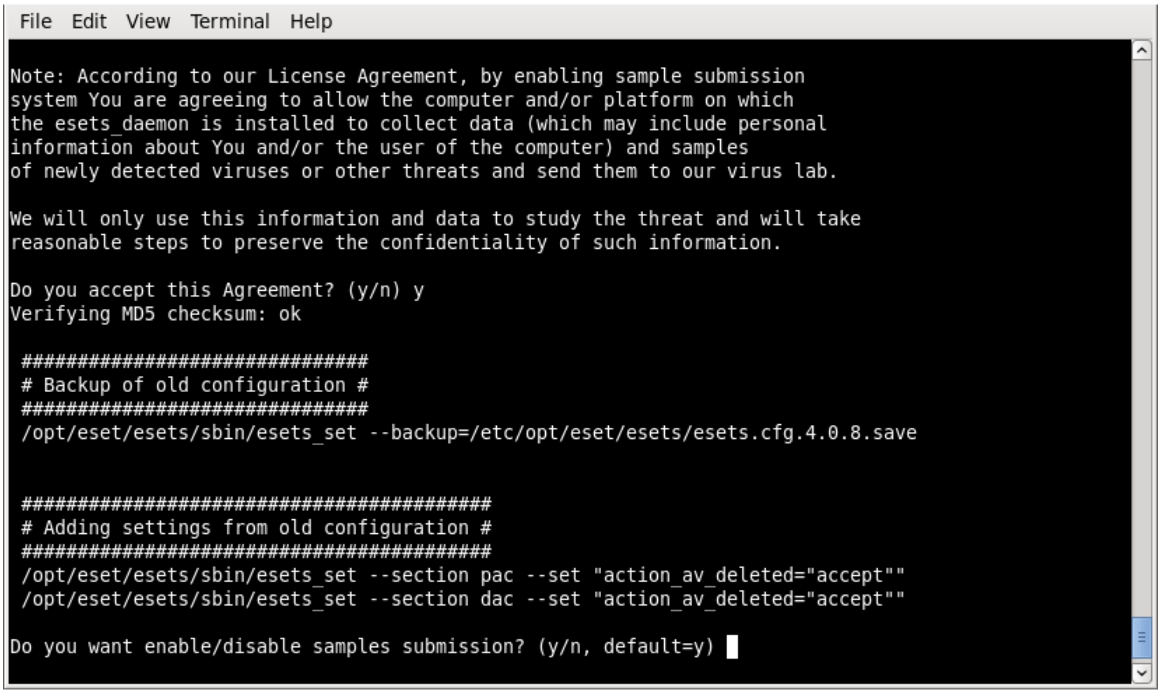
In the binary file shown above, *'ext'* is a Linux, BSD and Solaris OS distribution dependent suffix, i.e., 'deb' for Debian, 'rpm' for RedHat and SuSE, 'tgz' for other Linux OS distributions, 'fbs7.tgz' for FreeBSD 7.x, 'fbs8.tgz' for FreeBSD 8.x, 'nbs4.tgz' for NetBSD 4.xx and 'sol10.pkg.gz' for Solaris 10.
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.fbs8.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.



```
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.

We will only use this information and data to study the threat and will take
reasonable steps to preserve the confidentiality of such information.

Do you accept this Agreement? (y/n) y
Verifying MD5 checksum: ok

 ################################
 # Backup of old configuration #
 ################################
 /opt/eset/esets/sbin/esets_set --backup=/etc/opt/eset/esets/esets.cfg.4.0.8.save


 ############################################
 # Adding settings from old configuration #
 ############################################
 /opt/eset/esets/sbin/esets_set --section pac --set "action_av_deleted="accept""
 /opt/eset/esets/sbin/esets_set --section dac --set "action_av_deleted="accept""

Do you want enable/disable samples submission? (y/n, default=y)
```

An installation package *esets-version.arch.ext* will be created and placed in the current working directory. Information regarding the installation, uninstallation or upgrade will be displayed onscreen.
To complete the installation or upgrade of your product, run the newly created *esets-version.arch.ext* file using the appropriate syntax for your OS distribution:

Linux OS:

```
dpkg -i esets-4.0.x.i386.deb
rpm -U esets-4.0.x.i386.rpm
```

BSD OS:

```
pkg_add esets-4.0.x.i386.fbs8.tgz
```

Solaris:

```
gunzip esets-4.0.x.i386.sol10.pkg.gz
pkgadd -d esets-4.0.x.i386.sol10.pkg
```

Note: The procedure with an installation package *esets-version.arch.ext* is available only for versions 4.0.8 and below. Enabling or disabling the Samples submission system is available from version 4.0.10.

Import the license files:

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

Enter your Username and Password information into the global section of the ESET configuration file using a text editor:

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

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

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

Start main daemon service:

Linux OS:

```
/etc/init.d/esets start
```

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:

```
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.

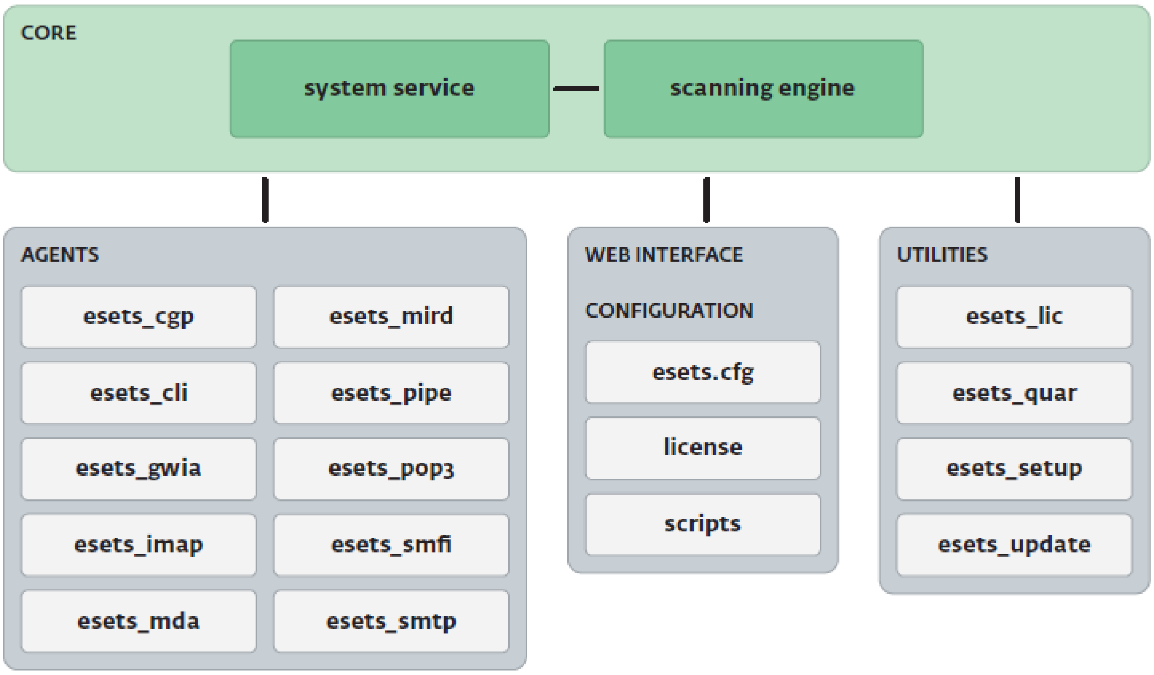
To help you easily integrate ESET Security with your system, you can also use the ESET Security interactive automated install script. You can undo all changes later. A list of available ESETS installations/uninstallations according to imported licenses will be displayed.

```
@SBINDIR@/esets_setup
```

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, BSD and Solaris 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.

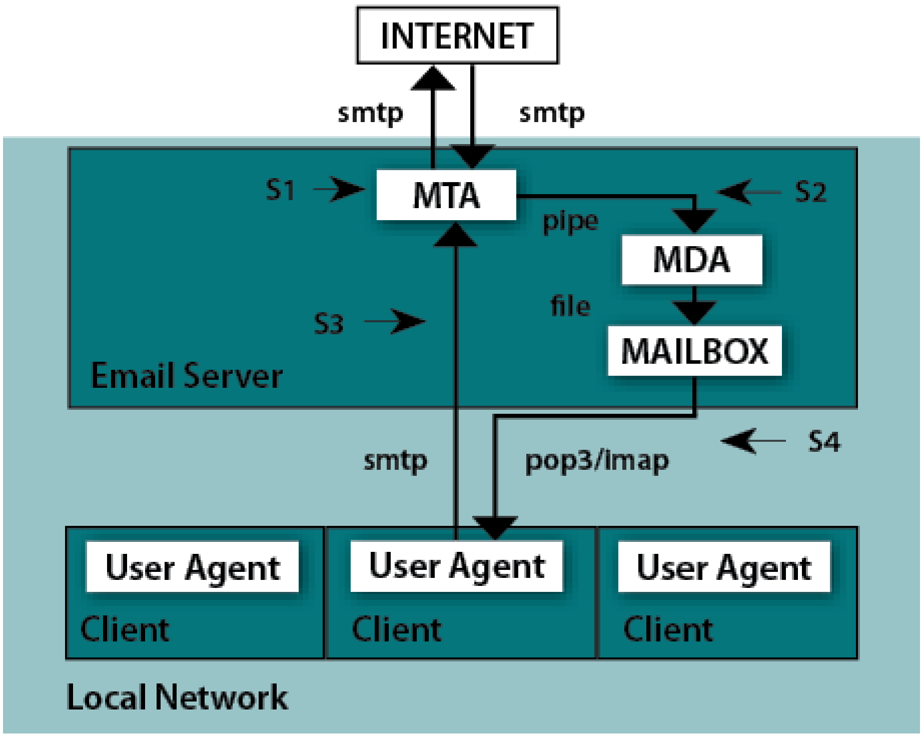
@ETCDIR@/scripts/daemon_notification_script

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).

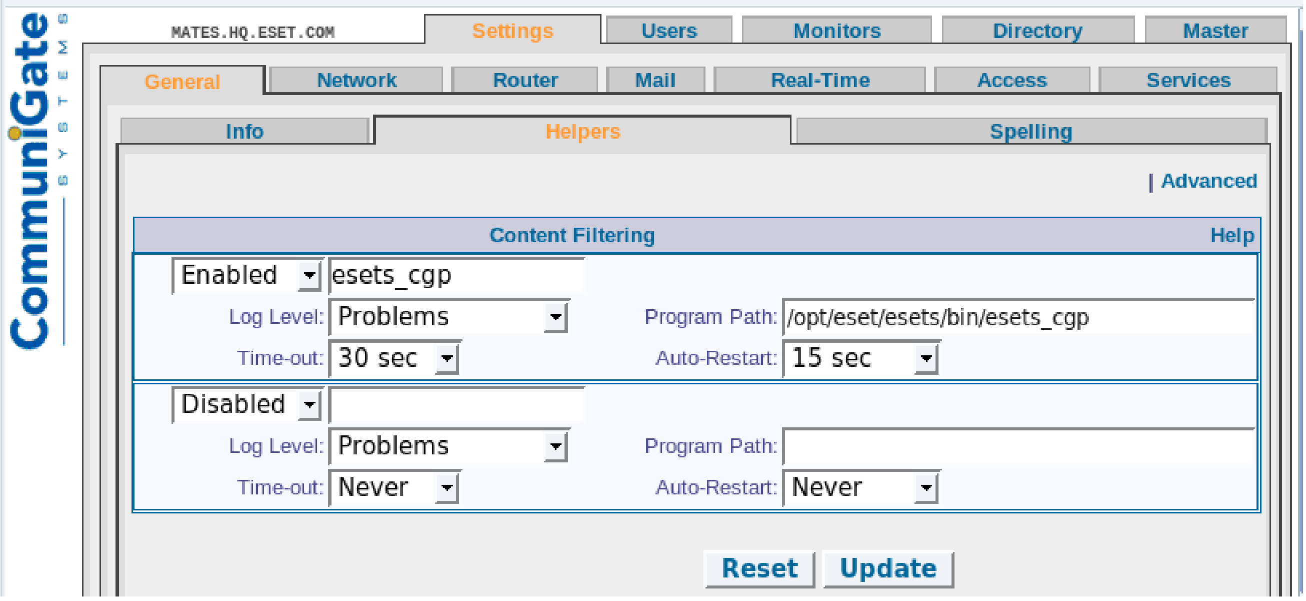
Esets_cgp only allows incoming email message scanning. *Esets_cgp* does not allow scanned email message modification and denies ESETS access to clean or delete infected email attachments. As a result, the ESETS footnote with log and status dependent header fields will not be written into the email message.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



Enabled esets_cgp

Log Level: Problems Program Path: /opt/eset/esets/bin/esets_cgp

Time-out: 30 sec Auto-Restart: 15 sec

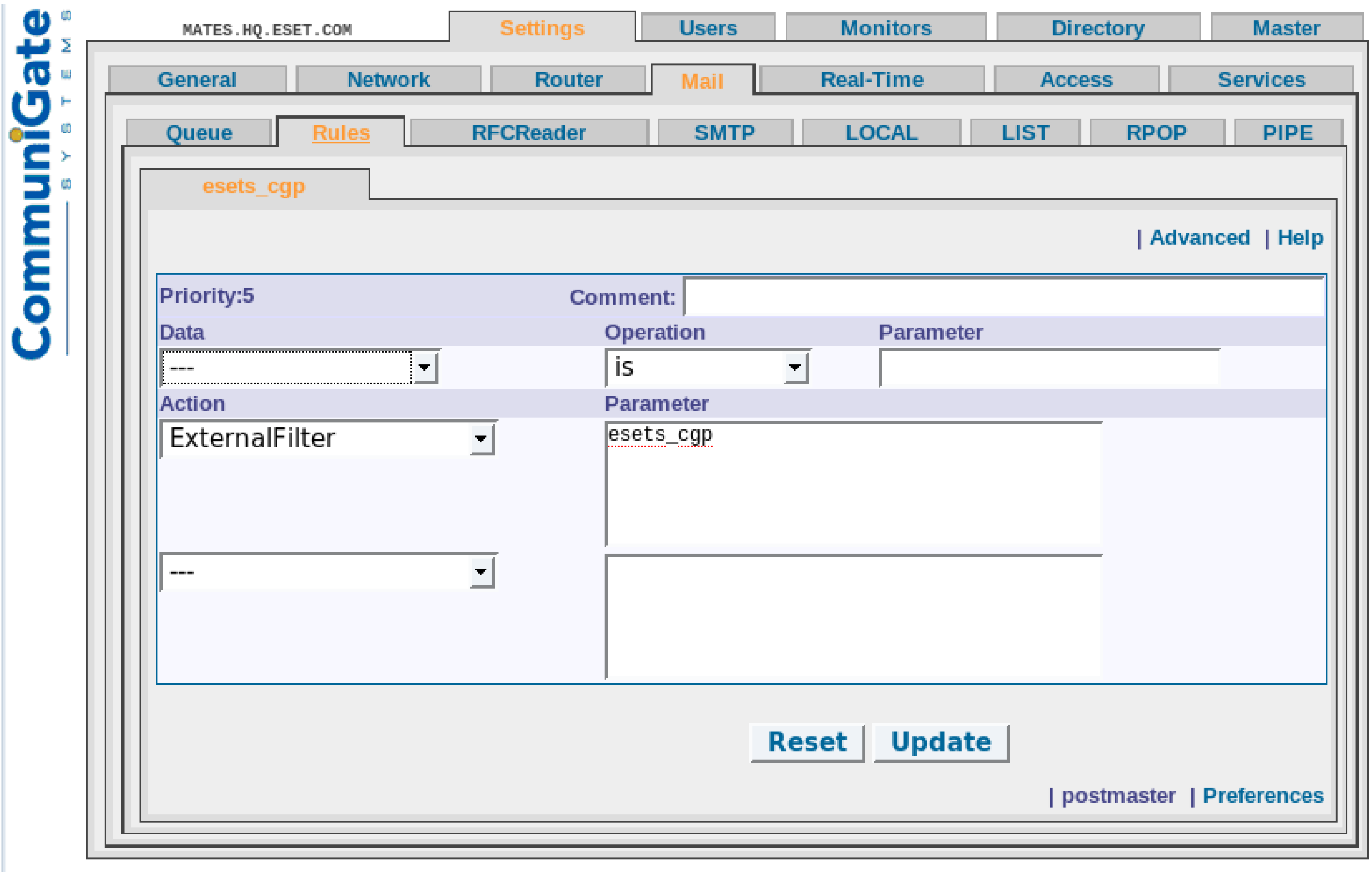
Disabled

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.



Priority:5

Comment:

Data	Operation	Parameter
---	is	

Action	Parameter
ExternalFilter	esets_cgp

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).

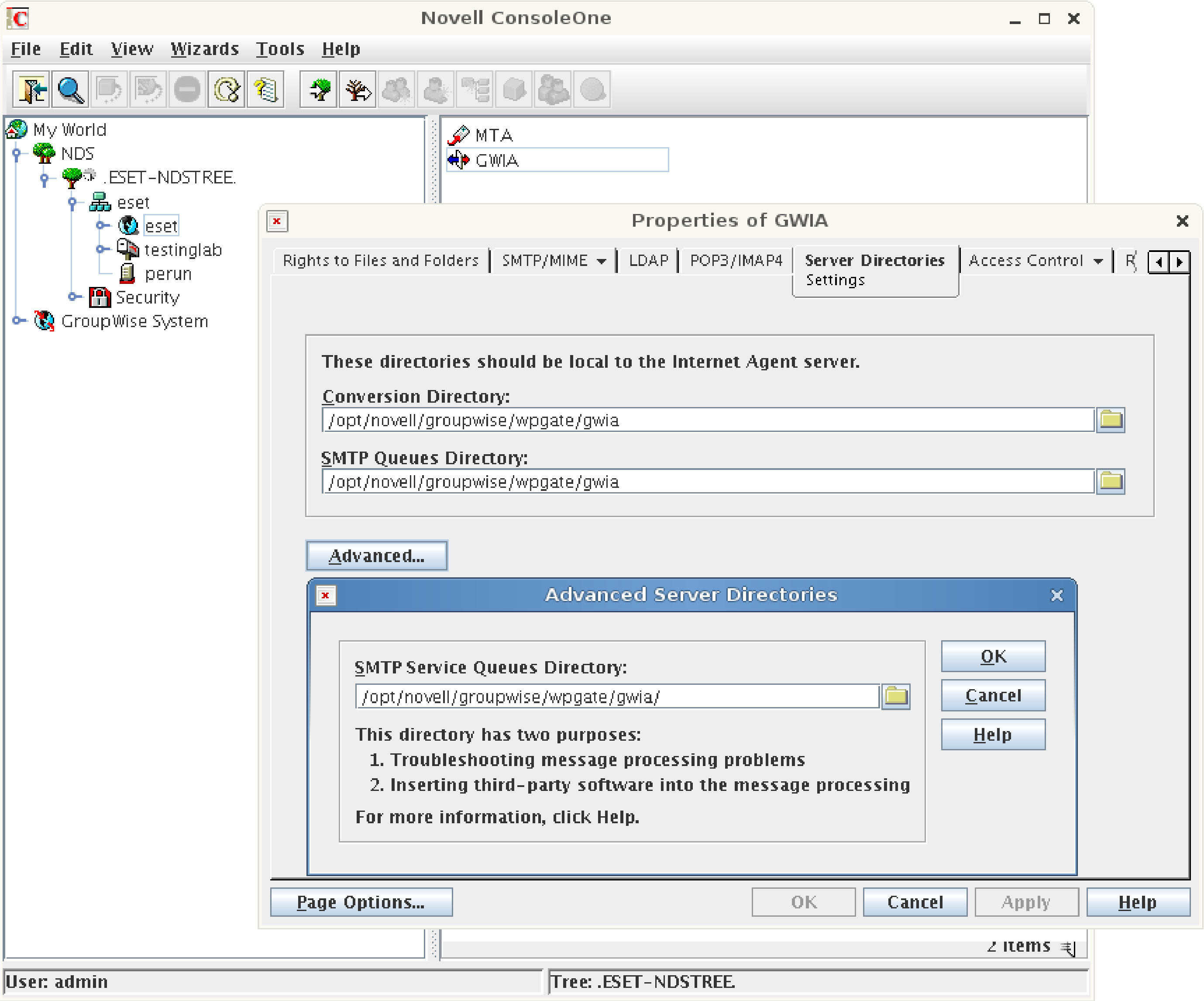
The module *esets_gwia* only allows the scanning of incoming email messages. For delivering email messages to clients immediately, the following GroupWise agent directories must have set the same paths:

- 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.



These directories should be local to the Internet Agent server.

Conversion Directory: /opt/novell/groupwise/wpgate/gwia

SMTP Queues Directory: /opt/novell/groupwise/wpgate/gwia

SMTP Service Queues Directory: /opt/novell/groupwise/wpgate/gwia/

This directory has two purposes:
1. Troubleshooting message processing problems
2. Inserting third-party software into the message processing

For more information, click Help.

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

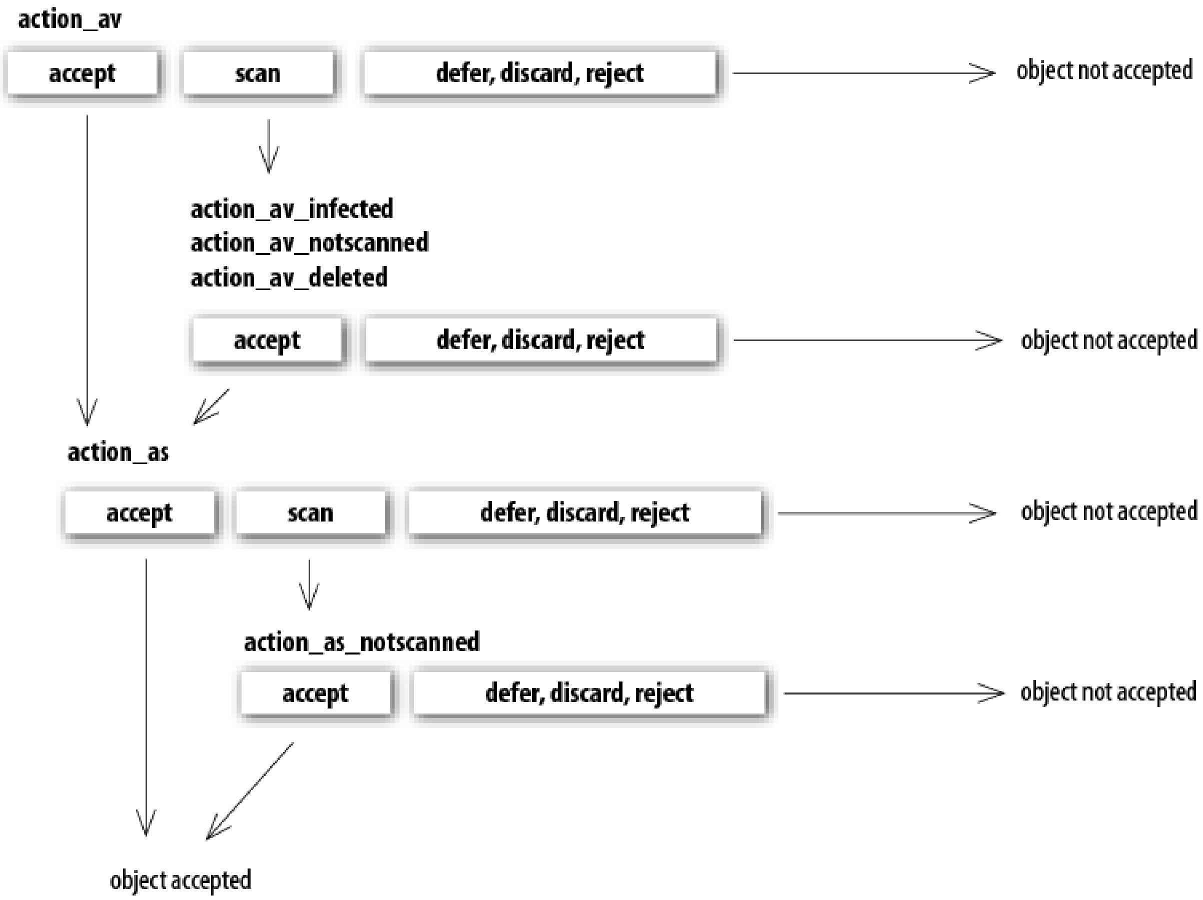
7.1 Handle Object Policy

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 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 only be used for email objects. Due to this, this functionality is relevant only for the following modules: esets_imap, esets_mda, esets_pipe, esets_pop3, esets_smtp, esets_smfi and esets_cgp.

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.

Regular updates of the anti-spam database can be administered using tasks in Scheduler. 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 then 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.most_accurate` files use the following command:

```
diff spamcatcher.conf spamcatcher.conf.most_accurate
```

spamcatcher.conf.most_accurate

- 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.

spamcatcher.conf.faster

- 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.least_network

- 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.

7.4.1 SpamCatcher settings

The *spamcatcher.conf* configuration file allows you to modify several additional settings that are not available in the ESETS confugration file. The settings in *spamcatcher.conf* are transparently structured and described:

- **Name** – parameter name
- **Arguments** – values the parameter can be assigned and their syntax
- **Default** – default parameter value
- **Description** – detailed parameter description

Blank lines and lines beginning with # are omitted.

A list of the most important settings in spamcatcher.conf

Parameter name	Details
approved_ip_list	List of approved IP addresses. You can specify IPs that should be approved, i.e., if the first non-ignored IP in Received headers matches any address in this list, the message scores 0 and no other checks are made.
blocked_ip_list	List of blocked IP addresses. You can specify IPs that should be blocked, i.e., if any non-ignored IP in Received headers matches the address in this list, the message scores 100 and no other checks are made.
ignored_ip_list	List of ignored IP addresses. You can specify IPs that should be ignored during Real-time Blackhole List (RBL) checks. You should include all internal IP addresses within the firewall not directly accessible from the Internet. Doing so prevents unnecessary checks and helps identify actual connecting IP

	addresses. Internal IP addresses are already skipped by the engine (192.168.x.y and 10.x).

rbl_list	List of Realtime Blackhole servers to be used when evaluating messages. The RBL request checks for presence of a specific IP address on a given RBL server. Subject to these checks are IP addresses in the Received: sections in the mail header.
	The entry format is as follows:
	`rbl_list=server:response:offset,server2:response2:offset2,...`
	The meaning of the parameters are explained below:
	• `server`
	RBL server name
	• `response`
	RBL server response if the IP address was found (standard responses are 127.0.0.2, 127.0.0.3, 127.0.0.4., etc.). This parameter is optional, and if not set, all answers will be considered.
	• `offset`
	Value from 0 to 100. Influences overall spam score. Standard value is 100, i.e. in case of a positive check the message is assigned the spam score of 100 and is evaluated as spam. Negative values lower the overall spam score of a message.
	Example 1:
	`rbl_list=ent.adbl.org`
	RBL check is performed using the `ent.adbl.org` server. If the check is positive, the message will be assigned a standard offset of 100 and marked as spam.
	Example 2:
	`rbl_list=ent.adbl.org::60`
	RBL check is performed using the `ent.adbl.org` server. If the check is positive, the message will be assigned an offset of 60 which increases its overall spam score.
	Example 3:
	`rbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	RBL check is performed using the defined servers (from left to right). In case of a positive check on `bx9.dbl.com` the offset of 85 will be added. If the check on `list.dnb.org` will be positive giving a response of 127.0.0.4 offset of 35 will be used. The offset will not be applied in cases of answers other than 127.0.0.4. If a check is positive on `req.gsender.org` the spam score will be decreased by 75 point (negative value).

rbl_max_ips	Maximum IP addresses that can be sent to RBL server check. Total number of RBL requests is the total amount of IP addresses in the Received: sections in the email header (up to the set limit in 'rbl_maxcheck_ips') multiplied by the number of RBL servers set in the 'rbl_list'. The value of 0 means there is no limit to the maximum number of IP addresses that can be checked. This parameter is applied only if the 'rbl_list' option is enabled (i.e. contains a minimum of 1 server).
approved_domain_list	Is a list of domains and IP addresses in the email body, that are to be considered as allowed. Do not use to whitelist emails by sender's domain!
blocked_domain_list	Is a list domains and IP addresses in the email body, that are to be considered as permanently blocked. This is not a blacklist of sender's addresses!
ignored_domain_list	List of domains in the email body, that are to be permanently excluded from DNSBL checks and ignored.
dnsbl_list	List of DNSBL (DNS-based Blackhole List) servers to be used in checks of domains and IP addresses in the email body. Format of entry is as follows: `dnsbl_list=server:response:offset,server2:response2:offset2,...` Meaning parameters used: • `server` DNSBL server name • `response` DNSBL server response if IP address/domain was found (standard responses are 127.0.0.2, 127.0.0.3, 127.0.0.4., etc.). This parameter is optional, and if not set, all answers will be considered. • `offset` Value from 0 to 100. Influences overall spam score. Standard value is 100, i.e. in case of a positive check the message is assigned the spam score of 100 and is evaluated as spam. Negative values lower the overall spam score of a message.

	DNSBL checks can have negative influence on server performance due to the fact that every domain/IP address from the message body is checked against all defined DNSBL servers and every single check requires processing a DNS server request. You can reduce the impact on system resources by deploying a DNS cache server for this purpose. For the same reason the non-routable IP addresses (10.x.x.x, 127.x.x.x, 192.168.x.x) are also omitted from DNSBL checks.
	Example 1:
	`dnsbl_list=ent.adbl.org`
	DNSBL check is performed against the `ent.adbl.org` server. If there is a positive, the message will be assigned the default offset 100 (it will be marked as spam).
	Example 2:
	`dnsbl_list=ent.adbl.org::60`
	DNSBL check is performed using the `ent.adbl.org` server. If the check is positive, the message will be assigned an offset of 60 which increases its overall spam score.
	Example 3:
	`dnsbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	DNSBL check is performed using the defined servers (from left to right). If there is a positive check on `bx9.dbl.com`, the offset of 85 will be added. If the check on `list.dnb.org` will be positive, giving a response of `127.0.0.4` an offset of 35 will be used. No offset will be applied in cases of answers other than 127.0.0.4. If a check is positive on `req.gsender.org` the spam score will be decreased by 75 points (negative value).

home_country_list	List of countries, that will be considered "home". Messages routed through a country not on this list will be evaluated using more strict rules (higher spam score will be applied). Entry format for countries is their two character code in compliance with ISO 3166.
home_language_list	List of preferred languages – i.e. languages that are the most used in your email messages. Such messages will be evaluated using less strict rules (lower spam score). Entry format for languages is their two character code in compliance with ISO 639.

custom_rules_list	Allows you to define custom lists of rules and store each list to an individual file. Each rule is stored on a separate line in the file in the following format:
	`Phrase, Type, Confidence, CaseSensitivity`
	Phrase – Any text, must not contain commas (,).
	Type – Can have the following values: SPAM, PHISH, BOUNCE, ADULT, FRAUD. If you enter other value that those listed above, the SPAM value will be used automatically. SPAM defines phrases that occur in classical spam messages (offers of goods and services). PHISH are phrases occurring in fraudulent messages (phishing), that are aimed at extraction of confidential data (names, passwords, credit card numbers, etc.) from users. BOUNCE are phrases used in automatic server responses - Non-Delivery Notification (used when spoofing sender's address). ADULT represents phrases typical for messages offering pornographic content. FRAUD stands for phrases used in fraudulent emails (scam) offering suspicious banking operations (money transfers via your account etc.). A typical example of this spam type is the so-called Nigerian spam.
	Confidence – Value from 0 to 100. Defines the probability of the phrase to be member of a specific spam category (listed above). If the Type PHISH has the Confidence 90, there is a very high probability of the phrase being used in phishing messages. The higher the Confidence score, the bigger impact it exerts on the overall spam score of the message. The Confidence value of 100 presents a special case, where the message spam score will also be 100, i.e. message will be marked as 100% spam. Analogically, if the value is 0, the message will be marked as not-spam.
	CaseSensitivity – values 0 or 1. 0 meaning the phrase is case insensitive. 1 meaning the phrase is case sensitive.
	Examples:
	`replica, SPAM, 100, 0`
	`Dear eBay member, PHISH, 90, 1`
	`return to sender, BOUNCE, 80, 0`

Other settings

enable_spf	This option enables/disables validation by SPF (Sender Policy Framework). This validation method checks the public rules of a domain - domain policy to determine whether a sender is authorized to send messages from that domain.

enable_all_spf	This option is to determine whether domains not on the 'spf_list' or Mailshell file can bypass the SPF validation. For this option to work correctly, the *'enable_realtime_spf'* parameter must be set to yes.
enable_realtime_spf	If this option is enabled, DNS requests will be sent in real-time during SPF validation. This can negatively influence the performance (delays during message evaluation).
spf_list	This option allows you to assign importance to a specific SPF entry, thus influencing the overall spam score of a message.
spf_*_weight	The asterisk represents 14 possible SPF validation results (see *spamcatcher.conf* for more details). The value entered for this parameter is an offset, that is then applied to the spam score according to individual result types. If the SPF validation results is "fail" the offset from the *'spf_fail_weight'* parameter will be applied. Depending on the offset value the resulting spam score is then increased/decreased.
spf_recursion_depth	Maximum nesting depth (using the "include" mechanism). The RFC 4408 norm specifies this limit to 10 (to prevent Denial-of-Service), however, some SPF records nowadays do not respect this limit, as more nesting levels need to be applied to fully satisfy the SPF request.
enable_livefeed_sender_repute	If this option is disabled, the SPF information from LiveFeed will be ignored.

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

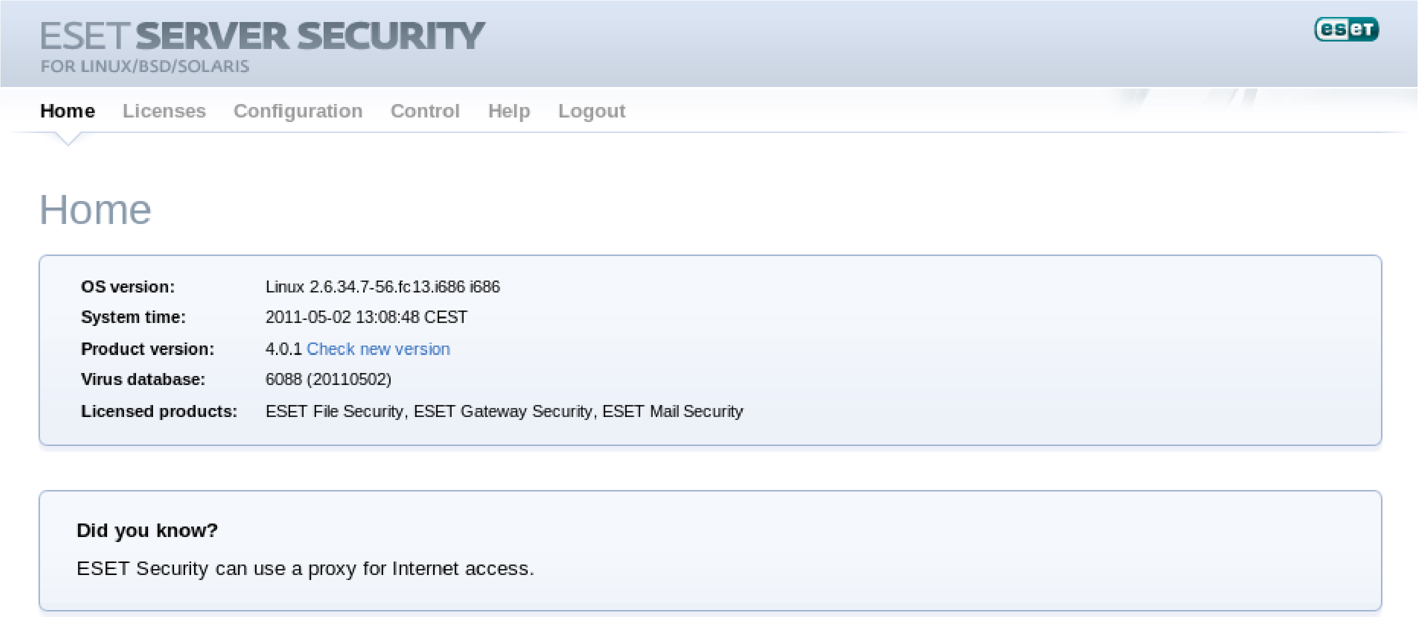
The web interface allows user-friendly configuration, administration and license management of ESET Security systems. This module is a separate agent and must be explicitly enabled. To quickly configure the *Web Interface*, set the following options in the ESETS configuration file and restart the ESETS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



Home

OS version: Linux 2.6.34.7-56.fc13.i686 i686
System time: 2011-05-02 13:08:48 CEST
Product version: 4.0.1 Check new version
Virus database: 6088 (20110502)
Licensed products: ESET File Security, ESET Gateway Security, ESET Mail Security

Did you know?

ESET Security can use a proxy for Internet access.

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 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 the **Save changes** button after making any changes in the **Configuration** section of the web interface to save your new settings. To apply your settings you will need to restart the ESETS daemon by clicking **Apply changes** on the left pane.

7.7.1 License management

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

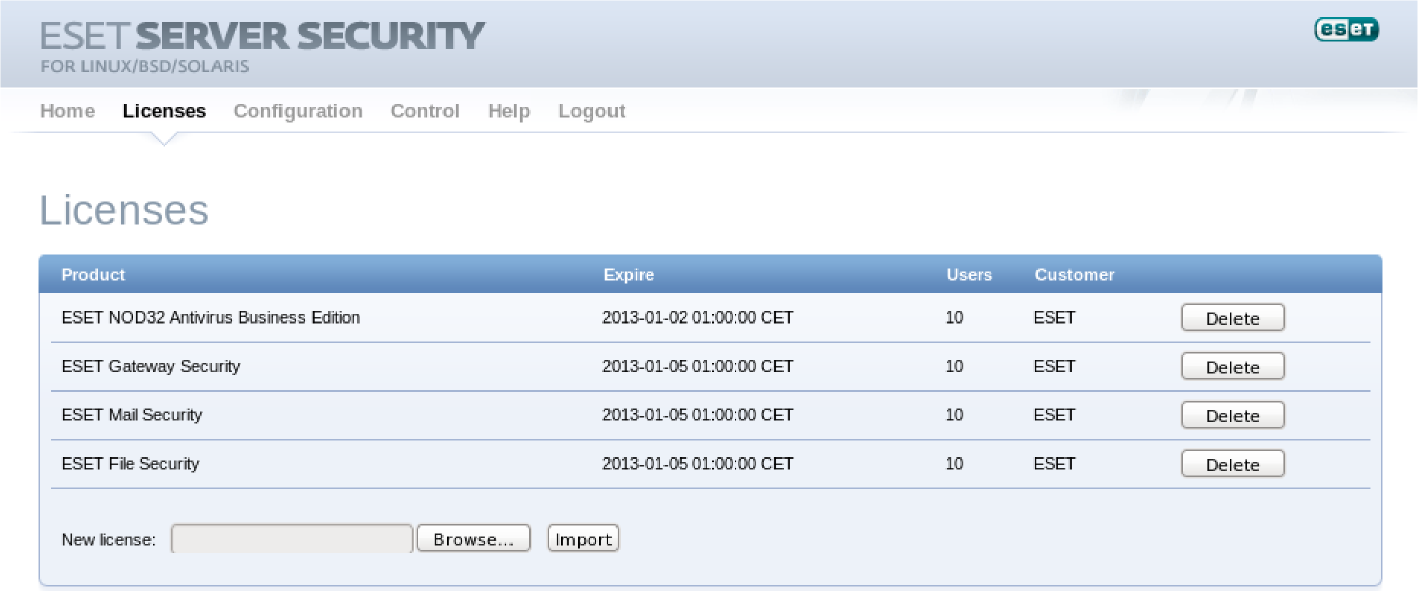
If you want to display licenses in the console, use the following command:

```
@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.



Licenses

Product	Expire	Users	Customer	
ESET NOD32 Antivirus Business Edition	2013-01-02 01:00:00 CET	10	ESET	Delete
ESET Gateway Security	2013-01-05 01:00:00 CET	10	ESET	Delete
ESET Mail Security	2013-01-05 01:00:00 CET	10	ESET	Delete
ESET File Security	2013-01-05 01:00:00 CET	10	ESET	Delete

New license: Browse... Import

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, 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.

7.7.2 SMTP+Postfix configuration example

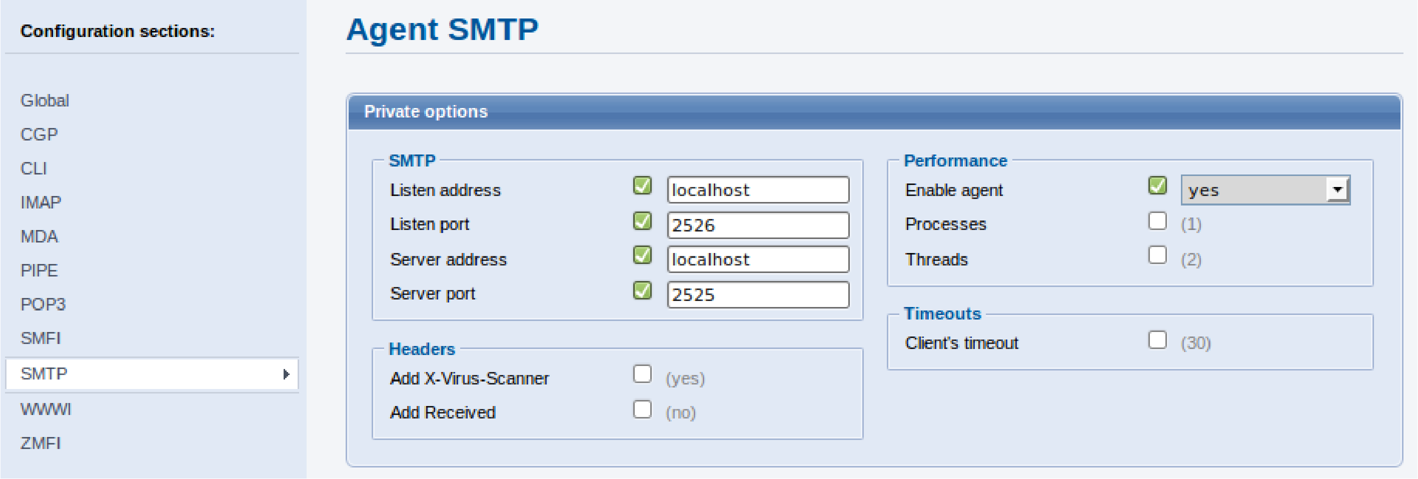
ESETS can be configured in two ways. In this example, we will demonstrate how to use both when configuring the SMTP module, leaving you the choice of your preferred configuration method:

- 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.



Configuration sections:

Global
CGP
CLI
IMAP
MDA
PIPE
POP3
SMFI
SMTP
WWWI
ZMFI

Agent SMTP

Private options

SMTP
Listen address ☑ localhost
Listen port ☑ 2526
Server address ☑ localhost
Server port ☑ 2525

Headers
Add X-Virus-Scanner ☐ (yes)
Add Received ☐ (no)

Performance
Enable agent ☑ yes
Processes ☐ (1)
Threads ☐ (2)

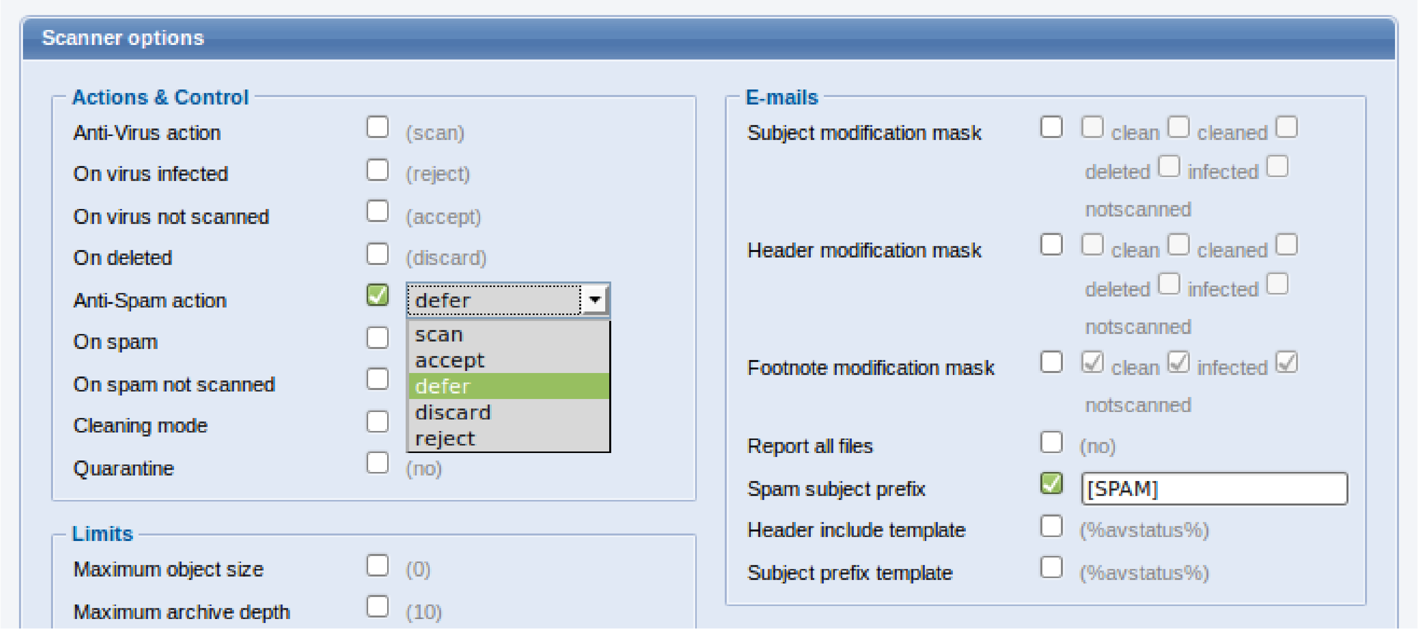
Timeouts
Client's timeout ☐ (30)

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.



Scanner options

Actions & Control
Anti-Virus action ☐ (scan)
On virus infected ☐ (reject)
On virus not scanned ☐ (accept)
On deleted ☐ (discard)
Anti-Spam action ☑ defer

On spam ☐
On spam not scanned ☐
Cleaning mode ☐
Quarantine ☐ (no)

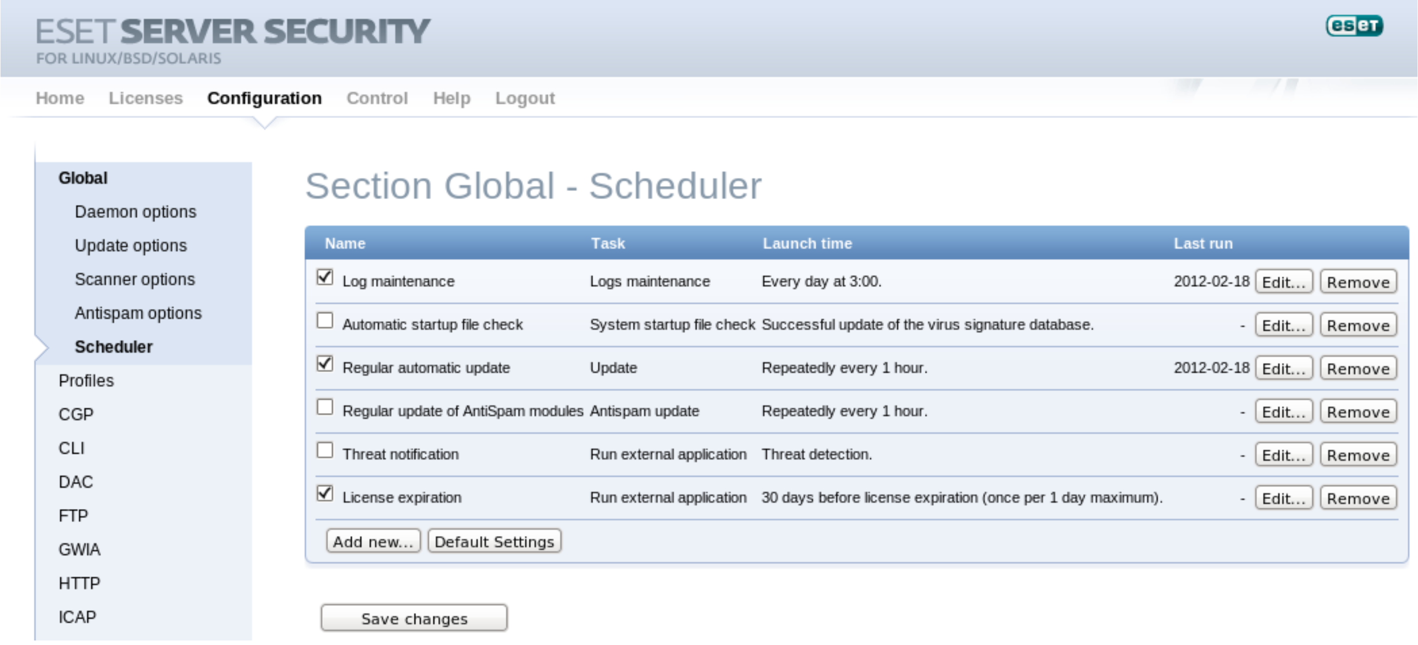
Limits
Maximum object size ☐ (0)
Maximum archive depth ☐ (10)

E-mails
Subject modification mask ☐ ☐ clean ☐ cleaned ☐ deleted ☐ infected ☐ notscanned
Header modification mask ☐ ☐ clean ☐ cleaned ☐ deleted ☐ infected ☐ notscanned
Footnote modification mask ☐ ☑ clean ☑ infected ☑ notscanned
Report all files ☐ (no)
Spam subject prefix ☑ [SPAM]
Header include template ☐ (%avstatus%)
Subject prefix template ☐ (%avstatus%)

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.



Section Global - Scheduler

Name	Task	Launch time	Last run
☑ Log maintenance	Logs maintenance	Every day at 3:00.	2012-02-18 Edit... Remove
□ Automatic startup file check	System startup file check	Successful update of the virus signature database.	- Edit... Remove
☑ Regular automatic update	Update	Repeatedly every 1 hour.	2012-02-18 Edit... Remove
□ Regular update of AntiSpam modules	Antispam update	Repeatedly every 1 hour.	- Edit... Remove
□ Threat notification	Run external application	Threat detection.	- Edit... Remove
☑ License expiration	Run external application	30 days before license expiration (once per 1 day maximum).	- Edit... Remove

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 is the best method of keeping the maximum level of security on your computer. See ESETS update utility for more information.

Regular update of AntiSpam modules – The period after which ESETS will check for available antispam module updates. If you do not set this scheduled task, ESETS will not regularly update its antispam database.

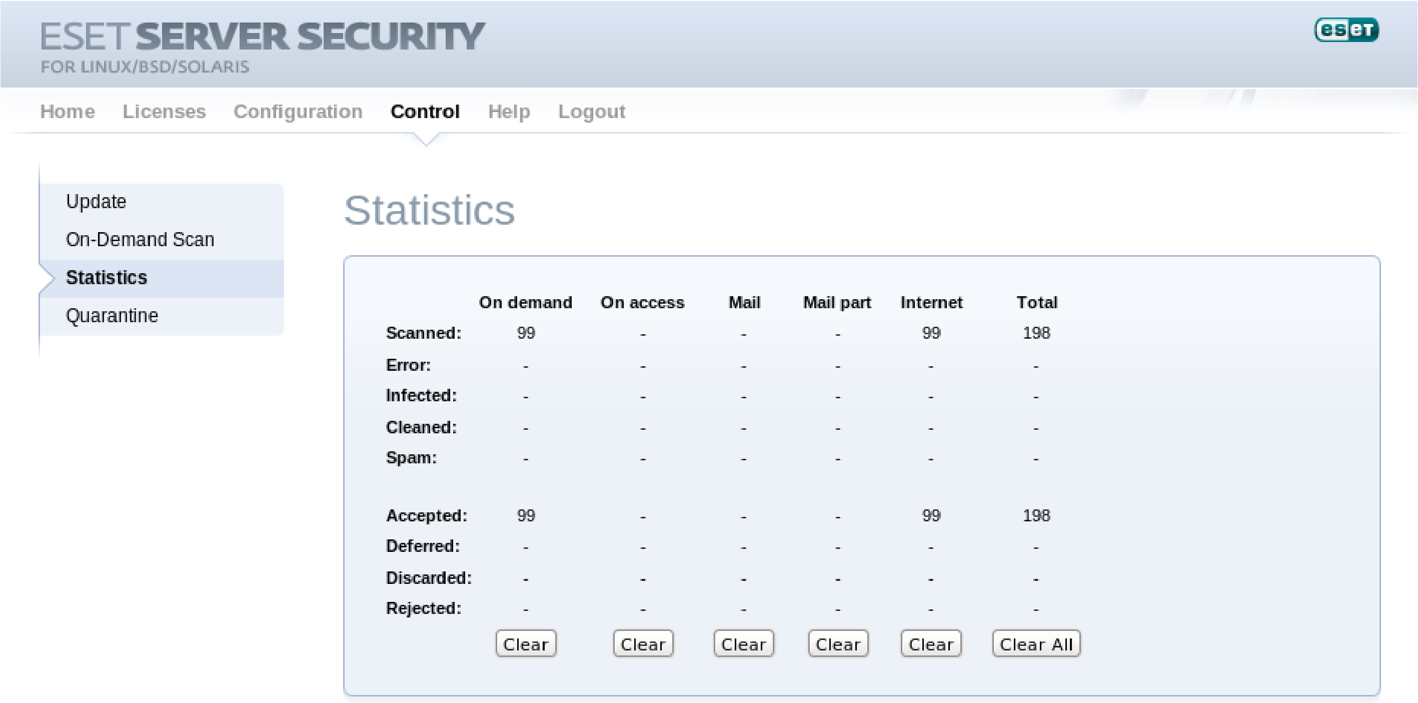
Threat notification – By default, each threat will be logged into syslog. In addition, ESETS can be configured to run an external (notification) script to notify a system administrator via email about threat detection.

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.



	On demand	On access	Mail	Mail part	Internet	Total
Scanned:	99	-	-	-	99	198
Error:	-	-	-	-	-	-
Infected:	-	-	-	-	-	-
Cleaned:	-	-	-	-	-	-
Spam:	-	-	-	-	-	-
Accepted:	99	-	-	-	99	198
Deferred:	-	-	-	-	-	-
Discarded:	-	-	-	-	-	-
Rejected:	-	-	-	-	-	-
	Clear	Clear	Clear	Clear	Clear	Clear All

7.8 Remote Administration

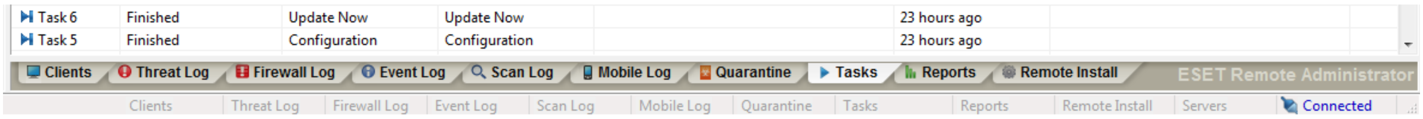
ESETS supports remote administration for mail security management in large computer networks. The ESETS Remote Administration Client is part of the main ESETS daemon and performs the following functions:

- 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 results 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 6-7. ERA Console tabs.



Task 6	Finished	Update Now	Update Now	23 hours ago
Task 5	Finished	Configuration	Configuration	23 hours ago

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

ESETS can be managed using ESET Remote Administrator 5.x. However, is is possible but not supported to configure ESETS to be managed by ERA 6.x; for more information please see this ESET Knowledgebase article.

7.8.1 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).

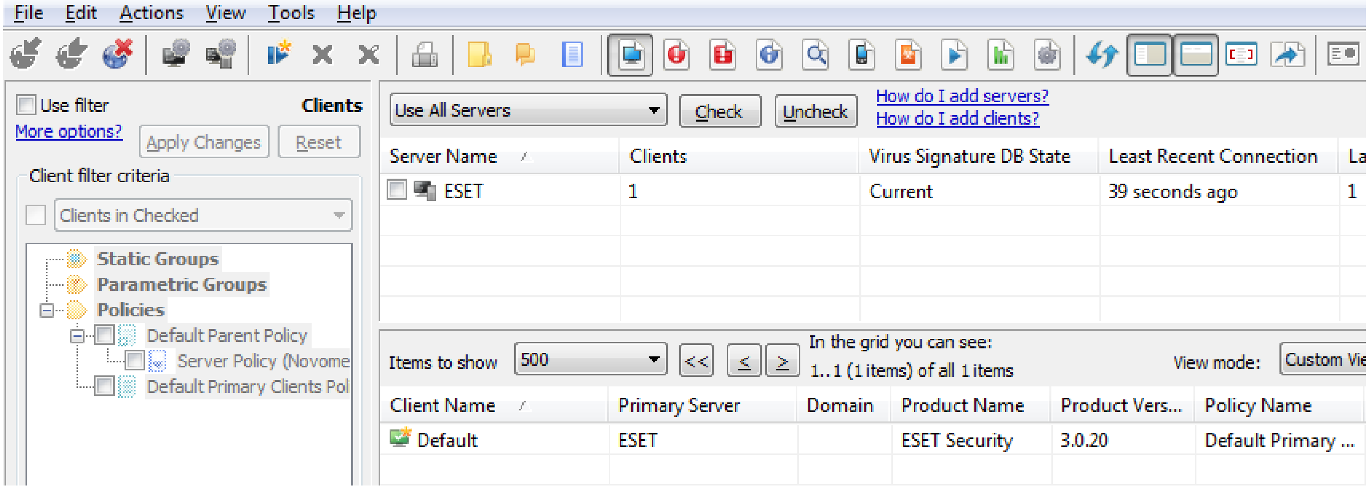
You can either use the web interface (see also previous chapter) to apply the new configuration, or you can adjust these parameters in the **[global]** section of the ESETS configuration file as follows:

```
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 6-8. ERA Console.



Server Name	Clients	Virus Signature DB State	Least Recent Connection	La
ESET	1	Current	39 seconds ago	1

In the grid you can see:
1..1 (1 items) of all 1 items

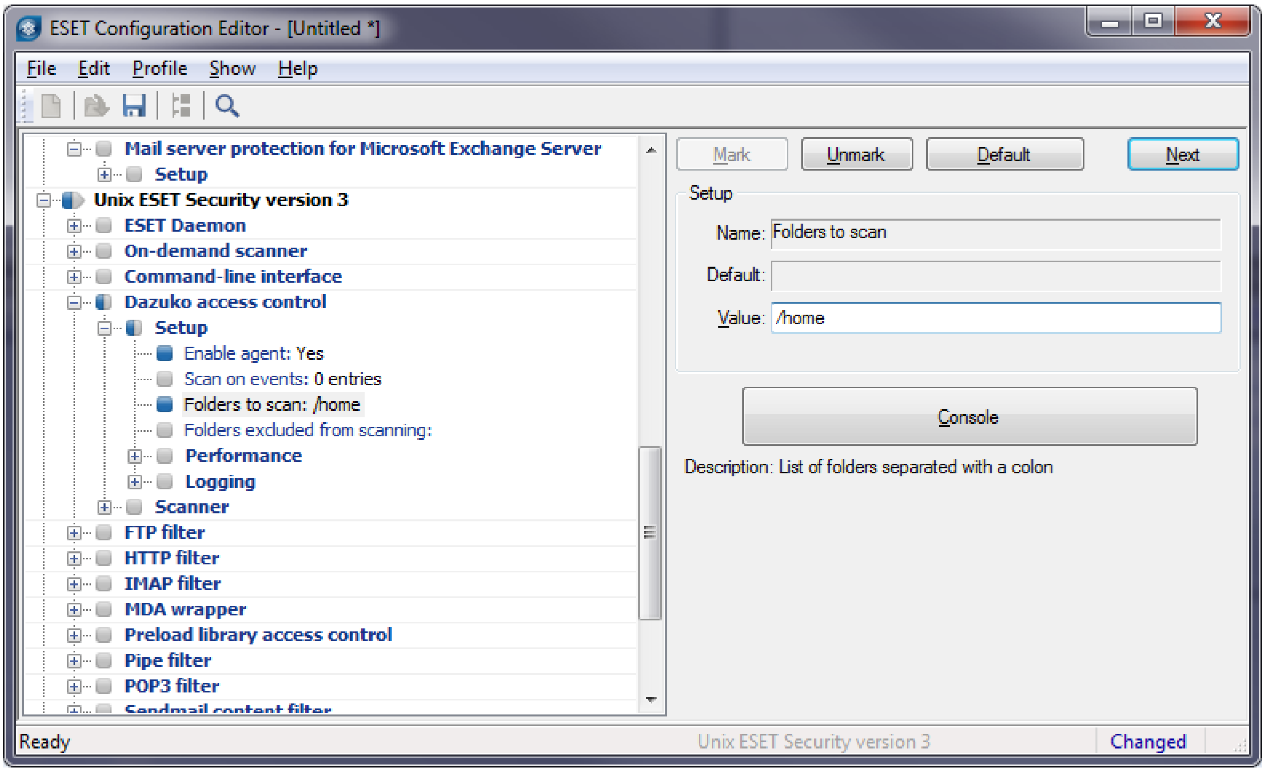
Client Name	Primary Server	Domain	Product Name	Product Vers...	Policy Name
Default	ESET		ESET Security	3.0.20	Default Primary ...

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 6-8. ERA Configuration Editor.



ESET Configuration Editor - [Untitled *]

- Mail server protection for Microsoft Exchange Server
  - Setup
- Unix ESET Security version 3
  - ESET Daemon
  - On-demand scanner
  - Command-line interface
  - Dazuko access control
    - Setup
      - Enable agent: Yes
      - Scan on events: 0 entries
      - Folders to scan: /home
      - Folders excluded from scanning:
      - Performance
      - Logging
    - Scanner
  - FTP filter
  - HTTP filter
  - IMAP filter
  - MDA wrapper
  - Preload library access control
  - Pipe filter
  - POP3 filter
  - Sendmail content filter

Setup

Name: Folders to scan

Default:

Value: /home

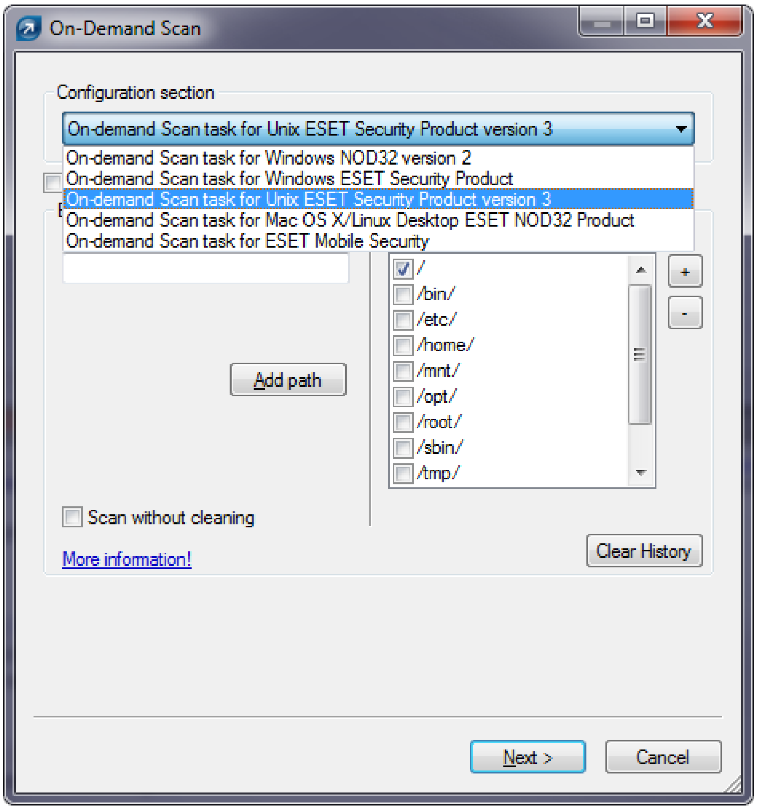
Description: List of folders separated with a colon

Ready — Unix ESET Security version 3 — Changed

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.



On-Demand Scan

Configuration section

On-demand Scan task for Unix ESET Security Product version 3

- On-demand Scan task for Windows NOD32 version 2
- On-demand Scan task for Windows ESET Security Product
- On-demand Scan task for Unix ESET Security Product version 3
- On-demand Scan task for Mac OS X/Linux Desktop ESET NOD32 Product
- On-demand Scan task for ESET Mobile Security

☑ /
□ /bin/
□ /etc/
□ /home/
□ /mnt/
□ /opt/
□ /root/
□ /sbin/
□ /tmp/

□ Scan without cleaning

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
```

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 scripts

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, 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 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://kb.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/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 scripts 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 scripts 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 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.

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
```

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.

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
```

On NetBSD and Solaris:

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

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
```

On NetBSD and Solaris:

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

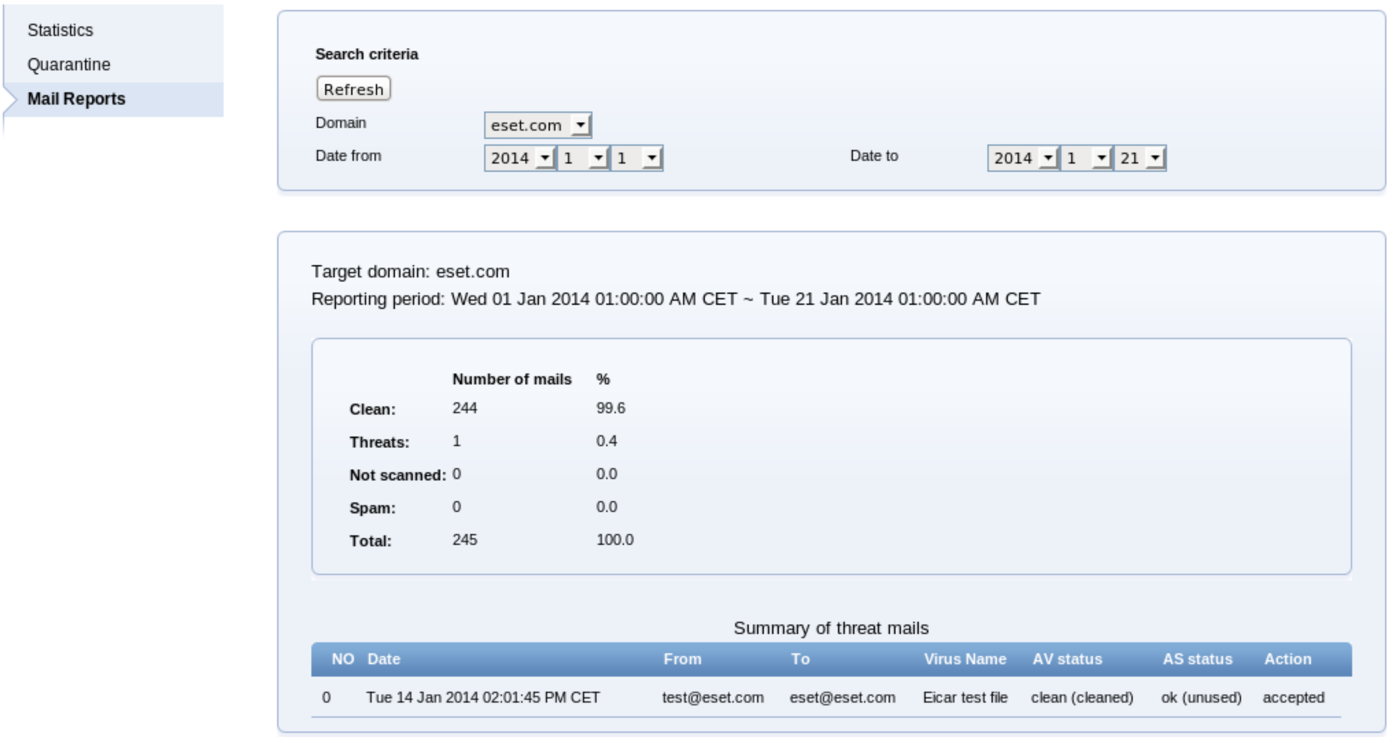
10.12 Setting ESETS to enable Mail reporting functionality

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.



Domain: eset.com

Date from: 2014 1 1 Date to: 2014 1 21

Target domain: eset.com
Reporting period: Wed 01 Jan 2014 01:00:00 AM CET ~ Tue 21 Jan 2014 01:00:00 AM CET

	Number of mails	%
Clean:	244	99.6
Threats:	1	0.4
Not scanned:	0	0.0
Spam:	0	0.0
Total:	245	100.0

Summary of threat mails

NO	Date	From	To	Virus Name	AV status	AS status	Action
0	Tue 14 Jan 2014 02:01:45 PM CET	test@eset.com	eset@eset.com	Eicar test file	clean (cleaned)	ok (unused)	accepted

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.

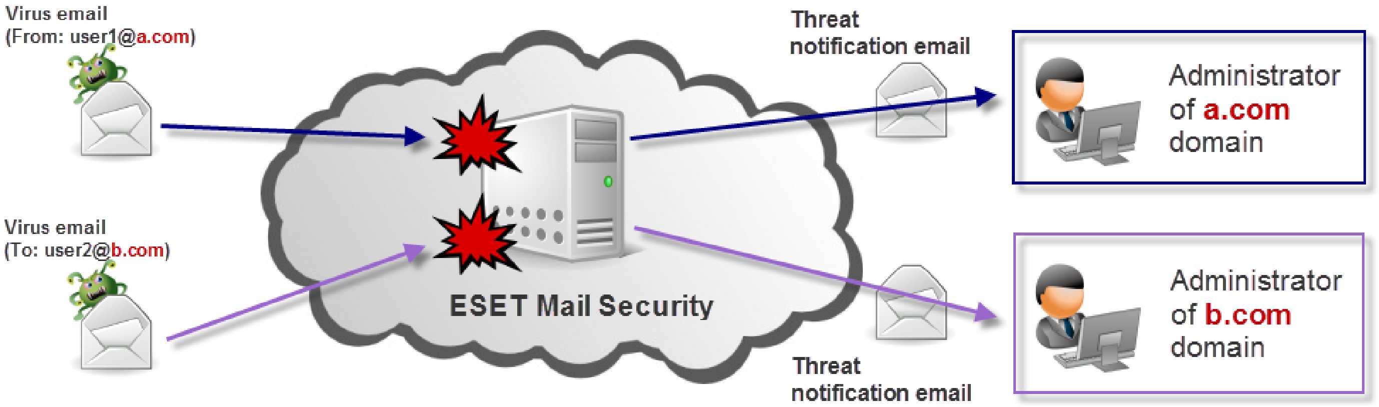
For more information please refer to the *esets_daemon(8)* man page.

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 - 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.
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.