



Spam filter and e-mail categorisation service

Installation and configuration of expurgate.Inhouse



---

## **Installation and configuration of eXpurgate.Inhouse**

<b>Prologue .....</b>	<b>4</b>
<b>Requirements for using eXpurgate.Inhouse .....</b>	<b>4</b>
<b>Notes on changes introduced with version 2.0 .....</b>	<b>4</b>
<b>The eXpurgate principle.....</b>	<b>5</b>
<b>1 eXpurgate.Inhouse plug-in functions .....</b>	<b>6</b>
1.1 <i>Using eXpurgate as an SMTP proxy</i>	6
1.2 <i>Using eXpurgate as a SpamAssassin server (spamd)</i>	6
1.3 <i>Using eXpurgate as a sendmail milter</i>	6
<b>2 Installing eXpurgate.Inhouse .....</b>	<b>9</b>
2.1 <i>Installing eXpurgate on a Windows system</i>	9
2.1.1 Windows service commands	16
2.1.2 Changing the TCP port for Microsoft Exchange 5.5	16
2.1.3 Changing the TCP port for Microsoft Exchange 2000 and 2003	17
2.1.4 How to test whether Exchange is listening on a port	18
2.2 <i>Installing eXpurgate on a Unix system</i>	19
2.2.1 Running eXpurgate on Sun Solaris	19
<b>3 Configuring eXpurgate .....</b>	<b>20</b>
3.1 <i>General command line options</i>	20
3.2 <i>Options when using the SMTP or SpamAssassin protocol</i>	21
3.3 <i>SMTP-specific options</i>	22
3.3.1 Prioritization when using more than one 'target' server	23
3.3.2 XCLIENT extension	23
3.4 <i>Logging-specific options</i>	24
3.5 <i>Meaning of the logfile entries</i>	25
3.6 <i>Usage of SOCKS</i>	25
3.7 <i>SSL/TLS for encrypted e-mail transfer</i>	25
3.8 <i>Adding 'Received' headers</i>	25
3.9 <i>Adapting SMTP messages</i>	25
3.10 <i>The expurgate.xml configuration file</i>	25
<b>4 Testing eXpurgate's functions .....</b>	<b>25</b>
4.1 <i>Basic tests of your eXpurgate installation</i>	25

---

4.2	<i>Specific options for testing eXpurgate</i>	25
4.3	<i>Notes on testing eXpurgate's e-mail categorization</i>	25
4.4	<i>Using telnet to check functionality</i>	25
5	<b>Integrating eXpurgate in an existing mail system .....</b>	<b>25</b>
5.1	<b><i>Running eXpurgate as an SMTP forwarder</i></b>	<b>25</b>
5.1.1	Necessary changes in Postfix when using eXpurgate as a forwarder	25
5.2	<b><i>eXpurgate as a Content_Filter in Postfix ("Sandwich")</i></b>	<b>25</b>
5.3	<b><i>eXpurgate in Postfix with other Content_Filters, like an antivirus solution</i></b>	<b>25</b>
5.4	<b><i>Integrating eXpurgate in Exim</i></b>	<b>25</b>
5.5	<b><i>Using eXpurgate as a SpamAssassin spamd</i></b>	<b>25</b>
5.6	<b><i>Integrating eXpurgate in Qmail</i></b>	<b>25</b>
6	<b>Fine-tuning e-mail processing .....</b>	<b>25</b>
6.1	<b><i>Global switches</i></b>	<b>25</b>
6.2	<b><i>User-specific control of the eXpurgate checks: User Features</i></b>	<b>25</b>
6.3	<b><i>Control depending on the sender</i></b>	<b>25</b>
6.3.1	Handling e-mails from specific sender addresses	25
6.3.2	Dealing with E-mails from Specific Sender IP Addresses	25
6.4	<b><i>Freezing</i></b>	<b>25</b>
6.4.1	Prerequisites	25
6.4.2	Configuration	25
6.5	<b><i>Handling of spam e-mails</i></b>	<b>25</b>
6.5.1	System-wide treatment of spam mail	25
6.5.2	User-specific processing of e-mail	25
6.5.3	Configuring the Reject text	25
6.6	<b><i>Handling of virus e-mails</i></b>	<b>25</b>
6.7	<b><i>Advanced options for processing individual E-mail types</i></b>	<b>25</b>
6.8	<b><i>Turning off sub-categories of "dangerous"</i></b>	<b>25</b>
6.9	<b><i>Treating "suspect" as "clean"</i></b>	<b>25</b>
6.10	<b><i>Dealing with Bounce E-mails</i></b>	<b>25</b>
6.11	<b><i>Treating certain sub-categories of "clean" as spam</i></b>	<b>25</b>
7	<b>Using eXpurgate statistics .....</b>	<b>25</b>
Supplement	<b>.....</b>	<b>25</b>
	<b><i>eXpurgate's e-mail categories</i></b>	<b>25</b>
	<b><i>IP nets of eXpurgate servers</i></b>	<b>25</b>
	<b><i>Licenses</i></b>	<b>25</b>

---

## Prologue

Using numerous examples, this documentation will explain the functionality of our spam-recognition and e-mail-categorization software eXpurgate.Inhouse. It is designed to give you an overview as well as a reference for dealing with special scenarios and customization. Please do not let the volume of this document startle you: a standard installation should only take about fifteen minutes. Please note that this document exclusively covers the eXpurgate.Inhouse solution, that is, the eXpurgate plug-in in combination with your existing mail server.

## Requirements for using eXpurgate.Inhouse

**In order for eXpurgate.Inhouse to categorize incoming e-mails, it is *mandatory* to ensure that eXpurgate can establish TCP connections to the following nets:**

**194.145.224.0/24**

***and***

**195.190.135.0/24**

**on port 55555.**

Please review and if necessary adjust your firewall settings.

## Notes on changes introduced with version 2.0

With the leap from version 1.3.x to 2.x, some fundamental changes were made in eXpurgate. Let's have a look at them in brief (for details, please refer to the corresponding chapters given in the links).

*Necessary changes to the configuration file expurgate.xml (please add the lines to the appropriate sections of your existing configuration file):*

- New section <SmtOutList>: Use this section to configure the SMTP relays to which eXpurgate shall pass on e-mails after the spam-check. You can configure several relays with different priorities. Note: This section must exist in the configuration file. It may remain empty however, if as SMTP relay is specified – as before – using the command line (see chapter 3.3.1: *Prioritization when using more than one 'target' server*).
- The parameter "filterOnOffForUserInFile" is not used any longer. It has been replaced by the parameters "noFreezingForAllUsers", "noExpurgateForAllUsers", and "noVirusCheckForAllUsers".  
What's more, you can use the parameter "userFeaturesDB" to specify the scanning features that shall be turned on or off on a per-user or per-domain basis (see chapter 6.2: *User-specific control of the eXpurgate checks: User Features*).
- Parameters to configure the new *Freezing* feature (see chapters 6.4 ff).
- Support for the XCLIENT extension to SMTP (introduced in v 2.0.5, see chapter 3.3.2)

**Command line options:** Starting with v 2.0.5, you **have to specify** `smtpouthost`.

For information on the new parameter `--logmailidalways` (introduced in v 2.0.4), please see chapter 3.4.

## The eXpurgate principle

eXpurgate is based on a new technology for spam recognition and e-mail categorization developed by **eleven**: among other tests, eXpurgate checks an e-mail for the determining characteristic of spam: its mass-mailing features. A fundamental part of the test is the so-called *bulkcheck*, for which eleven has developed a control sum algorithm that enables the system to compare several e-mails to each other without having any knowledge of their contents. This is carried out by reducing an e-mail to only a few bytes of code, from which no conclusions whatsoever can be drawn as to the e-mail's original contents. The more often an identical or similar e-mail has been received before, the greater the possibility that the e-mail being checked is spam or similar bulk e-mail. Identification occurs solely by way of a short checksum.

The combination with further test procedures enables eXpurgate to unambiguously classify an e-mail as spam and separate it from other (welcome) bulk mail at the same time, for example newsletters, mailing lists, forums, etc. In addition, eXpurgate also recognizes e-mail attachments containing dangerous components, such as viruses and worms, which could cause harmful changes to a user's system. As a rule, eleven's self-learning *bulkcheck* technology causes negligible split-second delays to the delivery of customers' e-mail. What's more, privacy is guaranteed due to coded transfer. As opposed to hitherto available spam filters, the technology *reduces* 'false positives' (e-mail wrongly recognized as spam) to an absolute minimum.

After an e-mail has been categorized, headers are added to it to enable automatic processing. For more information on headers see supplement A of this document. Additional hints on configuring your e-mail program can be found at [www.eleven.de/support/](http://www.eleven.de/support/)

## 1 eXpurgate.Inhouse plug-in functions

In the current version, eXpurgate works as an *SMTP proxy* (relay), a so-called *Spam Assassin Server* (*spamd*), or as a *Sendmail Militer*. We would like to briefly introduce these functions. One thing these concepts have in common is that eXpurgate only deals with the categorization of e-mails, not their delivery to users. Therefore, an existing e-mail server is always needed for user and e-mail account administration. Because of its small demand for resources, eXpurgate generally does not require any extra hardware, but can be installed on the machine which already runs the mail server.

All installation modes are based on the bulkcheck as the main principle of eXpurgate: During the analysis of each incoming mail, a special kind of checksum is generated and transferred (via an encrypted SSL-connection) to one of the central eXpurgate servers. These redundantly equipped servers are located at several sites in order to provide the highest possible availability of the service. To transfer the checksum, eXpurgate.Inhouse requires to establish a connection to the servers in the nets 194.145.224.0/24 and 195.190.135.0/24<sup>1</sup> on port 55555, and to receive their answers. Therefore, your firewall may have to be reconfigured accordingly. Alternatively, the SOCKS protocol - if available - may be used. The central eXpurgate servers do not establish connection of their own: they only reply to external requests.

### 1.1 Using eXpurgate as an SMTP proxy

When used as an *SMTP proxy*, eXpurgate works like an additional, upstream mail server: it accepts incoming e-mails via SMTP (Simple Mail Transfer Protocol) on a defined port, checks the e-mail, and forwards it via SMTP together with a corresponding mark to a defined host and port. eXpurgate is purely a relay server that forwards e-mails to precisely one host. Mechanisms such as DNS MX records are ignored. When used as a proxy, eXpurgate itself accepts the incoming mail, forwarding it to the 'real' mail server after examination.

### 1.2 Using eXpurgate as a SpamAssassin server (spamd)

As a *Spam Assassin Server*, however, eXpurgate will not directly accept incoming e-mails. Instead, it receives requests and e-mails from a SpamAssassin client on a defined input port and answers them using the SpamAssassin protocol, depending on whether or not the respective e-mail is classified as spam. An additional header is also returned containing the e-mail's category. For more information, please see the *Spamd* configuration example below (cf. 5.5, p. 25) as well as [www.spamassassin.org](http://www.spamassassin.org).

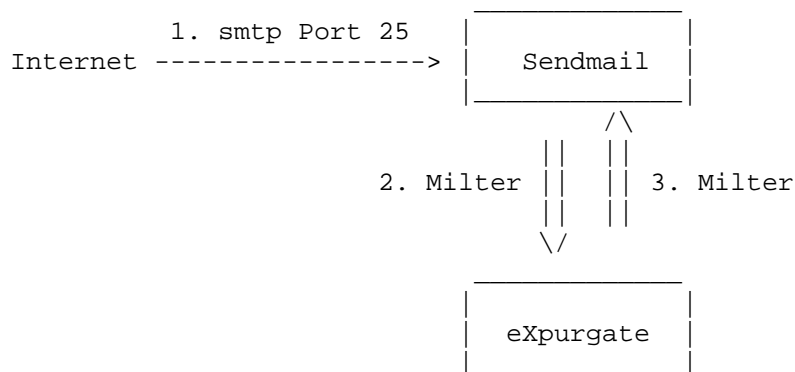
### 1.3 Using eXpurgate as a sendmail militer

When used as a *sendmail militer* (Mail Filtering API), eXpurgate works in a similar manner to a SpamAssassin daemon, in that it uses the militer protocol. However, the militer protocol will only work with *Sendmail* (officially with version 8.12 and newer).

---

<sup>1</sup> Both nets are documented in the public RIPE database as ELEVEN-NET and ELEVEN-NET2 (please see the supplement).

How it works can be roughly described as follows:



Please note that the functionality described in chapter

### 6.2: User-specific control of the eXpurgate checks: User Features

is only available with eXpurgate configured as an SMTP proxy (including before-queue content filter for Postfix). When using eXpurgate with the Militer interface, however, user features are unavailable, as the milter protocol does not offer to transmit the recipient data necessary to accomplish those features.

To integrate eXpurgate in sendmail, sendmail must be compiled to include the ability to connect to milter programs. In order to check whether it can, use the following command:

```
sendmail -bt -d0.4 < /dev/null
```

Among other things, this will provide you with a list of options compiled into sendmail (*Compiled with*). The output should look something like this:

```
Compiled with: DNSMAP LOG MAP_REGEX MILTER MIME7TO8 MIME8TO7
```

If 'milter' can be found in this list, sendmail is ready for usage with milter. If 'milter' is not listed, sendmail has to be recompiled, with "devtools/Site/site.config.m4" containing the following line:

```
APPENDDEF(`confENVDEF', ` -DMILTER')
```

Afterwards, sendmail has to be recompiled using the option `-c2`.

There are several ways for sendmail to establish contact to a milter program. This can be accomplished by using a **configuration string** in which you specify the protocol to be used, followed by a colon. The following protocols can be used:

Named Sockets	unix:/path/to/communication/file
	local:/path/to/communication/file
IP V4 Sockets	inet:port@hostname
IP V6 Sockets	inet6:port@hostname

<sup>2</sup> The option `-c` tells the compiler to use the changes made in site.config.m4. It need not be added if sendmail is compiled for the first time.

You have to set the same communication protocol in sendmail and eXpurgate. The following entry must be present in 'sendmail.mc':

```
INPUT_MAIL_FILTER(`eXpurgate', `S=<communication_string>, F=, T=C:10m;S:5m;R:5m;E:5m')dnl
define(`confINPUT_MAIL_FILTERS',`eXpurgate')dnl
```

<communication\_string> has to be replaced by your custom string.

**Example:**

```
INPUT_MAIL_FILTER(`eXpurgate', `S=local:/var/run/sendmail/eXpurgate.sock,
F=, T=C:10m;S:5m;R:5m;E:5m')dnl
```

To start eXpurgate as a milter, the command line must look like this:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml --servermode
--milter <communication_string>
```

Please replace <communication\_string> with the same string as above.

**Example:**

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml -servermode
--milter local:/var/run/sendmail/eXpurgate.sock
```



## 2 Installing eXpurgate.Inhouse

In the following section, we would like to show you how to install eXpurgate on a Windows or a Unix system. Both sections are tailored to the operating system in question, meaning you only have to read the section dealing with the operating system that interests you. In any case, please read the next main section on configuring eXpurgate: for the most part, this is independent of the operating system on which eXpurgate runs, which is why it has its own chapter.

Whilst developing eXpurgate, we have striven to make working with it as easy as possible. Therefore, you will need to make very few, if any, changes to the default configuration.

### 2.1 Installing eXpurgate on a Windows system

When installing eXpurgate on Microsoft Windows, all necessary parameters are inquired during the installation process. eXpurgate is then installed as a service and started.<sup>3</sup>

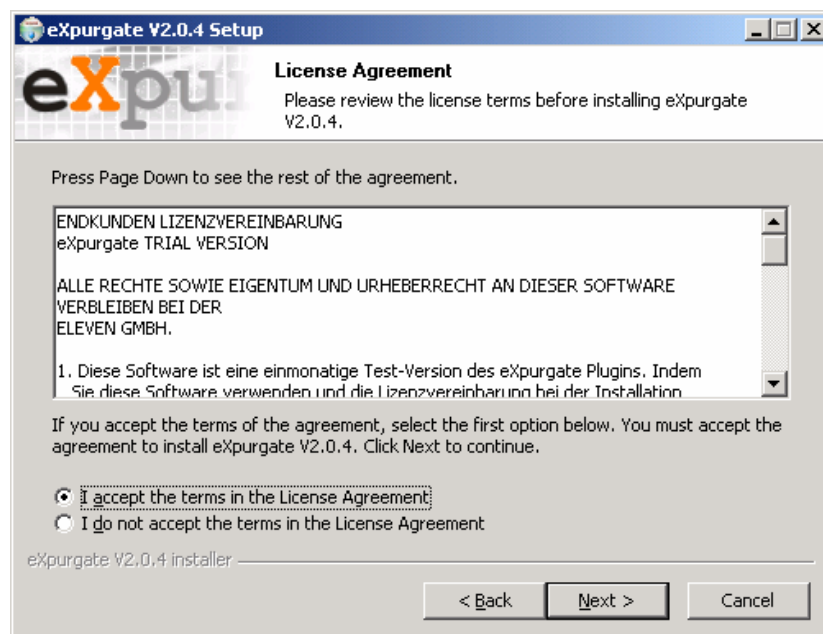
To begin the installation process, double-click the eXpurgate installation file (named e. g. expurgate-V2\_0\_0\_WindowsNT\_x86.exe). The installation assistant appears, which will guide you through the rest of the installation.



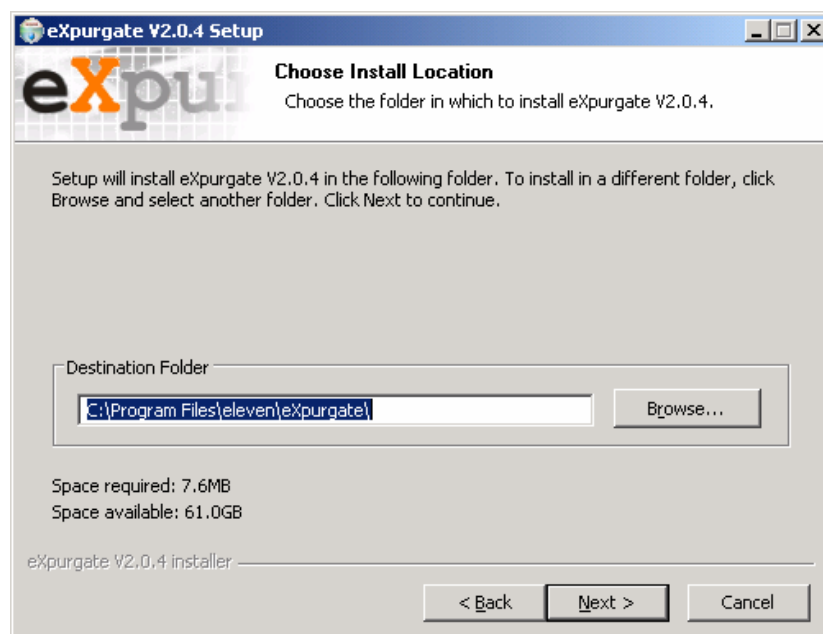
Click *Next* to start the installation.

---

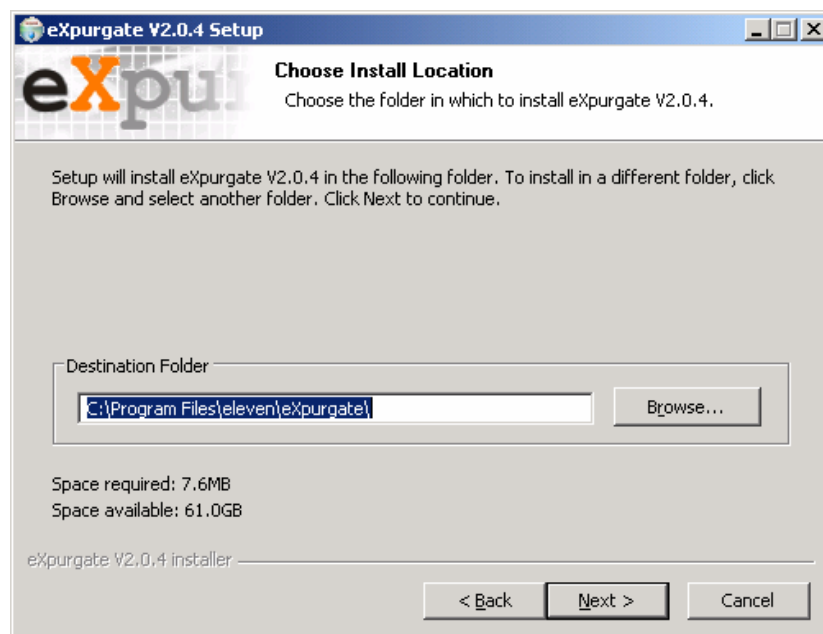
<sup>3</sup> You can repeat the initial installation at any time by running the installer again, or by starting the eXpurgate setup menu in the Windows start menu. Please note: This will overwrite your eXpurgate.xml file, meaning any settings from a previous installation will be overwritten.



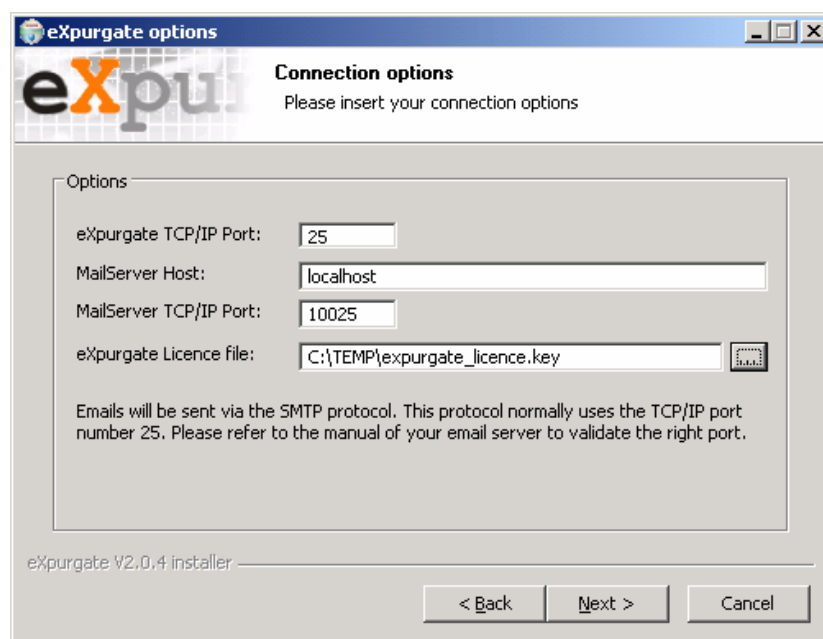
Please read the license agreement carefully and tick *"I accept the terms in the License Agreement"*. Then, click *Next*.



Now choose the directory in which you wish to install eXpurgate. The default setting corresponds to `eleven\eXpurgate` in your program directory (which would, for example, result in `C:\Program Files\eleven\eXpurgate`). You are free to change this to suit your installation needs.



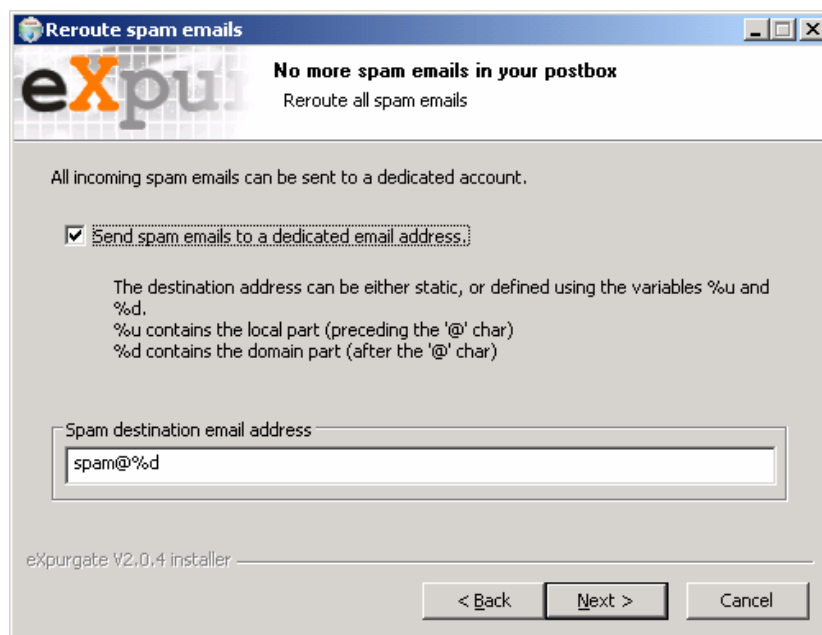
Define the start menu item under which eXpurgate should be listed, then click *Next*.



Under Connection Options, define the port eXpurgate uses to accept incoming e-mail (default: 25). The address and port for eXpurgate to connect to your mail server are defined in *Mailserver Host* and *Mailserver TCP/IP Port*. If eXpurgate and the existing server are to run on the same machine, the port should be changed to one that is not in use. Otherwise, enter the other server's name and the mail server port.

After you have entered the path to the eXpurgate license file and confirmed the entries by clicking on *Next*, eXpurgate will try to establish a connection to your existing mail server on the

specified port. If it can be reached, clicking on *Next* will take you to the next window:<sup>4</sup>



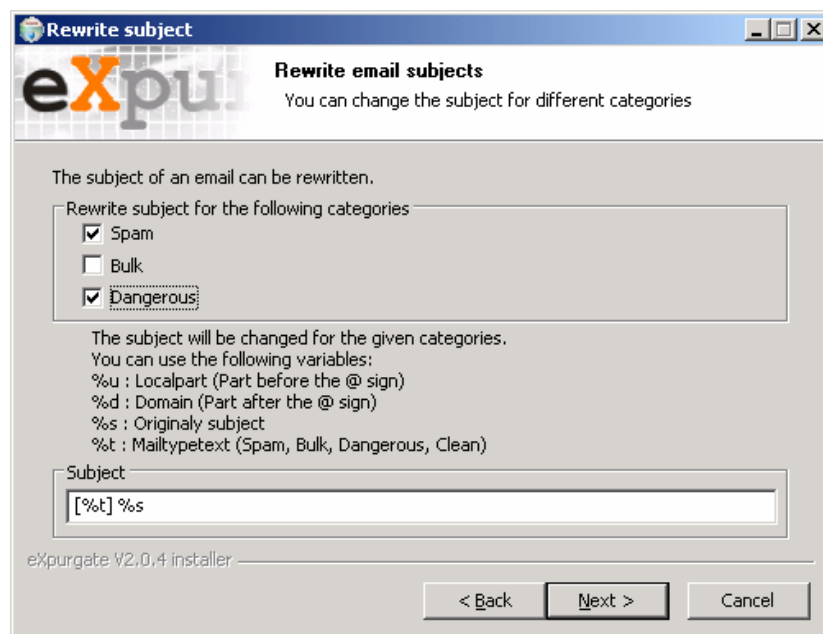
In the *Reroute all spam e-mails* window, you can specify whether all spam e-mail should be forwarded to a single e-mail address. To use this option, please tick the *Send all spam e-mail to one specific e-mail address* box. Enter the address to which the e-mails will be sent. The `spam@%d` specification will forward all e-mail containing spam to the spam e-mail address within your domain (`spam@yourdomain.dom`, for example).

This will forward all e-mail classified as spam to a separate mailbox. Consequently, most of your users will not even see unwanted e-mail, while you can process it in the spam mailbox.

**Please make sure that the e-mail address you enter exists (create it if necessary), otherwise any e-mail that cannot be delivered will be sent back to you together with an error message, thereby possibly worsening your problem.**

Click *Next*.

<sup>4</sup> If the specified mail server is unreachable, eXpurgate will display the error message "Cannot connect to given mailserver on given port". Confirm the message by clicking on *OK*. This brings you back to the previous dialog window. Please check the entries you made/make sure that eXpurgate can contact the specified server. Click *Continue* to try to connect again.



The *Rewrite e-mail subjects* option enables you to rewrite the subject for each incoming bulk e-mail according to its category. As a result, you can see at a glance what sort of e-mail it is, and whether reading it is worthwhile – or dangerous. This method is especially suited for e-mail you wish to check manually after it has been classified by eXpurgate.

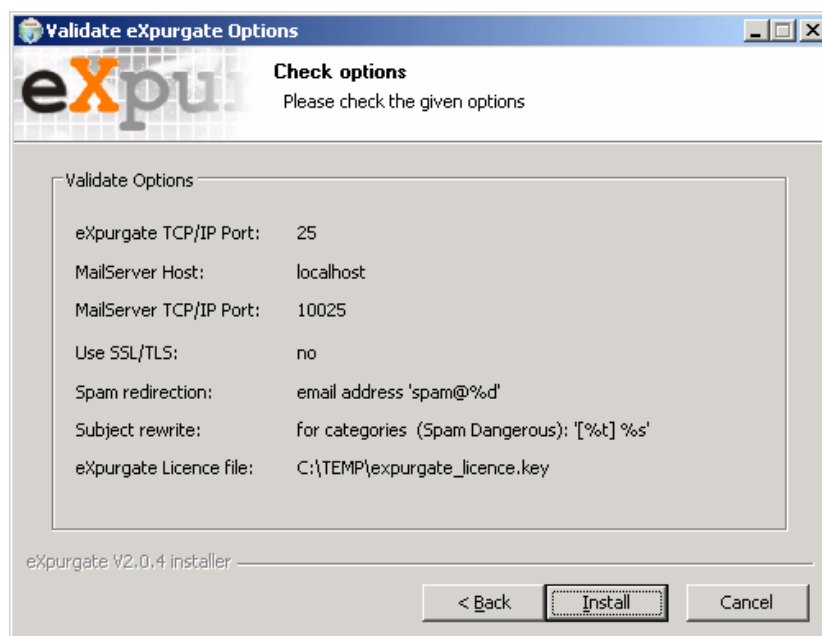
For e-mail classified as *Spam*, *Bulk* and/or *Dangerous*, you can specify as to how the subject line should be rewritten. The default setting `[%t] %s` causes the subject line of an incoming spam e-mail to be rewritten from something like *"Hi Allen, make money fast"* to *"[spam] Hi Allen, make money fast"*, which is much easier to spot and sort.

Click *Next* to set the *SSL/TLS options*. These options enable an encrypted transfer between servers that support the feature. In case you don not wish to use this rather new and uncommon way of transfer, do not modify the default values. Instead, click *Next*.

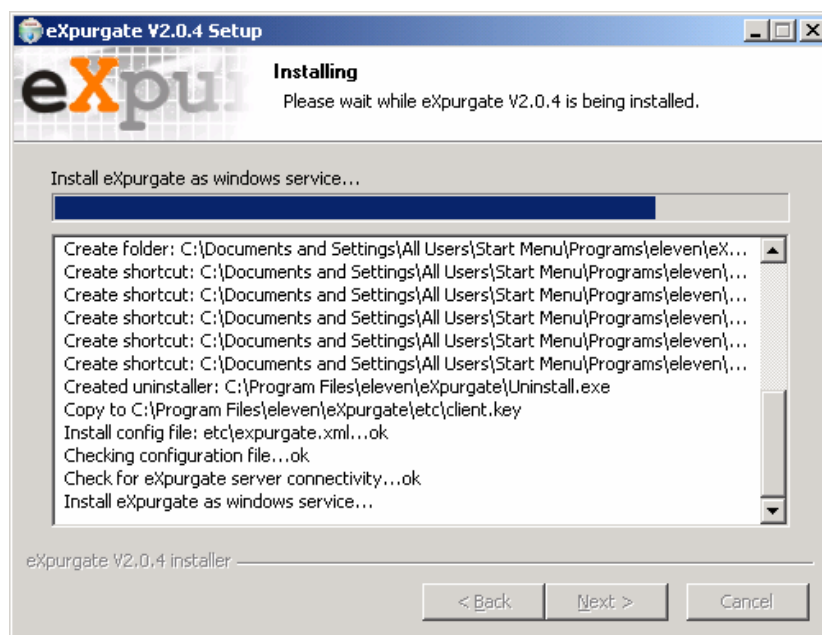


For more information on SSL/TLS, please see the corresponding section below (Section 3.7, p. 25). In order to use the common transfer via SMTP widely used on the internet, there is *no need* for you to enable this option. eXpurgate will work just fine without it.

At the end of the installation process, your specifications are summarized. Please check and correct them if necessary. Afterwards, click *Install*.



eXpurgate will now be installed as a Windows service on your computer according to your specifications and then started.

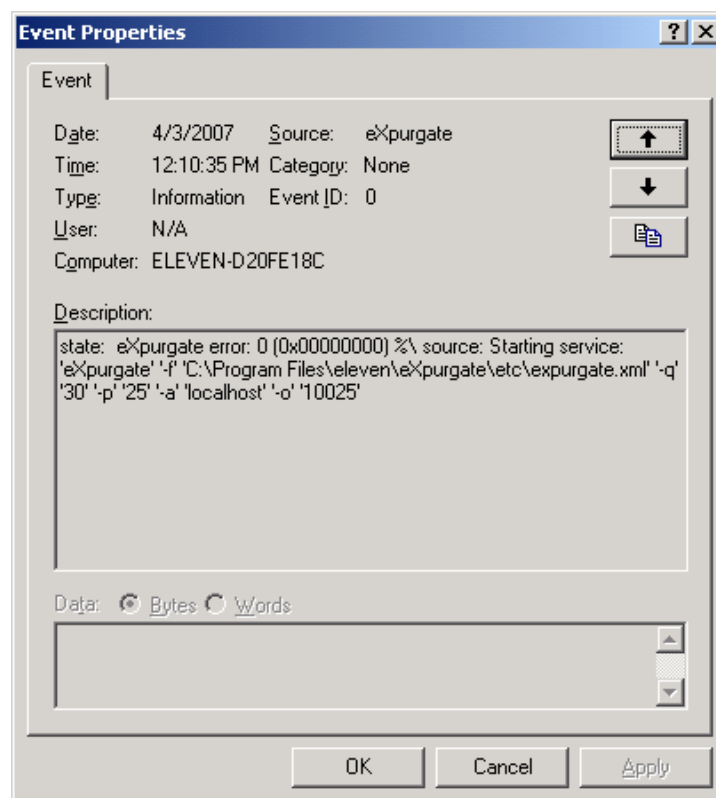


Finally, the setup program checks the connection to the eXpurgate servers (exDBs) of eleven. If the installation was successful, you will see the last step.



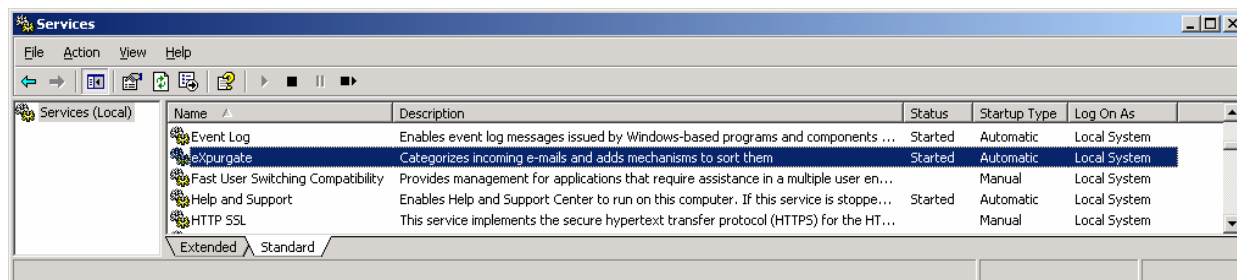
To properly end the installation assistant, click *Finish*. eXpurgate is now properly installed and ready to run.

eXpurgate writes all start events including command line options to the Windows event log (which can be found via Start/Programs/Administration/Event Log). The event log provides you with information in case you encounter errors during installation.



### 2.1.1 Windows service commands

eXpurgate is installed as a service on Windows, so that it is automatically started when the system boots. You can verify this in Start/Programs/Administration/Services.



When eXpurgate is run as a Windows service, the following control parameters can be used:

<code>install</code>	installs eXpurgate as a Windows service without running it. The options to be passed to eXpurgate on startup follow this command.
<code>remove</code>	Uninstalls eXpurgate as a Windows service.
<code>start</code>	Starts the installed eXpurgate service.
<code>stop</code>	Stops the installed eXpurgate service.
<code>isinstalled</code>	Checks whether eXpurgate was installed as a service.
<code>isrunning</code>	Checks whether the service is currently running.
<code>getpath</code>	Returns the path in which the service was installed.
<code>getparameter</code>	Returns the parameters with which the service starts.
<code>setparameter</code>	Sets new startup parameters (analogous to 'install').

### 2.1.2 Changing the TCP port for Microsoft Exchange 5.5

Should you wish to run eXpurgate and Microsoft Exchange 5.5 on the same server, you have to make sure that Exchange accepts e-mails on a port different from 25.<sup>5</sup> Exchange 5.5's SMTP connector takes the port to bind to from the `services` file, which can be found in your Windows directory (%SystemRoot% or C:\WINNT) in `system32\drivers\etc`. You can edit it as follows:

```
notepad %SystemRoot%\system32\drivers\etc\services
```

The underlying structure of the `services` file is as follows:

```
# <Service name> <Port number>/<Protocol> [Alias...] [#<Comment>]
[ ... ]
smtp                25/tcp          mail          #Simple Mail Transfer Protocol
```

Please modify the value after `smtp` (default: 25/tcp) to the number of a new and available port on which Exchange should accept e-mail, for example 10025. Using this as an example, the modified entry in `services` should look like this:

```
smtp                10025/tcp        mail          #Simple Mail Transfer Protocol
```

The service has to be restarted for the change to take effect.

You can test it by using `telnet` (please see chapter 2.1.4).

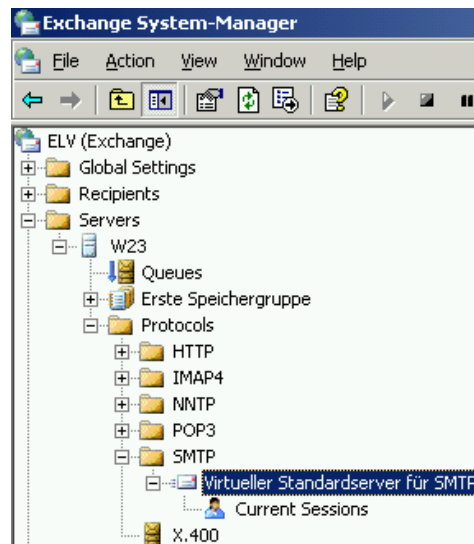
<sup>5</sup> This modification is not necessary if you run eXpurgate and Exchange on different machines, as the two server programs will not have to share port 25 in that case.



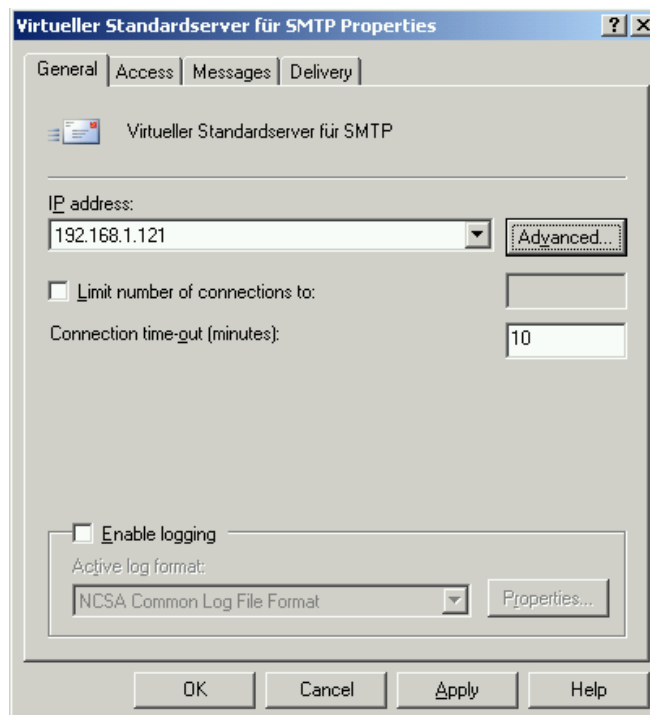
### 2.1.3 Changing the TCP port for Microsoft Exchange 2000 and 2003

Exchange 2000 and 2003 both have a built-in option for changing the port Exchange listens on. To do so, please carry out the following steps:

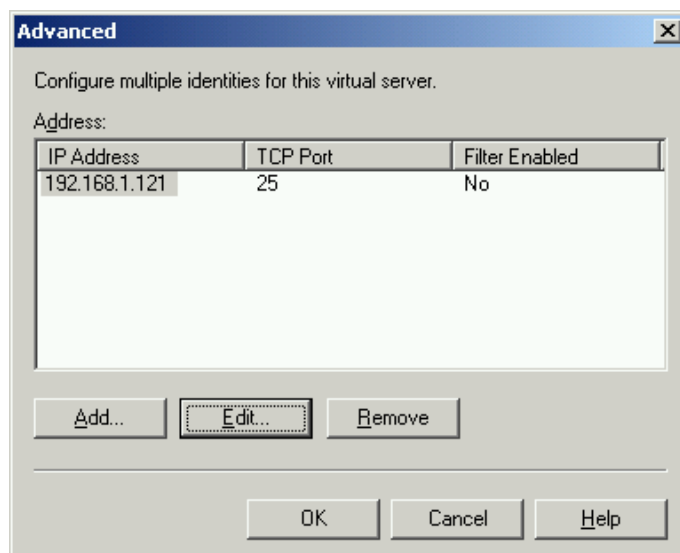
- Open the Exchange System Manager (usually in the start menu in Programs/Microsoft Exchange/System Manager).
- In the System Manager directory, click Server, then on the server in question and in Protocols/SMTP, right-click Virtual Standard Server for SMTP and then on Attributes in the menu that follows.



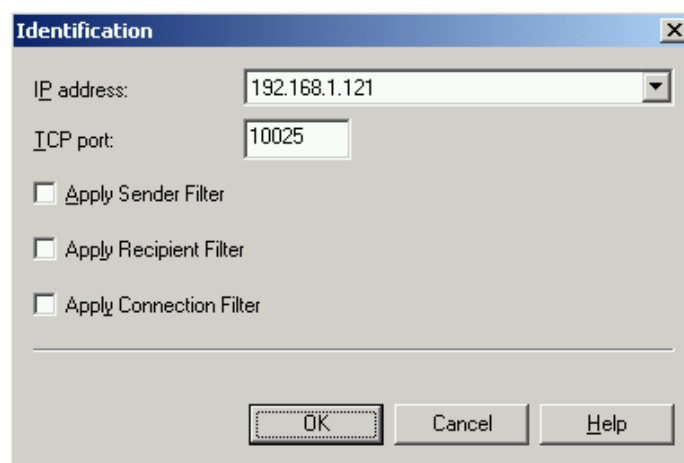
In the "General" tab, select the server's IP address, then click Advanced.



Click Edit to change this virtual server's attributes.



In the TCP connection tab, you can change the port on which Exchange accepts incoming e-mail. Enter a different port which is currently unused, such as 10025, and confirm with **OK**.



By clicking on **OK** again, you will return to the Exchange System Manager. Please stop the virtual server and then start it again. Your Exchange server should now be listening on port 10025. Please read the following section on how to test whether the changes made were successful.

#### 2.1.4 How to test whether Exchange is listening on a port

If you would like to test whether your Exchange server has accepted a port change, you can test this using telnet. Go to the command line and type the following command:

```
telnet 192.168.1.121 10025
```

(instead of 192.168.1.121, please use your Exchange server's IP address; 10025 corresponds to the TCP port you just altered)

Your Exchange server should greet you with a message similar to the following, providing the changes were successful and the virtual SMTP server was restarted:

```
220 W23.intern Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready
```

End the SMTP dialogue with Exchange by typing `quit`. If this test was successful, you can now start eXpurgate on port 25, so that it can forward incoming e-mail to Exchange after classification.

## 2.2 Installing eXpurgate on a Unix system

Should you wish to install eXpurgate on a Unix-based system, please copy the archive for your platform to the root directory '/', and unpack it ("tar -xzvf eXpurgate-1\_1\_1\_Linux\_i686.tar.gz"). eXpurgate will be unpacked and installed in the default directory /usr/local/eleven.<sup>6</sup>

The config file `expurgate.xml` must be placed in the subdirectory `etc` of eXpurgate's install directory for eXpurgate to run. To prevent the file from being overwritten by a newer installation, there's only a file named `expurgate.xml-orig` included (from version 1.3.29). You can copy the file's contents, or rename it to `expurgate.xml` in order to have a working configuration file. You can also edit the file to adjust the settings to your needs.

Afterwards, you will have to run an init script specific for your system. Sample files for various distributions can be found in `etc/init.d` in the eXpurgate installation directory. Please change into the appropriate directory for your system and read the instructions in the `expurgate` script.

In order for eXpurgate to work properly, you have to install your license file. This is expected to be named `client.key` and installed in the `etc` subdirectory in the eXpurgate installation directory. Should it be necessary, you can change the `license` file's name and path in the central configuration file, `expurgate.xml`. To display information on your license, run `./expurgate --testshowlicence --configfile ../etc/expurgate.xml` from the eXpurgate program folder.

This ends the basic installation - the following section will show you how to tailor eXpurgate to your system and start it.

### 2.2.1 Running eXpurgate on Sun Solaris

The features of the Sun Solaris operating system may, under certain circumstances, require you to make some adjustments to the operating system. Depending on the version number, the following patches for the Sparc platform are required:<sup>7</sup>

Solaris 10	No patch required	
Solaris 9	111711-16 (or newer)	32-bit Shared library patch for C++
	112963-30 (or newer)	Linker Patch (32-bit)

The required patches are available from:

<http://developers.sun.com/prodtech/cc/downloads/patches/index.html>

<sup>6</sup> If you prefer a different installation directory (e.g. /opt/expurgate), you need to alter the install-path in `expurgate.xml` (see below).

<sup>7</sup> On the x86-platform, eXpurgate is only available for Solaris 10 (no patches required).

## 3 Configuring eXpurgate

After dealing with the basic installation of the eXpurgate plug-in on your system in the previous section, we would like to show you the various configuration options available to control eXpurgate's behavior.

Configuring eXpurgate is done by parameters which are passed to the program on startup (command-line options) and also by editing the configuration file named `expurgate.xml`. You can find more information on these options in the corresponding chapters of this document.

### 3.1 General command line options

You can control eXpurgate's operation by using the following command line options. These options are for the most part independent of the operating system used. For a list of possible options, please type `expurgate --help`. The short notations set in parentheses were used with older versions of eXpurgate. Currently, they can still be used alternatively, but support for them will be discarded in future versions of the program. Please note that the long options must be preceded by two hyphens ('--'), whereas a single hyphen is used with the short options.

<code>help (h)</code>	Prints the available options (help)
<code>version (v)</code>	Prints the program version
<code>shortversion (V)</code>	Prints a compact summary of the program version
<code>configfile &lt;configfile&gt; (f)</code>	Specifies the configuration file (default: <code>expurgate.xml</code> )
<code>connectiontimeout &lt;secs&gt; (m)</code>	Maximum time for a connection in seconds, 0 for unlimited (default: 300).
<code>datatimeout &lt;secs&gt;</code>	Specifies for how many seconds eXpurgate waits at maximum for data from the communication partner when sending or receiving. If the threshold is reached, eXpurgate closes the connection, issuing a temporary error (value 0 means "no timeout", default: 0)
<code>servermode (s)</code>	Starts the program in the background as a <i>daemon</i> .
<code>spamd (r)</code>	Starts eXpurgate in <i>spamd</i> mode, using the SpamAssassin protocol instead of SMTP.
	For successful classification, the line 'sender:<sender>' is needed in the header of the SpamAssassin protocol. <sender> denotes the MAIL FROM part of the mail envelope used in the SMTP dialogue.
<code>pidfile &lt;pidfile&gt; (P)</code>	Writes the process number of the running eXpurgate server to the file specified.
<code>mlter &lt;socketIdent&gt; (M)</code>	If this parameter is passed to the program, eXpurgate will not communicate via the SMTP protocol but the sendmail mlter protocol and <socketIdent> instead (see 1.3)
<code>mltertimeout &lt;seconds&gt; (T)</code>	libmlter MTA connection timeout (30)
<code>testexit &lt;numofmails&gt; (Y)</code>	For testing purposes only: After the number of e-mails to be processed as specified in <numofmails>, eXpurgate will exit(0).
<code>exdbproxy &lt;port&gt; (N)</code>	Starts an exDB-proxy on the given port.
<code>uid &lt;userid&gt;</code>	Switches to the provided userid (numeric or by name) after a successful start
<code>gid &lt;groupid&gt;</code>	Switches to the provided groupid (numeric or by name) after a successful start

## 3.2 Options when using the SMTP or SpamAssassin protocol

<code>ipaddress &lt;ip/hostname&gt; (i)</code>	The IP address or hostname on which to accept connections (default: 0.0.0.0)
<code>bindport &lt;port&gt; (p)</code>	Binds the server to this port number (default: 11011).
<code>socketqueuesize &lt;size&gt; (q)</code>	If connection queries come in faster than can be processed by the operating system, this is the maximum number of connections which can be buffered (default: 5).
<code>mrtgfile &lt;path&gt; (g)</code>	MRTG Debugfile Path + Fileprefix If this is set, two files are created which include runtime information which can be processed by MRTG (Multi Router Traffic Grapher). The setting is taken to be a filename with a path, to which either <code>'_proc.mrtg'</code> (for the first file) and <code>'_times.mrtg'</code> (for the second file) is added. The files are updated every 60 seconds. The <code>'_proc'</code> file contains the following values: <ul style="list-style-type: none"> <li>- Number of processed e-mails</li> <li>- Active connections</li> <li>- Program uptime in seconds</li> <li>- Description</li> </ul> The <code>'_times'</code> file contains the following values: <ul style="list-style-type: none"> <li>- Elapsed processor time in relation to elapsed time in percent</li> <li>- How often has the maximum process number been exceeded?</li> <li>- Program uptime in seconds</li> <li>- Description</li> </ul>
<code>maxprocesses &lt;maxproc&gt; (x)</code>	Maximum number of running processes, 0 for an infinite number (default: 50)
<code>blockip &lt;iplist&gt; (b)</code>	A comma-separated list of IP addresses and networks with netmask which are not allowed to connect to this program. Alternatively, you can specify the path to a file containing IP addresses. Example of a list of IP addresses: 192.168.1.100, 192.168.2.0/24, 192.168.3.0/255.255.255.0
<code>permitip &lt;iplist&gt; (c)</code>	A comma-separated list of IP addresses or networks with netmasks that are allowed to connect to this program. If this parameter is set, connections are only allowed to be established from computers whose IP addresses correspond to one of the specified addresses. If an address is used as a parameter for both <code>'b'</code> and <code>'c'</code> , it is not permitted to connect ( <code>'b'</code> has a stronger bind than <code>'c'</code> )

### 3.3 SMTP-specific options

<code>smtpouthost &lt;ip/hostname&gt; (a)</code>	Specifies the mail server address for forwarding (default: localhost). If you wish to use several 'target' servers, please also read the next section. Note that eXpurgate <b>will not run</b> if <code>smtpouthost</code> is not specified.
<code>smtpoutport &lt;port&gt; (o)</code>	Specifies the port number on which the server specified in the 'a' option accepts e-mails (default: 10024)
<code>helohostname &lt;hostname&gt; (n)</code>	Hostname that is returned on HELO (default: localhost)
<code>smtpwelcomemsg &lt;message&gt; (w)</code>	SMTP welcome message issued directly after connecting (default: <i>XXX -eXpurgate 2.0.7 (August 13, 2007 11:00:00) eleven GmbH, Berlin/Germany</i> )
<code>allowrelaydomain &lt;List&gt; (k)</code>	If specified, the program only accepts e-mails for the domains listed (comma-separated list or file name). Can and should be supplemented by the 'j' option.
<code>allowrelayip &lt;IPList&gt; (j)</code>	If the 'k' parameter is set, this parameter returns a list of IP addresses which can send e-mail to all domains. Without the 'k' option, this option is void.
<code>smtpmaxrcpts &lt;maxRcpt&gt; (R)</code>	Defines the maximum number of recipients for an e-mail. Should this number be exceeded, e-mail to any further recipients will be refused (default: 250)
<code>validatesmtpenv (u)</code>	The recipient specified in the SMTP envelope is checked on the fly on the destination mail server before the rest of the e-mail is processed. This Option is obsolete, as the envelope check is turned on by default. It can be deactivated by using <code>dontvalidatesmtpenv</code> .
<code>dontvalidatesmtpenv</code>	The envelope data check, turned on by default in this version, can be deactivated by this option. This is especially useful when in a serial arrangement of mail servers the very first mail server has already performed the check. In that case, passing on to the next mail server in the chain is not only pointless, it may also be that the secondary instance is configured with shorter time-out parameters, as it usually gets all mails from localhost within a brief time-span.
<code>passgivenhelo (U)</code>	Results in the hostname as defined in the HELO command being passed to the destination mail server; otherwise the hostname defined by the '-n' option (default: localhost) is used.
<code>noanglebrackets (B)</code>	prevents the e-mail address as specified in the SMTP envelope from being enclosed by angle brackets ("<" and ">").
<code>smtpshortreply (S)</code>	This option sets eXpurgate to only return OK for positive SMTP replies. This may be helpful if your mail server has trouble with eXpurgate's SMTP replies
<code>allowpercenthack</code>	Enables the use of e-mail addresses in the format <code>user%nextdomain.dom@mydomain.dom</code>
<code>allowquotinghack</code>	Enables the use of e-mail addresses in the format <code>"user@nextdomain.dom"@mydomain.dom</code>
<code>allowbangpathhack</code>	Enables the use of e-mail addresses in the format <code>nextdomain.com!user@mydomain.com</code>
<code>allowxforwardip &lt;iplist&gt;</code>	If the <code>allowrelaydomain</code> option is set, then the address variants specified by the above hack options are automatically blocked and can be explicitly re-authorized with these options. Specifically for operation with the Postfix mail server, this option specifies the IP addresses of servers that are allowed to use the postfix command <code>XFORWARD ADDR=w.x.y.z</code> , in order to transmit the IP address of a server, which is sending from an external source, to a back-end instance.
<code>allowxclientip</code>	Accept the XCLIENT extension. See chapter 3.3.2 below

### 3.3.1 Prioritization when using more than one 'target' server

Expanding the possibilities of eXpurgate versions 1.x, you can specify (and prioritize) several 'target' servers with eXpurgate 2.0.

For the delivery/forwarding of e-mails, eXpurgate will always try to use the server ranked highest with regard to priority. Should the highest-ranking server be unreachable, eXpurgate will try to contact the target MTA that ranks next with regard to priority. If several target MTAs have been specified with the same priority, one of them is selected at random.

If you only use *a single* target server, you can specify it (as in eXpurgate v 1.x) using the command line option `-a` (or `--smtpouthost`) for the name or the IP address, respectively, and `-o` (or `--smtpoutport`) for the port, *or* by entering the parameters in `expurgate.xml`.

However, if you wish to use several target servers, you have to enter them in the configuration file `expurgate.xml` in the section `SmtpOutList`, according to the following scheme:

```
<host name="hostname" port="number" priority="number" />
```

The meaning of the parameters above is as follows:<sup>8</sup>

hostname	Name or IP address of the target server. If a name can be resolved to more than one IP addresses, all corresponding IP addresses will be treated with the same port number and Priority
port	Specifies the port number of the MTA on the target server
priority	Specifies the priority of the host as a number with reversed ranking. Analogous to MX entries in DNS, the highest number corresponds to the lowest priority. This means: the lower the number, the more important the server

The following example shows you how to assign different priority to several servers.

```
<SmtpOutList>
<host name="server1a.dom" port="25" priority="10"/>
<host name="192.168.1.125" port="25" priority="10"/>
<host name="backup.dom" port="25" priority="50"/>
</SmtpOutList>
```

### 3.3.2 XCLIENT extension

Starting with version 2.0.5, eXpurgate supports the **XCLIENT Extension** to SMTP. By means of the extension, access control requests can be transmitted in multi MTA filter designs.<sup>9</sup>

When acting as a sender (that is, eXpurgate delivers to the relay), XCLIENT is automatically used if the relay announces the extension during the SMTP dialogue.

In order to make eXpurgate accept the extension when receiving messages, you have to use the command line option `--allowxclientip`, followed by a list of IP addresses or nets. If the option is active, eXpurgate will accept the XCLIENT command from the specified IP addresses. eXpurgate will then also transmit the XCLIENT command to an upstream MTA.

<sup>8</sup> If you make use of both ways at the same time, the server specified in the command line will always have the highest priority. For the sake of lucidity, we recommend you only use one of the methods outlined above.

<sup>9</sup> See [www.postfix.org/XCLIENT\\_README.html](http://www.postfix.org/XCLIENT_README.html)

### 3.4 Logging-specific options

Should you wish to make use of eXpurgate's logging facility, this must be explicitly enabled. You can log to one or several files, or STDOUT, should you so wish. The following parameters control *where* eXpurgate logs, whereas the information priorities control which information is logged (loglevel, see below).

```
logstderr <prio>-<prio>[:...] (E) Logs information pertaining to the specified priorities
                                ("from ... to ...") to STDERR. This option cannot be used with
                                the option '-s' (daemon mode).

logfile <prio>-<prio>:<file> (F) Logs information pertaining to the given priorities to the
                                specified file. In order to log to more than one file, just specify
                                another <prio>-<prio>:<file> range and file, using a
                                colon to separate it from the first entry (see further down for an
                                example).
```

#### Priorities pertaining to information (listed from high to low rank)

EMERG	Errors that occur when starting eXpurgate
ALERT	Serious runtime errors which lead to e-mail processing being aborted
CRIT	Runtime errors which do not lead to e-mail processing being aborted
ERR	Connection error. This includes communication with the eXpurgate servers and e-mail forwarding
WARNING	General warnings, which can also point to possible error sources
NOTICE	Information on the current e-mail, like sender and type
INFO	More information on the current e-mail, for example forwarding mail server responses
DEBUG	Debug information, especially concerning the transfer protocol

For example,

```
--logfile EMERG-ERR:/var/log/expurgate-errors.log
```

has the effect that all notices belonging to the EMERG, ALERT, CRIT and ERR priorities are logged to the file expurgate-errors.log located in /var/log. You can also specify several files for different priorities and thereby control which messages are written to which files. Just make sure you separate the additional entry / entries with a colon:

```
--logfile EMERG-ERR:/var/log/expurgate-err.log;NOTICE-
INFO:/var/log/expurgate.log
```

In case you only wish to log information of *a single* type, you have to specify the desired type twice. If for example you only want to log the type NOTICE, you could accomplish this in the following way:

```
--logfile NOTICE-NOTICE:/var/log/expurgate-notice.log
```

Unix provides you with the following *additional* options:

```
logsyslog <facility>.<prio>-<prio> (L) Passes information in the defined priority area via
                                the specified facility to the Unix syslog daemon (cf. Unix
                                Syslogfacilities). Additional facilities have to be separated by
                                semicolon.

logconsole <prio>-<prio>[:...] (O) Logs information pertaining to the specified priority areas to
                                the system console via '/dev/console'.
```



Feel free to use the following Unix syslog facilities: AUTHPRIV, CRON, DAEMON, FTP, KERN, LOCAL0-7, LPR, MAIL, NEWS, SYSLOG, USER, and UUCP. Should you wish to read more about Unix syslog facilities, please consult the manpage for syslog(3) of your Unix system for more information.

### The *logmailidalways* option

The command line option `--logmailidalways` (introduced with eXpurgate 2.0.4) makes sure that each log entry will additionally carry the ID of the currently processed e-mail as a prefix.<sup>10</sup> The log message itself will remain unaffected by this setting.

#### Example:

```
[2007-04-04 16:16:46.950490] eXpurgate[6425.3084928704] [NOTICE] Process  
handle connect from [127.0.0.1/32:35697]
```

will be issued (when using `--logmailidalways`) as

```
[2007-04-04 16:16:46.950490] eXpurgate[6425.3084928704] [NOTICE]  
ID:070404161646-191946C0-559B8336 Process handle connect from  
[127.0.0.1/32:35697]
```

Thus, it will be much easier to "grep" for log entries relating to a specific e-mail.

## 3.5 Meaning of the logfile entries

For an overview of the logfile entries, please refer to the Support area on [www.eleven.de/support](http://www.eleven.de/support).

## 3.6 Usage of SOCKS

SOCKS may be used to "tunnel" eXpurgate's connections to the central eXpurgate servers from the internal net through the firewall via a specified proxy. eXpurgate supports SOCKS versions 4 and 5. In order to use the SOCKS protocol, you have to enable it in the configuration file `expurgate.xml` by setting the parameter `'usesocks="1"'`. By setting the values of this parameter `<socksProxy>` name, port, SOCKS version, username and password are set. Further information can be found as comments in the configuration file `expurgate.xml`.

## 3.7 SSL/TLS for encrypted e-mail transfer

The TLS function of eXpurgate complies with RFC 2487, i. e. on behalf of the server, STARTTLS is automatically issued as an SMTP extension in reply to "EHLO". The TLS negotiation is initiated as soon as the client sends the STARTTLS command.

On behalf of the client, eXpurgate issues STARTTLS, if this extension has been announced by the server. That means that it will always try STARTTLS if supported by the counterpart, but STARTTLS is not mandatory.

---

<sup>10</sup> Of course, this only applies to log entries that refer to e-mail processing.

TLS support in eXpurgate is limited to encrypting the transfer using STARTTLS. Therefore, a private and a public key (or a self-signed certificate) is needed.<sup>11</sup>

eXpurgate automatically activates TLS, if a private and a public key (certificate) is specified. This can be accomplished by either the command line option (`--usetls`), or by using the configuration file `expurgate.xml`, with the command line option having higher priority.

The private and public key must be compliant with PKCS (Public Key Cryptography Standards), as well as having one of the following file formats:

DER	ASN1-DER-encoded is compatible with PKCS#1 RSAPrivateKey
PEM	A base64-encoded DER format, containing additional headers and footers
PFX	PFX files are X.509 certificate files (self-signed). This format is compatible with PKCS#12 (Personal Information Exchange Syntax Standard)

If the specified private key is encrypted with a password, eXpurgate will query the password upon program start. However, if you enable the option "Cache/store password in a file" (using `--tlspasswordfile`), eXpurgate saves the passwords in the specified file (encrypted). Upon next program start, eXpurgate will not ask you for the password anymore.

In general, the password query is performed using a dialog box under Windows (even if eXpurgate runs as a service), whereas the console is used in Unix.<sup>12</sup>

## Command line options

```
--usetls "<privatekey file>,<certificate file>"
```

or

```
--usetls <self-signed certificate file e.g. PFX/X.509 file>
--tlspasswordfile <file>
```

If you do not provide a password (neither via the command line, nor in `expurgate.xml`), passwords cannot be saved: You will then have to enter the password of the private key every time eXpurgate is started. Further information on how to enable TLS can be found in the configuration file `expurgate.xml`.

## 3.8 Adding 'Received' headers

In SMTP mode, eXpurgate can add Received lines to each incoming e-mail, which can be configured using the `received-header` parameter. Please see the notes and example in the `expurgate.xml` file for a description of the available options.

<sup>11</sup> Please note that certificate management and authentication are not supported, i. e., a host-based authentication is not performed; the public keys of the counterpart will not be verified, and TLS negotiation is simply cooperative.

<sup>12</sup> If eXpurgate starts up automatically under Unix, the password query will be problematic or even impossible. You can fix this by starting eXpurgate at least once from the console, allowing passwords to be saved by means of `--tlspasswordfile <file>`. In the same way, you can fix possible problems with eXpurgate when it is running as a Windows service.

## 3.9 Adapting SMTP messages

All replies of a receiving SMTP server that go to the mail sender consist of a number and an explanatory text (e. g. 220 OK). With eXpurgate.Inhouse, it is now possible to replace the default SMTP messages with your own messages.

To use this function, you have to create a configuration file containing the mapping between the original and the desired message. The file must be text-only, comprising the following:

```
<SMTP message code>: The text to be displayed, with possible %VARIABLES%
```

Note that you only have to define the message codes you wish to modify. That is, a file containing only a single line, like "OK: no problems" is perfectly valid. A sample file listing all possible message codes and their corresponding variables can be found as `SMTPMessages.txt` in the folder `etc`, stored within eXpurgate's program folder.

After you have created the configuration file, you have to enable its usage in eXpurgate by adding the following line to the configuration file, `expurgate.xml`:

```
<setConstString name="smtpMessageFile" value="<path/to/your/file>" />
```

Some message codes contain `%VARIABLES%`, which are analyzed if called up.

## 3.10 The expurgate.xml configuration file

eXpurgate's configuration file, `expurgate.xml`, contains configuration data in the XML format. Editing this file is best done with XML or HTML editors, but you can use other editors such as the Windows Editor (Notepad) or `vi` instead if you prefer. Comments and configuration examples are always enclosed by `<!--` and `-->`. The most important configuration options are explained in the following section; the file itself contains further information.

### eXpurgate installation path

The program path used by eXpurgate is defined by the `installpath` parameter, as seen in the following line:

```
<setconststring name="installpath" value="/usr/local/eleven"/>
```

This line defines the directory in which eXpurgate was installed. Should you wish to change the default directory, the line above has to be modified accordingly.<sup>13</sup>

### Path to the DynamicEngine

The DynamicEngine serves as a kind of "afterburner" for e-mail processing. It can significantly improve the spam recognition rate, especially for new kinds of spam-waves (image-only spam, for instance).

If this feature is turned on (by activating the `useDynamicEngine` option), a directory to be used as a storage for administrative files and run-time information is required. That directory must be

---

<sup>13</sup> When installing eXpurgate on a Windows system, the path is set as follows: "C:/Program Files/eleven/expurgate". Should you wish to modify it manually, please note that you need to use forward slashes ('/') as path separators instead of the usual backslashes ('\\').

writable for the eXpurgate program.

```
<setconststring name="dynamicenginepath" value="{installpath}/dynamic"/>
```

The default configuration will attempt to use a directory named `dynamic` located below the configured `installpath`.

## Setting the language for runtime errors

```
<setstring name="language" value="en"/>
```

In this line, you can set the language eXpurgate uses to issue runtime errors: currently, you can either select English (`en` = default) or German (`de`). Runtime errors contain information that is made visible to the end user. These errors can be due to various reasons, such as:

- the eXpurgate license has expired
- the virus checker could not be contacted, so the e-mail could not be checked for viruses
- others

## Configuring eXpurgate headers

In order for eXpurgate to rewrite the subject line of classified e-mails, you have to make several changes to `expurgate.xml`. Should you wish e-mails belonging to the categories `spam`, `bulk`, `dangerous`, and/or `virus` to reflect this in their subject line, the following lines have to be edited accordingly.

```
<setconststring name="setSpamSubject" value="" />
<setconststring name="setBulkSubject" value="" />
<setconststring name="setDangerousSubject" value="" />
<setconststring name="setDangerousVirusSubject" value="" />
```

If the value enclosed in quotation marks in `value=""` is not empty, the specified text is used for every subject line in the corresponding category. If `value` is empty, the subject line will not be altered. Wildcards can be used which are dynamically replaced by the corresponding text.

<code>%u</code>	corresponds to the part of the e-mail address before the '@', i.e. the user name
<code>%d</code>	corresponds to the part of the e-mail address after the '@', i.e. the domain name
<code>%s</code>	corresponds to the original subject line
<code>%t</code>	eXpurgate category name (clean, spam, bulk, dangerous)
<code>%v</code>	name of detected virus

Example: You would like the subject line of spam messages to be altered so that an e-mail with the subject line *"Hello"* to Fred Bloggs is rewritten to *"spam to fred.bloggs@domain.com Hello"*. This would be configured as follows:

```
<setconststring name="setSpamSubject" value="%t an %u@%d %s"/>
```

## What to do with *bulk.advertising* and *bulk.porn*

Should you wish e-mails belonging to the *bulk.advertising* and *bulk.porn* categories to be treated as spam, you can do this by editing the following line:<sup>14</sup>

```
<setconstinteger name="handleBulkSubsLikeSpam" value="1"/>
```

If you do not wish those e-mail categories to be treated equally, please set value to "0" instead of "1".

## Redirecting bulk e-mail to a central account

Should you wish to forward all bulk e-mail to a central account, the following lines have to be edited. However, you can only use this option when running eXpurgate as an SMTP proxy or milter.

```
<setconstinteger name="sendSpamMailsToOneAccount" value="0"/>
```

Changing "0" to "1" in this line will result in all e-mail classified as spam being sent to a specified e-mail address. It is irrelevant to whom the e-mail was originally addressed: all e-mail classified as spam will be sent to this address. If you wish this function to be active, you **must** also modify the following line.

```
<setstring name="spamMailbox" value=""/>
```

If you wish redirection, you must also edit the `spamMailbox` parameter by adding a valid e-mail address to `value`.

Please make sure the e-mail address you specified is actually present and activated on your server.

## Support for GTUBE

Starting with version 2.0.5, eXpurgate supports the GTUBE test<sup>15</sup> of SpamAssassin. To enable the test, the following line must be inserted into `expurgate.xml` in the section `<mailCheck/>`:

```
<setconstinteger name="obeyGTUBE" value="1"/>
```

Please note, however, that it is **not advisable** to permanently enable the GTUBE test on production systems, as it impairs performance.

---

<sup>14</sup> A description of e-mail categories can be found in the supplement.

<sup>15</sup> Also see <http://spamassassin.apache.org/gtube/>

## 4 Testing eXpurgate's functions

In the following section, we will show you how to use command line options to test your brand new eXpurgate installation. Afterwards, you can find information on how to simulate a running system.

### 4.1 Basic tests of your eXpurgate installation

If you are running eXpurgate on Windows, the two most important tests have already been carried out during installation. However, you are free to run them manually at any time. If you are using eXpurgate on Unix, these tests are not carried out automatically.. Please see the next section on how to test availability of the eXpurgate servers and your existing mail server.

#### Checking the availability of the eXpurgate servers

```
expurgate --configfile etc/expurgate.xml --testexdb
```

As the file `expurgate.xml` contains the eXpurgate servers to use, its name (and possibly its path as well) must be specified.

If the connection fails, "ERROR: [...]" will be issued. In the case of successful connection, "CONNECT: [...]" will be issued, followed by information on the server response time.

#### Checking your mail server's availability

```
expurgate --testsmtpcheckdest --smtpouthost localhost --smtpoutport 10025
```

Tests whether the other mail server is available on localhost using port 10025.

### 4.2 Specific options for testing eXpurgate

The following options are available for testing your eXpurgate installation. They all have one thing in common: the test is run *without starting eXpurgate*.

<code>testconfig (t)</code>	Tests the specified parameters.
<code>testexdb (Z)</code>	Tests the connection to one of the eXpurgate servers specified in the configuration file.
<code>testexdb &lt;eXdbServer&gt; (W)</code>	Tests if the specified eXpurgate Server can be reached.
<code>testshowlicence (l)</code>	Displays information on the license file specified in the configuration file
<code>testshowlicencefile &lt;license file&gt; (z)</code>	Displays information on the specified license file
<code>testsmtpcheckdest (C)</code>	Checks whether the mail server specified for SMTP forwarding is available

### 4.3 Notes on testing eXpurgate's e-mail categorization

eXpurgate does without classic methods of spam recognition such as complex phrase checks ("viagra", "make money", etc.) or checking IP addresses via Real-time Blackhole Lists (RBLs). Instead, eXpurgate mainly checks spam's main distinguishing feature: its *bulk* mail characteristics.

For this purpose, eXpurgate creates a key for each e-mail which enables the system to compare various e-mails to each other as to similarities or degrees thereof, using the eXpurgate database. In combination with further tests this method enables spam to be undisputedly identified. At the same time, it reduces the risk of individual e-mails being wrongly marked to a minimum.

Therefore, eXpurgate is only able to recognize *current* and *unmodified* spam. For performance reasons, eXpurgate uses only recent data. Therefore, it is hard to determine the recognition rate by feeding it archived spam e-mails. When carrying out a test, please make sure that spam fed to eXpurgate is unmodified (i.e., exactly as sent). This is the reason why you cannot test the recognition rate by forwarding a complete directory: On the one hand, most e-mails will be outdated, on the other hand, the e-mails will likely contain data added to them by your e-mail program. Furthermore, inserting a stored e-mail into a freshly composed one will result in the former's header becoming the body of the latter. The e-mail to be tested, along with its checksum, would thus be altered considerably.

To test your setup, you can use the various types of test e-mails that are located in the "mails" directory in your eXpurgate installation directory. For example, you can use these e-mails to test filter and forwarding rules for the individual e-mail types. As far as possible, please ensure that you send these e-mails to eXpurgate in their original unmodified form.

The best and only meaningful way to judge eXpurgate, to our opinion, is to feed it 'real', current mails. This will convince you of the high recognition rate as well as of the typically very low rate of 'false positives'.

## 4.4 Using telnet to check functionality

To check your eXpurgate installation's functionality, you can use `telnet` to simulate the following dialogue between a sending computer and your eXpurgate installation. All you need is a command line<sup>16</sup> In the following example, manual commands are in bold print.

```
telnet localhost 25

220 localhost ESMTP - eXpurgate 2.0.7 (August 13, 2007 11:00:00), eleven
GmbH

helo localhost

250 localhost Hello localhost [127.0.0.1/32]

mail from: <postmaster@localhost>

250 <postmaster@localhost> is syntactically correct

rcpt to: <postmaster@localhost>

250 <postmaster@localhost> is syntactically correct

data

354 Enter message, ending with "." on a line by itself

this is a test
.
250 OK localhost id=040511124439-0360-156D8029 [[OK id=1BNUkb-0000KF-8f]]

quit

221 localhost closing connection
```

To end the message, type a full stop on a line by itself. eXpurgate will then contact eleven's servers in order to classify the e-mail. If this was successful, eXpurgate quits with the code `250 OK` and an ID similar to the one shown above.

---

<sup>16</sup> If you use Microsoft Windows, you can get to the command line via Start/Run by typing `cmd` and pressing Enter.

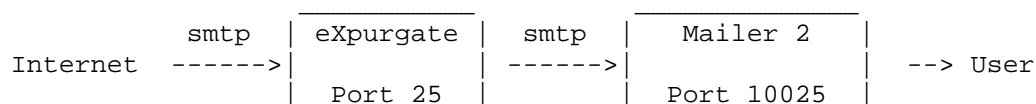


## 5 Integrating eXpurgate in an existing mail system

The following section will provide information on how to integrate eXpurgate in an existing mail system. We would like to apologize should your mail system not be listed here. We are always eager for our documentation to reflect our users' actual needs, but are unfortunately unable to include every system.

### 5.1 Running eXpurgate as an SMTP forwarder

When run as an SMTP forwarder or proxy, eXpurgate communicates with an existing mail server as follows:



To start the service, please change to the directory in which you have installed eXpurgate (cd \program files\eleven\expurgate on Windows or cd /usr/local/eleven/bin/expurgate on Unix, for example), and run it using the following parameters:

```
./expurgate --configfile etc/expurgate.xml --bindport 25
--smtpoutport 10025 --servermode
```

This command starts eXpurgate in daemon mode (`--servermode`). The `--configfile` option sets eXpurgate's configuration file.

eXpurgate binds to port 25 and sends incoming e-mail to a second mailer on port 10025 on the local computer. In order to be able to use those ports, you must run eXpurgate with root or administrator privileges. By use of `--uid` or `--gid`, you can configure eXpurgate to change its userid or groupid, respectively, after a successful start.

The following diagram gives more details about what goes on during the SMTP dialogue when an e-mail is delivered to eXpurgate:

Sender	eXpurgate	Mailer 2
Connect----->		
<-----Welcome (220)		
HELO----->		
<-----Hello (250)		
MAIL FROM----->		
	Connect----->	
	<-----Welcome (220)	
	HELO----->	
	<-----Hello (250)	
	MAIL FROM----->	
	<-----OK (250)	
<-----OK (250)		
RCPT TO----->		
	RCPT TO----->	
	<-----OK (250)	
....		
<-----OK (250)		....
DATA----->		
<-----Enter message (354)		
Sending data----->		
....		
','----->		
	<b>eXpurgate e-mail check</b>	
	DATA----->	
	<-----Enter message (354)	
	Sending data----->	
	....	
	','----->	
	<-----OK (250)	
	-----disconnect-----	
<-----OK (250)		
-----disconnect-----		

As you can see, eXpurgate only returns a success message (OK) when the server to which it passes on the e-mail (Mailer 2 in our example) has actually accepted it. If the check could not be carried out and/or the e-mail could not be sent to the receiving server, the sending server will be notified with an error message.

### 5.1.1 Necessary changes in Postfix when using eXpurgate as a forwarder

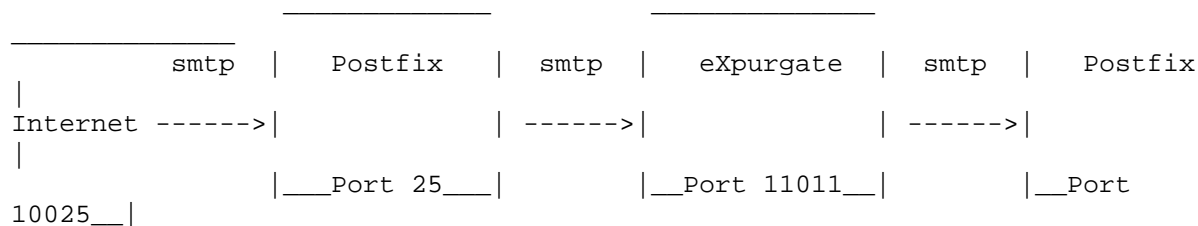
In addition to the instructions of the previous chapter, several changes have to be made when using Postfix. In order for Postfix to "listen on a port different from port 25, its configuration file `master.cf` has to be changed. In this file, you have to find the line starting with "SMTP", and replace "SMTP" with the appropriate port number (e. g. "10025").

In Postfix's configuration file `main.cf`, you have to remove the entry "127.0.0.0/8" from the variable `my_networks`. Unfortunately, this implies that you won't be able to send e-mails from `localhost` to external recipients anymore (sending to your domains will still be possible).

Furthermore, eXpurgate must use the startup option `--smtpout localhost`. Otherwise, it will not deliver its messages using 127.0.0.1, but with the local IP, which may be listed in `my_networks`, thus resulting in an Open Relay.

## 5.2 eXpurgate as a Content\_Filter in Postfix ("Sandwich")

In the following section, we will describe how to integrate eXpurgate with the popular Unix mail daemon in "sandwich" style. Please note, however, that we *strongly advise* you to use the configuration described above (see chapter 5.1/5.1.1) instead of the "sandwich configuration", which can be depicted as follows:



In Postfix, using eXpurgate can be included by using the `content_filter` option. To do so, add the following entries to Postfix's configuration files (usually found in `/etc/postfix`):

Add to `main.cf`:

```
content_filter = smtp:localhost:11011
```

This entry defines a new content filter for Postfix. Postfix will now send incoming messages via SMTP to port 11011 on localhost (which is eXpurgate). Should you use several content filters, please separate them by commas.

Add to `master.cf` (in a single line):

```
localhost:10025 inet n - n - - smtpd -o content_filter= -o
myhostname=localhost
```

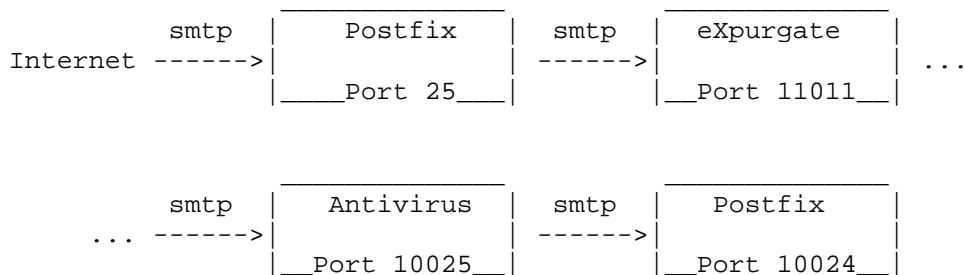
This entry defines a further action for Postfix. It will now listen on port 10025 for incoming SMTP connections. Incoming messages on port 10025 will not be sent to another content filter.

Then start eXpurgate as a daemon on port 11011 using port 10025 for redirection to the second Postfix instance (in a single line).

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 11011 --smtpoutport 10025 --servermode
```

### 5.3 eXpurgate in Postfix with other Content\_Filters, like an antivirus solution

Integrating eXpurgate with an antivirus solution in Postfix is done as in the configuration above. However, the antivirus solution is now another service that needs to be integrated. Communication looks as follows:



Should eXpurgate be used in combination with an antivirus solution, it is recommended to install the latter first, and eXpurgate afterwards. An antivirus solution is installed as a Postfix content filter listening on port 10025 by default. In order to add eXpurgate, the Postfix configuration file `main.cf` has to be modified so as to adapt the content filter port to eXpurgate:

```
main.cf:
content_filter = smtp:localhost:11011
```

This entry defines the content filter for Postfix. Postfix will now send incoming messages via SMTP to port 11011 on localhost, which is eXpurgate. eXpurgate then has to forward the categorized e-mail to the antivirus solution. Thus, the e-mail can be checked for viruses and the like. The antivirus solution sends the e-mail back to Postfix after checking.

In order to run as a content filter for Postfix in combination with an antivirus solution, eXpurgate has to be run with the following parameters (in a single line):

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 11011 --smtpoutport 10025 --servermode
```

Specifically for operation with Postfix, the `allowxforwardip` command line option can be used to indicate the IP addresses, from which servers are allowed to use the Postfix command `XFORWARD ADDR=w.x.y.z`, in order to transmit the IP address of a server, which is sending from an external source, to a back-end instance.<sup>17</sup>

<sup>17</sup> For further information on the XFORWARD command, please see the postfix-FAQ, which can be accessed online, e.g. on: [www.postfix.org/XFORWARD\\_README.html](http://www.postfix.org/XFORWARD_README.html)

## 5.4 Integrating eXpurgate in Exim

There are two ways to integrate eXpurgate into an Exim mailer. eXpurgate can either be run as an SMTP forwarder, much like sendmail, or as a SpamAssassin *spamd*. In the first case, Exim is started using a port different from 25. To do this, the option `daemon_smtp_port` within the Exim configuration has to be set up or modified to a port like 10125.

```
daemon_smtp_port = 10125
```

This results in Exim accepting e-mail on port 10125 as soon as it has been restarted. eXpurgate has to be run in a way that it accepts e-mails on port 25 and passes them on to port 10125 after categorization. Therefore, it has to be started with the following parameters (in a single line):

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 25 --smtpdesport 10125 --servermode
```

Further information on the subject of running eXpurgate as an SMTP forwarder can be found in this document.

Should you wish Exim to send e-mail to eXpurgate using the SpamAssassin protocol, the Exim source code must be patched and recompiled. The patch can be found at <http://duncanthrax.net/exiscan-acl/>. Since version 4.50, the Exiscan patch is included in Exim.

Several options must be set in the Exim configuration file `"/etc/configure"`.

In the `MAIN CONFIGURATION SETTINGS` section:

```
acl_smtp_data = acl_check_content
spamd_address = 127.0.0.1 783
```

This results in content checks being run for every incoming e-mail. 'acl\_check\_content' refers to a new section in the Exim configuration file (see below). The second line specifies the *spamd* to be contacted. Furthermore, the Exim configuration file must be modified to include instructions on what to do with the result of the content check. The `ACL CONFIGURATION` section has to contain the following entries. Unfortunately, the configuration for older versions of Exim and version 4.5 (or newer) is different.

### Older versions of Exim (< 4.5)

```
begin acl
acl_check_content:
  warn message = X-purgate-Report: $spam_score - $spam_report
    Spam = nobody:true
  accept
```

### Exim version 4.5 or newer

```
begin acl
acl_check_content:
  warn message = X-purgate-Report: $spam_score - $spam_report
    spam = nobody:true
  accept
```

These lines specify a header (which includes the categorization result) is inserted into every e-mail.

To start eXpurgate as a *spamd*, the command line must be as follows:

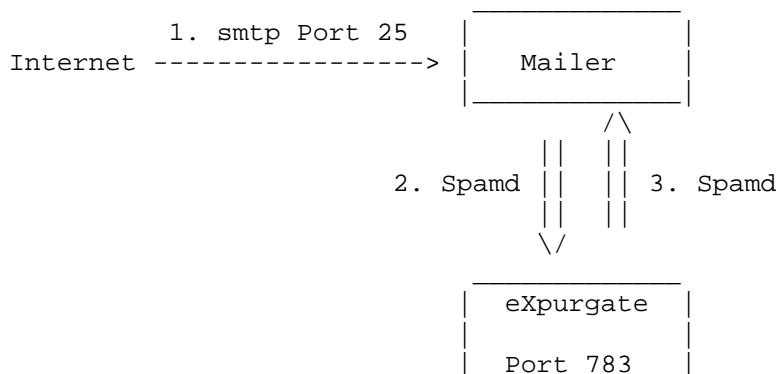
```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml
--bindport 783 --spamd --servermode
```

Further information on running eXpurgate as a SpamAssassin *spamd* can be found in the follow-

ing section.

## 5.5 Using eXpurgate as a SpamAssassin spamd

When run as a SpamAssassin spamd, eXpurgate communicates with the mail server as follows:



Start eXpurgate as a Spam Assassin *spamd* from the command line as follows:

```
expurgate --configfile /usr/local/eleven/etc/expurgate.xml --bindport 783
--spamd --servermode
```

To test this setup, use the SpamAssassin client application *spamc* from the SpamAssassin packet:

```
cat sample-spam.txt | spamc -R
100.0/10.0
X-purgate-Type: Spam
X-purgate-ID: 14123::040603215052-48E4-418BB983
```

In order for eXpurgate to have as high a recognition rate as possible, the spamd protocol should set the 'sender' header to the correct MAIL FROM value from the e-mail envelope.

eXpurgate supports all common spamd commands. eXpurgate answers '*Spam: True ; 1.0/1.0*' to requests if the e-mail in question is spam and '*Spam: False ; 0.0/1.0*' if it isn't. In addition, eXpurgate returns the headers '*X-purgate-Type:*' and '*X-purgate-ID:*' which are usually inserted in the header by the mailer. The '*X-purgate*' header contains the e-mail's category. The '*X-purgate-ID:*' header contains a unique ID which can be used to contact eleven's support department ([report@eleven.de](mailto:report@eleven.de)) should an e-mail have been wrongly categorized.

## 5.6 Integrating eXpurgate in Qmail

Further information on how to setup qmail with SpamAssassin can be found at the following links. eXpurgate can be configured like this too.

[http://sylvestre.ledru.info/howto/howto\\_qmail\\_spamassassin.php](http://sylvestre.ledru.info/howto/howto_qmail_spamassassin.php)

[www.magma.com.ni/~jorge/spamassassin.html](http://www.magma.com.ni/~jorge/spamassassin.html)

[www.gbnet.net/~jrg/qmail/ifspamh/](http://www.gbnet.net/~jrg/qmail/ifspamh/)

[www.pycs.net/lateral/stories/9.html](http://www.pycs.net/lateral/stories/9.html)

## 6 Fine-tuning e-mail processing

With eXpurgate, you can control the filtering on a recipient or domain basis: you can individually enable or disable filtering and reject or delete e-mails classified as spam, virus, outbreak, or dangerous when they are received. We would like to introduce the necessary configuration options in this section.

### 6.1 Global switches

Using the following options, you can define the global default behavior of e-mail processing affecting all users connected to your installation:

```
<setconstinteger name="noExpurgateForAllUsers" value="0"/>
<setconstinteger name="noFreezingForAllUsers" value="0"/>
<setconstinteger name="noVirusCheckForAllUsers" value="0"/>
```

By default, spam check, freezing, and virus check is turned on for all users (i. e., "value" is set to "0"); however, you can explicitly and independently disable the options by setting "value" to "1" for the corresponding option. Usually, globally disabling one or several options only makes sense if you make use of *User Features* (see below) to enable a feature for selected users only.

As a rule, the user features described hereafter are of higher priority than the global switches. You can save yourself some time if you define the global switches that affect most of the users, then make exceptions to the rules for single users where necessary. Thus, the configuration is more clearly to you, and eXpurgate won't have to process large configuration files on each incoming e-mail.<sup>18</sup>

### 6.2 User-specific control of the eXpurgate checks: User Features

You can set the functions spam check, virus check, and freezing separately for each user – independent of the global switches mentioned before. To control the per-user behavior, use the parameters in the config file expurgate.xml described below. In order to use this function, eXpurgate has to be running in SMTP mode – it will not work with eXpurgate configured as Milter or spamd.

User-specific rules are set in text files with the following structure:

```
E-mail address or domain: feature list
```

#### Examples:

```
info@domain1.dom: expurgate
info@domain2.dom: freeze
```

---

<sup>18</sup> Basically, user-specific configuration files are read for each incoming e-mail. This is usually not a problem, as these files are buffered by the operating system. Should they grow very big, however, it is a better idea to permanently load them into your computer's memory. Using the "preLoadAllDB" option will result in eXpurgate loading the files on startup, permanently keeping them in memory. With the option enabled, however, each time you make changes to the list eXpurgate has to be restarted for the changes to come into effect.

To enable user-specific rules, edit the following string in the config file `expurgate.xml`:

```
<setconststring name="userFeaturesDB" value="" />
```

Replace value with the name and path of the recipient-specific configuration file, like in the following example:

```
<setconststring name="userFeaturesDB"
value="{installpath}/etc/userFeaturesDB" />
```

The `userFeaturesDB` file in the folder `etc` (located in eXpurgate's installation directory) must look like this:

```
E-mail address: Feature [Feature]
```

"Feature" can be set to the following:

```
expurgate:      Spam check enabled.
noexpurgate:    Spam check disabled.
viruscheck:     Virus check enabled.
noviruscheck:   Virus check disabled.
freeze:        Freezing enabled.
nofreeze:       Freezing disabled.
```

It is possible to define more than one feature per user. Use commas or blank spaces to separate the features.

### Examples:<sup>19</sup>

```
postmaster@domain1.dom: noexpurgate
chef@domain1.dom: noexpurgate
sales@domain1.dom: noexpurgate noviruscheck
domain2.dom: nofreeze
domain3.dom: noviruscheck
```

E-mails to "chef" and "postmaster" within the domain "domain1.dom" are processed without categorization, those to "sales" will neither be categorized, nor checked for viruses. Furthermore, e-mails to all addresses within the domain "domain2.dom" are not delayed by freezing, whereas all mails to users within "domain3.dom" are not checked for viruses. This way, you can exclude single addresses from the filtering process, and filter all other e-mail for a domain. User-specific features are applied before those for the entire domain, as eXpurgate works through them from high to low specification.

**Please bear in mind that turning off filtering also turns off all the methods mentioned in the following sections. Should you set the `noexpurgate` option for one or more e-mail addresses, the rules mentioned hereafter will not be applied.**

<sup>19</sup> The entries in the `userFeaturesDB` have to be regarded as exceptions to the global rules. In order to run eXpurgate, you do not have to add user features here that are covered by global settings. If for example "Freezing" is globally turned off ("`noFreezingForAllUsers`" `value="1"`), entering "nofreeze" in the `userFeaturesDB` would be redundant. Note, however, that a "double specification" does not have any negative impact on eXpurgate apart from producing bigger configuration files due to additional entries.



## 6.3 Control depending on the sender

### 6.3.1 Handling e-mails from specific sender addresses

Using the `whiteBlackMailFromListFile` option, you can define that certain senders' addresses are *always* to be dealt with in a certain manner, *regardless of their contents*. For this, you have the following functions at your disposal: <sup>20</sup>`spam`, `clean`, `delete`, `reject` and `tagAndDeliver`. To use this option, you need to specify the path and name of a configuration file at

```
<setconststring name="whiteBlackMailFromListFile" value="" />
```

in `expurgate.xml`. For a file named `senderlist.txt` in `/etc/usr/eleven/etc`, it could look like this:

```
<setconststring name="whiteBlackMailFromListFile"
value="{installpath}/etc/senderlist.txt" />
```

The following actions can be used for value:

<code>spam</code>	all e-mail from this sender is treated as "spam"
<code>clean</code>	all e-mail from this sender is treated as "clean"
<code>delete</code>	all e-mail from this sender is deleted
<code>reject</code>	all e-mail from this sender is rejected. At the end of the SMTP dialogue, code 522 is returned together with a plain text message. You can freely define the text as "rejectText" for the individual e-mail types (see 6.5.3)
<code>tagAndDeliver</code>	All e-mails from this sender are subjected to the normal categorization process, thus being classified <i>depending</i> on their contents.

In this way, you can easily have all incoming e-mails that originate from addresses or domains which you know only send spam marked as "spam" *regardless* of the actual content, whereas e-mails from trusted senders or domains can be marked as "clean" without checking. The file should be structured in the same format as in the previous section, looking something like this:

```
trusteddomain.dom: clean
spammer@spamdomain.dom: spam
spammer@spamdomain2.dom: reject
important@trusted.dom: clean
```

E-mails coming from unlisted domains are categorized based on their contents. As a rule, you should only define exceptions for particularly important or annoying sender addresses, otherwise you run the risk of artificial results due to the static nature of the rules.

### 6.3.2 Dealing with E-mails from Specific Sender IP Addresses

As with the analysis of a sender's specified e-mail addresses, `eXpurgate` can also initiate predefined actions based on the IP address of a sending server. With the aid of the `whiteBlackIPListFile` option, you can specify that e-mails from specific sending hosts should, depending on their IP address, always be classified as "spam" or "clean" (regardless of their content), rejected, deleted, or tagged-and-delivered.

To carry out filtering based on the sending host's IP address, you need to specify the path and

<sup>20</sup> Please note that in order to use these mechanisms, contact to `eXpurgate` must be established via SMTP or the Milter protocol.

name of a file containing the IP addresses as the "value" for the `whiteBlackIPListFile` option. The file should be structured in the same format as in the previous section, with one IP address per line. In addition to individual IP addresses, you can also specify network ranges using masks (like 255.255.255.0) or CIDR (e. g. 192.168.1.0/24). The file could therefore be structured as follows:

```
10.11.12.13: clean
192.168.10.0/24: spam
172.16.0.0/255.255.252.0: nofilter
```

In addition to the options based on the sender's e-mail address, you can also use the `nofilter` option for IP-based situations. For example, you could use this option to switch off the filter for local and/or outgoing e-mails by entering the IP address(es) of the local computer or server.<sup>21</sup>

## 6.4 Freezing

By nature, a bulk e-mail cannot be recognized unambiguously as such during the early stages of its circulation. The first e-mails of a spam wave will therefore always be tagged as "clean". To counter this problem and to enhance eXpurgate's recognition rate even further, you can have suspicious e-mails that are not widely circulated yet stopped or "frozen" for a certain amount of time. They can later be "unfrozen" and checked again.

By means of *freezing*, delivery of e-mails susceptible to being bulk e-mail is deliberately delayed for a freely definable period. All incoming susceptible e-mails will be accepted, but they will remain in a queue for a certain amount of time, or until they could be clearly classified. During the freeze period, each frozen e-mail will be checked at fixed intervals by consulting the eXpurgate database servers (exDBs). If in the mean time a classification for the affected e-mail(s) is available from the server, delivery will start according to the rules defined for the respective types. Otherwise, the e-mail will remain queued and checked again later.

Please note that only susceptible e-mails are treated in this way, but not normal (individual) e-mails. Susceptible e-mails make up for only a minor percentage of the total e-mail communication. Extracting the e-mails actually classified "spam" from the group of susceptible e-mails, however, very effectively boosts spam recognition.

### 6.4.1 Prerequisites

Please note that in order to use *freezing*, a special license is necessary. Furthermore, eXpurgate must run in SMTP or proxy mode, as *freezing* does not work in milter or SpamAssassin mode.

Please use the file `expurgate.xml` to activate and configure *freezing*. We would like to briefly introduce the relevant parameters in the next section. Please see the respective notes in the `expurgate.xml` file for further information.

### 6.4.2 Configuration

To enable *freezing*, you have to alter the value of the parameter "`freezingEnabled`" from "0" to "1" (default: 0, disabled)

```
<setconstinteger name="freezingEnabled" value="0"/>
```

---

<sup>21</sup> In milter mode, the IP address corresponds to the address of the delivering, not the sendmail host. In SMTP mode, the IP address of the delivering server is used, unless a different one is transmitted by the XFORWARD command.

The maximum time (in seconds) that an e-mail will be delayed can be set by using the parameter `maxFreezingTime` (default: 3600, corresponding to an hour)

```
<setconstinteger name="maxFreezingTime" value="3600"/>
```

By using `maxNonBusinessHoursFreezingTime`, you can determine for how long e-mails will be delayed out of business hours. Thus, you can improve the recognition rate even further by setting a greater value for times at which usually no (or at least significantly less) e-mail communication occurs. The preset is two hours (7200 seconds).

```
<setconstinteger name="maxNonBusinessHoursFreezingTime" value="7200"/>
```

To specify the time of day that is considered "non business", use the parameters `nonBusinessHoursStart` (defining the start of the period) and `nonBusinessHoursEnd` (defining its end). Those values are given as an integer in 24h notation according to the following formula:

Hours\*10000 + minutes\*100 + seconds. Usually, the period is defined as starting 02:30 AM and ending 07:00 AM.<sup>22</sup>

```
<setconstinteger name="nonBusinessHoursStart" value="23000"/>
```

```
<setconstinteger name="nonBusinessHoursEnd" value="70000"/>
```

The Parameter `freezeCheckInterval` allows you to set the interval at which "frozen" e-mails will be re-checked; the default is ten minutes (600 seconds). For all e-mails in question, a query is issued every ten minutes whether they have been categorized in the meantime.

```
<setconstinteger name="freezeCheckInterval" value="600"/>
```

The parameter `addFreezingHeader` tells eXpurgate to generate a dedicated freezing header, which contains useful information when you want to find out for how long an e-mail was actually frozen:

```
<setconstinteger name="addFreezingHeader" value="0"/>
```

You can set `value` to "0" (off, default) or "1" (on). If the function is enabled, the header line `X-purgate-Freeze: <frozen for, given in seconds>` is inserted in each e-mail that was frozen.

## Options for delivery to the mail server

As it may occur that the actual mail server cannot be reached after "unfreezing" of an e-mail, you can use `"maxAttempts"` and `"intervalMinutes"` to specify the number of attempts and the interval used to establish a connection. If the e-mail still cannot be delivered, the delivery will be attempted again as specified.

```
<setconstinteger name="maxAttempts" value="12"/>
```

```
<setconstinteger name="intervalMinutes" value="5"/>
```

If the delivery still fails, the e-mail would normally be bounced, meaning that the sender would be notified about the failure (please see `"bounceHostAddress"`, `"bounceState"`, and `"bounceSpam"`). As it is generally not a very good idea to notify the (alleged) sender of a suspicious or "spam" e-mail, you can configure this to happen or not. We advise you not to send bounces - especially if the triggering e-mail is "spam".

You can enable or disable the sending of bounces (by eXpurgate!) globally by means of

<sup>22</sup> You can also determine these integers by omitting the usual separators from the usual notations: e.g. 8h 30min 00s or 08:30:00 will produce "83000"

bounceState.<sup>23</sup>

```
<setconstinteger name="bounceState" value="0"/>
```

You control the sending of bounces triggered by "spam" e-mails by means of "bounceSpam". We expressly advise you not to send bounces for e-mails classified as "spam", as they usually have fake entries for their sender, thus the bounce would annoy "innocent bystanders". Therefore, bouncing of spam e-mails is disabled by default.

```
<setconstinteger name="bounceSpam" value="0"/>
```

As a working directory for *freezing*, eXpurgate uses the *spool* folder within the installation directory. There, in addition to the usual files containing the Message-ID ending with -D (Body) and -H (Header), extra files ending with -C and -P are generated. The latter are updated dynamically according to runtime. After restarting eXpurgate, they are re-read, and the *Freezing* (or the "un-freezing") is continued according to the stored status information. After successful "unfreezing" and delivery, those files are deleted.

Please also see the notes on setting freezing on a per-user basis above: 6.2 "User Features" (starting on page 25).

## 6.5 Handling of spam e-mails

With the help of the following options, you can define how an e-mail categorized as spam will be processed. You can reject it, delete it, re-write the subject line, or forward it to a central address or its original recipient. The rules can be set centrally or on a per-user or per-domain basis.

### 6.5.1 System-wide treatment of spam mail

System-wide behavior can be controlled with the "deleteSpamsGlobal", "rejectSpamsGlobal" and "sendSpamMailsToOneAccount" parameters – if you activate one of these options, all recipients are affected.

Should you wish to delete all incoming spam mail (with the exception of those recipients which have the "nofilter" option set), the following option should be set to 1 (default value=0).

```
<setconstinteger name="deleteSpamsGlobal" value="1"/>
```

You can also set spam e-mail to be rejected by setting rejectSpamsGlobal to 1:

```
<setconstinteger name="rejectSpamsGlobal" value="0"/>
```

The junk e-mail sender will receive the message defined in rejectText.

Should you decide to forward all spam mail to a central account, you can activate this option with the help of "sendSpamMailsToOneAccount" by setting the value to 1. Afterwards, the "spamMailbox" parameter has to be set to the address to which the e-mail is to be forwarded.

```
<setconstinteger name="sendSpamMailsToOneAccount" value="0"/>
```

```
<setstring name="spamMailbox" value="spam%d"/>24
```

In order to use system-wide spam rules, contact to eXpurgate must be established via SMTP or Milster.

<sup>23</sup> What's more, you can specify the host and port used for sending bounces, as well as the HELO that eXpurgate uses when contacting the server (cf. expurgate.xml).

<sup>24</sup> Please refer to the supplement for a list of available variables.

## 6.5.2 User-specific processing of e-mail

Setting the parameter below as follows

```
<setconststring name="spamActionsForUserInFile" value=
"${installpath}/etc/useractionlist.txt"/>
```

enables you to control how incoming spam mail is processed on a per-user basis. You can delete, reject, or categorize and then deliver e-mail. "value" has to be set to the path and the name of the file containing user-specific data.

The structure for user-specific configuration files (useractionlist.txt in our example) corresponds to the familiar pattern:

```
user1@domain1: reject
user2@domain2: delete
domain3: tagAndDeliver
```

Initially, the complete e-mail addresses are searched. If a "hit" is found, the corresponding method is used. If no hits are found, the rules for the domain are applied.

## 6.5.3 Configuring the Reject text

Whenever eXpurgate rejects an e-mail, the sending server receives code 552, followed by an error message. The "rejectText" parameter enables you to set the error message text to whatever you wish.

```
<setconststring name="rejectText" value="This e-mail is considered spam,
the server is rejecting it."/>
```

For further information, please read the central configuration file `expurgate.xml`.

## 6.6 Handling of virus e-mails

*Please note: Virus detection requires the use of AntiVir SAVAPI, which must be separately installed and licensed. You also need a special eXpurgate license key to unlock this additional functionality within eXpurgate.<sup>25</sup>*

Using the same methods as those used for spam e-mails, it is also possible to reject, redirect or delete e-mails that contain viruses and/or to change their subject lines, on either a global or a per-user basis. AntiVir SAVAPI must be installed and started as a service before it can be used with eXpurgate.

To activate virus scanning via eXpurgate, the "value" for the following parameter in the `expurgate.xml` file must be changed from "0" (default) to "1":

```
<parameter name="ActivateVirusChecker" value="1"/>
```

You also need to specify the directory in which the SAVAPI files required by eXpurgate were installed by modifying the following lines in `expurgate.xml` accordingly:

---

<sup>25</sup> If you are already using an antivirus solution, you will unfortunately not be able to use it together with eXpurgate in the way described here, as these functions are based exclusively on AntiVir-SAVAPI. You can, however, use the existing antivirus solution as before to detect viruses. In this case, a virus being detected by the antivirus solution will not affect the classification by eXpurgate (which would be dangerous.virus). If your antivirus solution features real-time file system protection, you should exclude the eXpurgate spool folder from examination.

```

<parameter name="AntiVir_windows_loadLibrary" value="C:/Program
Files/H+BEDV/AntiVir SAVAPI/SAVAPI.DLL"/>

<parameter name="AntiVir_windows_AVEWIN32.DLL" value="C:/Program
Files/H+BEDV/AntiVir SAVAPI/AVEWIN32.DLL"/>

<parameter name="AntiVir_windows_ANTIVIR.VDF" value="C:/Program
Files/H+BEDV/AntiVir SAVAPI/ANTIVIR.VDF"/>

<parameter name="AntiVir_windows_HBEDV.KEY" value="C:/Program
Files/H+BEDV/AntiVir SAVAPI/HBEDV.KEY"/>

```

In addition, you can use the `scanEveryEMailForViruses` parameter to specify whether every e-mail (value=1) should be scanned for viruses, or only those e-mails that have attachments (value=0, default). In practice, it should be sufficient to only scan attachments for viruses, since this is beneficial in terms of performance.

Once eXpurgate has been restarted, it will also be capable of classifying e-mails with viruses as *"dangerous.virus"*.

Please also see the notes on setting the freezing function on a per-user basis above: 6.2 "User Features" (starting at page 25).

## 6.7 Advanced options for processing individual E-mail types

For e-mails classified as spam, virus, virus-outbreak, or dangerous, you have the following global options: delete, reject and forward to a central address, change subject line, and user-specific rules.

You control how these types of e-mails are processed in the corresponding sections of the `expurgate.xml` file. The available options are modeled on the options for processing spam e-mails described in detail in the previous section.

The following global options each have an effect on all the mail server's recipients, while the user-specific options allow you to control processing on the basis of individual recipients. To activate these options, change the default value "0" (disabled) to "1" (enabled) and restart eXpurgate.

```

delete<email type>Global
reject<email type>Global

```

Delete: incoming virus e-mails will be deleted

Reject: mails of the relevant type are rejected with a 552 error upon receipt. You can define the text that the sender will receive in `<email type>RejectText` (default: "This e-mail is `<email type>`. Therefore, the server rejects it."). This option is only available if eXpurgate is run as an SMTP proxy.

```

send<email type>MailsToOneAccount

```

Redirect: mails are routed to a central address regardless of their original target address, so that they can be checked by an administrator, for example, and kept from reaching users' mailboxes. You can set the redirection address using `"<email type>Mailbox"`. You can either input this as a static value or use the variables `%u` and `%d` to make it dependent on the original recipient (local part) or the original domain. It is also possible to employ combinations of fixed and variable components, such as `virus-%u@%d`.

In addition to the global rules, eXpurgate can also process mails on the basis of user-based rules. You can define these rules using the file specified in `"<email type>ActionsForUserInFile"` using the same familiar format. This enables you to delete, reject, or tag and deliver the specified mail types for individual addresses or domains.

The following overview shows the names of the parameters for the various e-mail types.

e-mail type / parameter	delete	reject	redirect	to mailbox	user-specific actions
<b>spam</b>	deleteSpamsGlobal	rejectSpamsGlobal	sendSpamMailsToOneAccount	spamMailbox	spamActionsForUserInFile
<b>virus</b>	deleteVirusesGlobal	rejectVirusesGlobal	sendVirusMailsToOneAccount	virusMailbox	virusActionsForUserInFile
<b>virus-outbreak</b>	deleteOutbreakGlobal	rejectOutbreakGlobal	sendOutbreakMailsToOneAccount	outbreakMailbox	outbreakActionsForUserInFile
<b>dangerous</b>	deleteDangerousGlobal	rejectDangerousGlobal	sendDangerousMailsToOneAccount	dangerousMailbox	dangerousActionsForUserInFile
<b>bounce</b>	-	-	sendBouncesMailsToOneAccount	bouncesMailbox	-

## 6.8 Turning off sub-categories of "dangerous"

All sub-categories of the type "dangerous" can be turned off except for *dangerous.virus*, *dangerous.virus-outbreak*, and *dangerous.attachment* by defining

```
< setconstinteger name="turnOffDangerousSubs" value="1" >
```

in `expurgate.xml`. Thus, e-mails with *potentially* dangerous content will not be tagged as "dangerous" anymore, but e-mails with definitely or potentially dangerous (executable) attachments, e. g. viruses or so-called worms, still will be tagged and treated as "dangerous".

## 6.9 Treating "suspect" as "clean"

In order to mark e-mails of the type "*suspect*" as "*clean*", you can change the parameter's

```
< setconstinteger name="handleSuspectAsClean" value="1" >
```

value to "1" (default). E-mails classified as "*suspect*", i. e. which could not be securely assigned to any category, will be tagged and treated as "*clean*". Therefore, the classification "*suspect*" cannot be misinterpreted as problematic or even Spam by the recipients anymore.

## 6.10 Dealing with Bounce E-mails

eXpurgate detects bounce e-mails (i.e., e-mails that are rejected by other servers and returned to the supposed sender) and can process them separately. Bounce e-mails can be forwarded to a central address specified under `bouncesMailbox` with the aid of the parameter `sendBouncesMailsToOneAccount`. You can also use `setBouncesSubject` to modify the subject line.

Due to the general usefulness of bounce e-mails, which normally, of course, indicate technical problems in sending e-mails, it is not possible to delete or reject these, even if they prove to be annoying during a wave of worms, for example.

## 6.11 Treating certain sub-categories of "clean" as spam

If you like, empty or almost empty e-mails can be tagged and treated as *"spam"*. Please note that even empty e-mails can transport information under certain circumstances. By using the following options, you can configure the empty (*"clean.empty"*) and almost empty (*"clean.emptybody"*) e-mails to be treated as *"spam"*. The categories differ as follows:

*clean.empty*

Emails that are completely empty. The only information they can transport is the fact of their receipt. However, even those e-mails may be useful and relevant under certain circumstances (e.g. for testing purposes or debugging). To treat e-mails of this type as *"Spam"*, you should set the value 1 (default) for **"handleEmptyLikeSpam"**.

*clean.emptybody*

Emails with no content in the body and without any attachment. They still may contain valuable information in the subject line. To treat e-mails of this type as *"Spam"*, you should set the value 1 (default: 0) for **"handleEmptyBodyLikeSpam"**.

*clean.almostempty*

Emails with only little content in their body (up to 12 characters), or with *"invisible"* text. To treat e-mails of this type as *"Spam"*, you should set the value 1 for **"handleAlmostEmptyLikeSpam"**.



## 7 Using eXpurgate statistics

The eXpurgate statistics function gives you the opportunity to receive a statistical view of how the individual mail types are distributed. First of all, you have to connect to <https://www.eleven.de/settings/actions/customers/> with your user name and password. Choose the statistics option to select which period to show statistics for.

☐ Show data since yesterday
 ☐ Show mail volume

☒ Show the last week

☐ Show the last month

☐ Show the last 3 months

☐ Show the specified time range  
 from  to   
format: YYYY-MM-DD (e.g. 2004-12-31)

---

Statistics generated at: 2007/2/26 16:34:03 (Mail count)

[Download Excelfile](#)

Mailtypes	Count	%	Avg. count/day
Clean	36.933	13.3	4616.6
Spam	221.277	79.7	27659.6
Bulk	12.755	4.6	1594.4
Bulk.Advertising	623	0.2	77.9
Bulk.Porn	12	0.0	1.5
Suspect	18	0.0	2.3
Clean.Empty	63	0.0	7.9
Clean.Almost-empty	0	0.0	0
Clean.Empty-body	306	0.1	38.3
Clean.Bounce	1.181	0.4	147.6
Dangerous	0	0.0	0
Dangerous.Virus	2.742	1.0	342.8
Dangerous.Attachment	25	0.0	3.1
Dangerous.Code	47	0.0	5.9
Dangerous.IFRAME	11	0.0	1.4
Dangerous.Virus-Outbreak	1.663	0.6	207.9
<b>Total</b>	<b>277.656</b>		

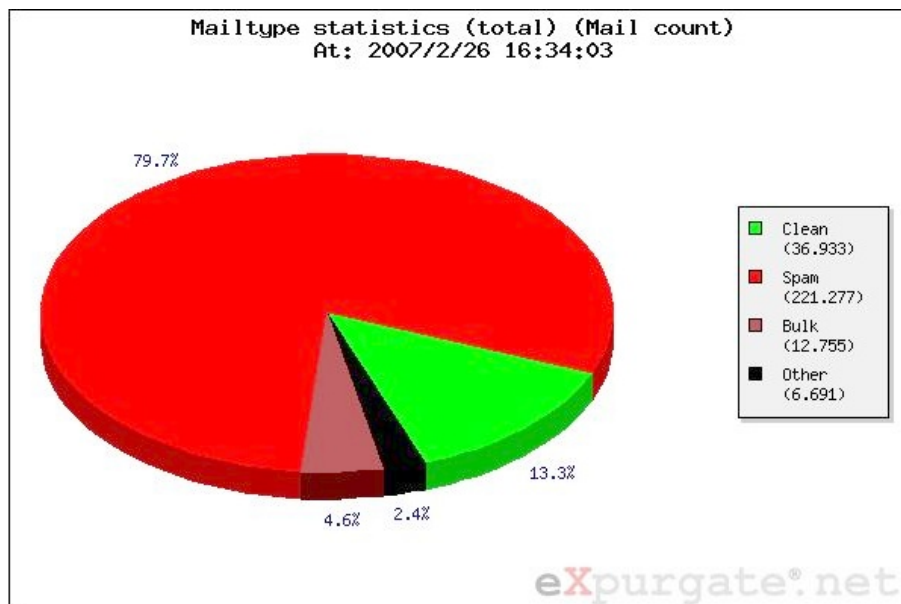
with just a few e-mails	with many e-mails
2479	2899

Mark "**Show the last week**", for example and click "**Submit Query**" to confirm, to see how your e-mails were distributed among the various categories over the past week.<sup>26</sup> The data is presented in three ways: as a spreadsheet, a pie chart and a line chart. You can download the spreadsheet details as an Excel file to use them for your own calculations or presentations.

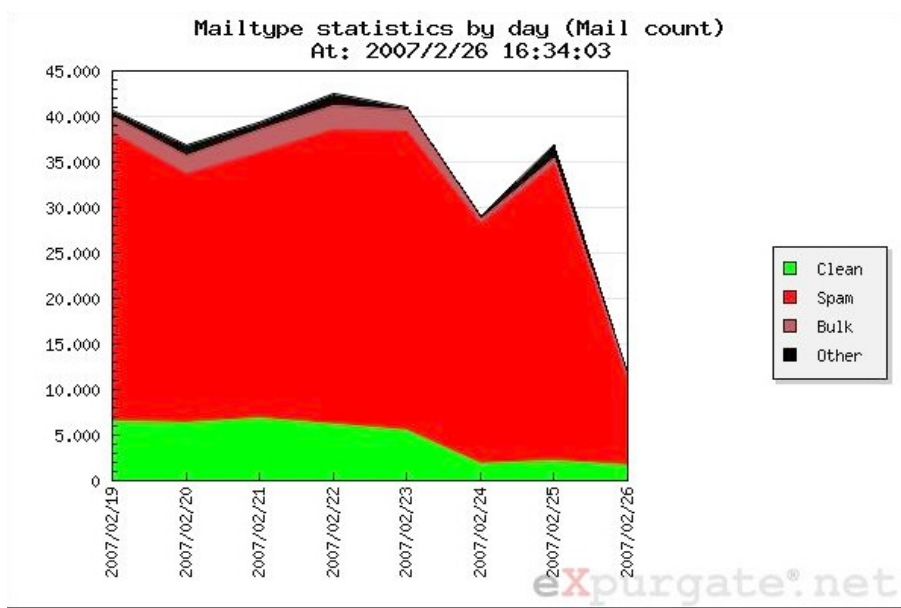
<sup>26</sup> Please note that processing the query (especially its graphical representation) may take several minutes, depending on the e-mail volume.

One thing the different presentation forms have in common is that the absolute number of incoming e-mail types and their percentage related to all e-mails is shown in color. This enables you to see at a glance how high the content of "useful" or "clean" e-mail is in relation to "less wanted" or even "unwanted" e-mail.

### Pie chart of e-mail types



### Line chart of e-mail types



## Supplement

### eXpurgate's e-mail categories

eXpurgate tags every e-mail with one of the following categories:

<code>clean</code>	Without any suspicious characteristics
<code>bulk</code>	Sent in bulk, e. g. newsletters
<code>spam</code>	Identified as a spam or phishing e-mail
<code>suspect</code>	Having one or more characteristics typical for "spam" or "bulk" e-mails, but not identified as such
<code>dangerous</code>	Containing code or attachments which are potentially dangerous
<code>dangerous.attachment</code>	E-mails containing an executable attachment
<code>dangerous.code</code>	E-mails containing potential dangerous content, e.g. references to local files
<code>dangerous.iframe</code>	E-mails using the iframe feature (For example, an embedded iframe in an e-mail message could be used to run some script to gain access to the local file system for reading or deleting files)
<code>dangerous.virus</code>	Containing one or more identified virus(es) (optional "virus check" is required)
<code>dangerous.virus-outbreak</code>	E-mails that most likely contain a new virus (not yet recognized by virus detection as they only recently emerged; optional "virus check" is required)
<code>bulk.advertising</code>	"Valid" – but generally unwanted – advertising e-mails
<code>bulk.porn</code>	E-mails with pornographic content which are not "spam" (e.g. pornographic newsletters)
<code>clean.empty</code>	E-mails without any content in subject or body, thus being completely without content
<code>clean.emptybody</code>	E-mails without any content in their body, but with content in the subject line
<code>clean.bounce</code>	E-mails that were returned to sender due to a delivery failure

Additional categories planned for future versions.

eXpurgate tags e-mails by adding entries to the header section. Some of these entries contain information about the category and/or sub-category. Thus, these entries may be used to filter or sort e-mails .

## IP nets of eXpurgate servers

At present, two nets are used exclusively by eleven GmbH for the eXpurgate service. They are documented in the public RIPE database as follows:

```
inetnum:      195.190.135.0 - 195,190,135,255
netname:      ELEVEN-NET
descr:        eleven GmbH
descr:         Germany
country:      DE
admin-c:      COLT2-RIPE
tech-c:       RR831-RIPE
status:       ASSIGNED PI
```

```
inetnum:      194.145.224.0 - 194,145,224,255
netname:      ELEVEN-NET2
descr:        eleven GmbH
country:      DE
org:          ORG-EA76-RIPE
admin-c:      RR831-RIPE
tech-c:       ERR11-RIPE
status:       ASSIGNED PI
```

## Licenses

eXpurgate uses the following licenses:

### *OpenSSL*

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (see [www.openssl.org](http://www.openssl.org)).

### *Expat*

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002 Expat maintainers.

### *Regex Lib*

Copyright (c) 1998-9 Dr John Maddock



eleven – Gesellschaft zur Entwicklung und Vermarktung von Netzwerktechnologien mbH

Hardenbergplatz 2 // 10623 Berlin // Germany

fon: +49 30 / 52 00 56 - 0 // fax: +49 30 / 52 00 56 - 299

e-mail: [info@eleven.de](mailto:info@eleven.de) // <http://www.eleven.de>

