

# eleven Documentation

## ■ eXpurgate.Inhouse (SMTP)

### eleven support

+ 49 30 - 52 00 56 130  
support@eleven.de

### eleven distribution

+ 49 30 - 52 00 56 210  
sales@eleven.de

### postal address

eleven Gesellschaft zur Entwicklung und Vermarktung  
von Netzwerktechnologien mbH  
Hardenbergplatz 2, 10623 Berlin, Germany

© eleven Gesellschaft zur Entwicklung und Vermarktung von  
Netzwerktechnologien mbH.

This document contains confidential information.  
All rights reserved. Distribution and reproduction – even  
in excerpts – without prior written consent by eleven are  
prohibited.

# Contents

|   |           |
|---|-----------|
| <b>1. Introduction</b>  | <b>5</b>  |
| 1.1. How eXpurgate.Inhouse works . . . . .                                  | 6         |
| 1.2. The eXpurgate principle . . . . .                                      | 7         |
| <b>2. Installing eXpurgate</b>  | <b>9</b>  |
| 2.1. Installing eXpurgate SMTP on a Unix system . . . . .                   | 9         |
| 2.1.1. Installation and removal of the packages . . . . .                   | 9         |
| 2.1.2. Activating and deactivating the service . . . . .                    | 11        |
| 2.1.3. Starting and stopping the service . . . . .                          | 12        |
| 2.1.4. Connectivity test . . . . .  | 12        |
| 2.1.5. Further Remarks . . . . .  | 13        |
| 2.2. Installing eXpurgate on a Windows system . . . . .                     | 14        |
| 2.2.1. Windows service commands . . . . .                                   | 24        |
| 2.2.2. Changing the TCP port with Microsoft Exchange 5.5 . . . . .          | 24        |
| 2.2.3. Changing the TCP port with Microsoft Exchange 2000 or 2003 . . . . . | 25        |
| 2.2.4. Test whether Exchange responds to a port . . . . .                   | 30        |
| <b>3. Configuring eXpurgate</b>   | <b>31</b> |
| 3.1. Command line options . . . . .   | 31        |
| 3.1.1. Information output options . . . . .                                 | 32        |
| 3.1.2. Options for operation on Unix . . . . .                              | 32        |
| 3.1.3. Options for logging of log messages . . . . .                        | 32        |
| 3.1.4. Options for testing eXpurgate . . . . .                              | 34        |
| 3.1.5. General functionality options . . . . .                              | 34        |
| 3.1.6. SMTP server options . . . . .  | 35        |
| 3.1.7. Options for downstream SMTP relays . . . . .                         | 35        |
| 3.1.8. Options for the Spam-Engine . . . . .                                | 35        |
| 3.1.9. Virus scanner configuration options . . . . .                        | 36        |
| 3.1.10. Options for the Simple Network Management Protocol . . . . .        | 36        |
| 3.1.11. Freezing options . . . . .  | 36        |
| 3.2. The configuration file . . . . .                                       | 36        |
| 3.2.1. General settings . . . . .   | 38        |
| 3.2.2. Logging . . . . .  | 40        |
| 3.2.3. SMTP server . . . . .  | 43        |
| 3.2.3.1. Local domains . . . . .  | 46        |
| 3.2.3.2. Access control . . . . .   | 47        |
| 3.2.3.3. Querying DNS Blacklists . . . . .                                  | 48        |
| 3.2.3.4. Bounce Address Tag Validation (BATV) . . . . .                     | 48        |
| 3.2.3.5. Sender Policy Framework (SPF) . . . . .                            | 50        |
| 3.2.3.6. Authentication via SMTP AUTH . . . . .                             | 51        |
| 3.2.3.7. SMTP protocol messages . . . . .                                   | 51        |
| 3.2.4. SMTP relay . . . . .   | 52        |
| 3.2.5. TLS . . . . .  | 55        |

|           |  |           |
|-----------|--|-----------|
| 3.2.6.    | Spam recognition . . . . .                                   | 58        |
| 3.2.6.1.  | Subsection Antivir . . . . .                                 | 59        |
| 3.2.6.2.  | Subsection NoFilter . . . . .                                | 61        |
| 3.2.7.    | Freezing . . . . .   | 62        |
| 3.2.8.    | Simple Network Management Protocol (SNMP) . . . . .          | 64        |
| 3.2.9.    | Lightweight Directory Access Protocol (LDAP) . . . . .       | 66        |
| 3.2.9.1.  | Queries for an LDAP server . . . . .                         | 67        |
| 3.2.10.   | eXelerate . . . . .  | 68        |
| 3.2.10.1. | Local Domains Query . . . . .                                | 69        |
| 3.2.10.2. | Recipient Validation Query . . . . .                         | 70        |
| 3.2.10.3. | Blacklist Query . . . . .                                    | 71        |
| 3.2.10.4. | BATV Policy Query . . . . .                                  | 71        |
| 3.2.10.5. | TLS Policy Query . . . . .                                   | 72        |
| 3.2.10.6. | TLS Store Query . . . . .                                    | 73        |
| 3.2.10.7. | User Feature Query . . . . .                                 | 74        |
| 3.2.10.8. | Mail Action Query . . . . .                                  | 75        |
| <b>4.</b> | <b>Fine tuning e-mail handling</b>                           | <b>77</b> |
| 4.1.      | Processing rules . . . . .                                   | 77        |
| 4.2.      | Defining a recipient . . . . .                               | 77        |
| 4.2.1.    | Selecting by domains . . . . .                               | 78        |
| 4.2.2.    | Selecting by recipients . . . . .                            | 78        |
| 4.3.      | Features . . . . .   | 79        |
| 4.3.1.    | Feature Spam . . . . .                                       | 79        |
| 4.3.2.    | Feature Virus . . . . .                                      | 79        |
| 4.3.3.    | Feature Outbreak . . . . .                                   | 80        |
| 4.3.4.    | Feature Freezing . . . . .                                   | 80        |
| 4.4.      | Define e-mail processing . . . . .                           | 80        |
| 4.4.1.    | Category-based rules . . . . .                               | 83        |
| 4.4.2.    | Sender-based rules . . . . .                                 | 84        |
| 4.4.3.    | Actions for IP addresses, senders and e-mail types . . . . . | 85        |
| 4.5.      | Application examples . . . . .                               | 85        |
| 4.5.1.    | Whitelisting . . . . .                                       | 85        |
| 4.5.2.    | Blacklisting . . . . .                                       | 86        |
| 4.6.      | Substitutions . . . . .                                      | 86        |
| 4.7.      | Limits . . . . .   | 88        |
| 4.8.      | Default settings . . . . .                                   | 88        |
| 4.8.1.    | Adding a header . . . . .                                    | 88        |
| 4.8.2.    | Features . . . . .   | 88        |
| 4.8.3.    | Delivery . . . . .   | 88        |
| <b>5.</b> | <b>Testing eXpurgate</b>                                     | <b>89</b> |
| <b>6.</b> | <b>eXpurgate reporting</b>                                   | <b>90</b> |
| <b>A.</b> | <b>Appendix</b>  | <b>91</b> |
| A.1.      | Best Practice Empfehlungen . . . . .                         | 91        |
| A.2.      | Example file . . . . .                                       | 92        |
| A.3.      | eXpurgate categories . . . . .                               | 95        |
| A.4.      | Variables . . . . .  | 96        |
| A.5.      | Log messages . . . . .                                       | 98        |
| A.6.      | SMTP replies . . . . .                                       | 101       |
| A.7.      | eXpurgate server IP ranges . . . . .                         | 103       |

|                         |     |
|-------------------------|-----|
| A.8. Licenses . . . . . | 103 |
|-------------------------|-----|

---

*Last updated: September 28, 2012*

# 1. Introduction

This documentation describes installation, configuration, and operation of the eXpurgate SMTP version 4. eXpurgate categorizes incoming e-mail before passing it on to a downstream e-mail server. eXpurgate is scalable without limits and hence capable of processing large volumes of e-mail. As three additional variants eXpurgate can cooperate with the open source solution SpamAssassin (spamd protocol), with a SendMail installation (milter protocol), or as an independent text based daemon.

For exploitation of eXpurgate's full functionality, eleven recommends installation of eXpurgate SMTP, since the other variants mentioned above are limited in functionality. For example the freezing function is not available and no statistical data can be gathered and processed via SNMP. A permanent internet connection is a necessary prerequisite for operating eXpurgate, serving for exchange of fingerprints with the eXpurgate database (eXdb).

Examination of e-mails is done without content analysis, so that confidentiality of e-mail communication is maintained. At the same time using fingerprints ensures maximum performance of email processing while achieving an unrivaled low rate of false positives. Additional features such as TLS encryption and certificate management secure communication in sensitive areas. eXpurgate does not need any training and is ready for use right after installation and configuration. During normal operation no maintenance is necessary, except for updates.

## New in eXpurgate 4

Aside from the classical fingerprint, with eXpurgate 4 eleven introduces the structure fingerprint. It allows for abstraction of characteristics making recognition and aggregation of e-mail of identical or similar structure more reliable than before. Improved hashbuster recognition: hashbusters are content blocks inserted automatically into spam e-mails to make analysis of similarity by eXpurgate more difficult. eXpurgate 4 improves recognition of such e-mails as spam by considering only the text of "page 1" for computation of the checksum and recognizing typical hashbuster blocks. Computation of the classical fingerprint was also optimized upon the previous version. As an example, contents having a negative impact on the fingerprint, such as rotating links, are removed. The HTML extractor was reworked as well. Performance of spam recognition could be increased with eXpurgate 4 again, now achieving 99.8 percent and more.

eXpurgate 4 is available for the following Linux distributions and Windows versions, as well as for FreeBSD and Solaris.

- Redhat 5 (i386/amd64)
- Redhat 6 (i386/amd64)
- Debian 5 (i386/amd64)
- Debian 6 (i386/amd64)
- OpenSUSE 11 (i386/amd64)
- OpenSUSE 12 (i386/amd64)
- SUSE Linux Enterprise Server 10 (i386/amd64)
- SUSE Linux Enterprise Server 11 (i386/amd64)

- Ubuntu 10.04 (i386/amd64)
- Ubuntu 12.04 (i386/amd64)
- FreeBSD 8 (amd64)
- Solaris 10 (sparc32/sparc64)
- Windows (i386)

## 1.1. How eXpurgate.Inhouse works

eXpurgate works either as an SMTP proxy (Relay), as a SpamAssassin server (Spamd) or as a Milter plug-in for Sendmail. Each of these variants has individual benefits and disadvantages. Due to limitations of the Milter and SpamAssassin interfaces, eXpurgate is most flexible when used as an SMTP proxy. Use as a Milter plug-in or SpamAssassin server can nevertheless offer advantages for integration into existing infrastructures.

eXpurgate's sole functionality is the categorization of e-mails. A separate e-mail server is therefore always necessary for managing users and e-mail accounts. Due to eXpurgate's low resource requirements separate hardware is not normally required for its installation. eXpurgate can normally be installed alongside the existing e-mail server (software) on the same hardware.

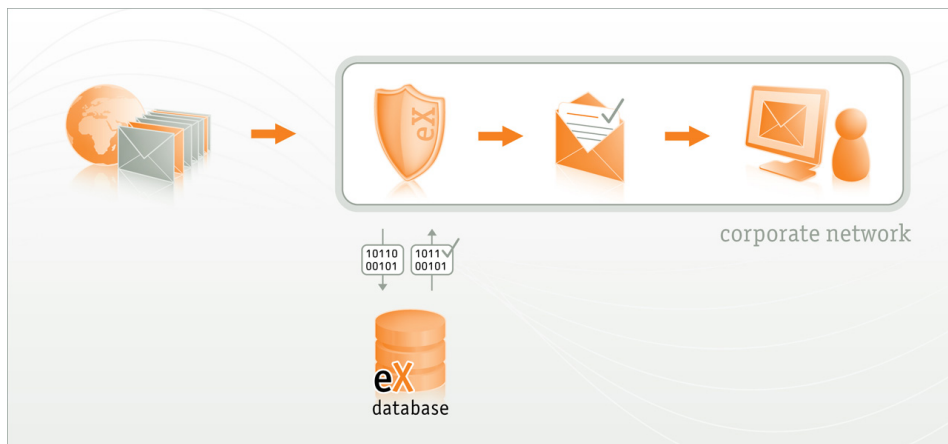


Figure 1.1.: eXpurgate as in-house installation. E-mails are processed in the company network. Only the check sums are compared with the eXpurgate database.

All installation types are based on the bulkcheck as the basic principle of eXpurgate. Each incoming e-mail is subjected to an analysis by eXpurgate during which a short check sum is produced and transmitted encrypted to the central eXpurgate servers. A comparison is made on the eXpurgate servers with the check sums of other e-mails. The result is returned to the requesting eXpurgate installation.

The eXpurgate servers are designed with redundancy and distributed across several locations in order to assure the highest possible availability. eXpurgate.Inhouse requires a connection to the eXpurgate servers in the 194.145.224.0/24 and 195.190.135.0/24 networks on port 55555 to transmit the check sums and receive incoming replies. You may need to adjust your firewall configuration accordingly. Alternatively, you can also direct the connections to the exterior with the help of the SOCKS protocol. The eXpurgate servers do not themselves actively make connections but just respond to queries from eXpurgate client installations.

### **eXpurgate as an SMTP proxy**

As an SMTP proxy, eXpurgate acts like an additional, upstream e-mail server: eXpurgate accepts incoming e-mails via SMTP (Simple Mail Transfer Protocol), categorizes them and passes them on via SMTP to the actual e-mail server. The mail is forwarded to pre-defined e-mail servers; MX entries in the domain name system (DNS) are ignored.

The SMTP proxy mode is the most flexible way of running eXpurgate. The entire functionality of eXpurgate, such as the reject mode, recipient-specific processing rules or integration of the enSurance e-mail firewall, is only available in this mode. For further information, please refer to the eXpurgate SMTP manual.

### **eXpurgate as a SpamAssassin server (Spamd)**

As a SpamAssassin server, eXpurgate does not actively accept incoming e-mails from outside. Instead, it receives queries or e-mails from a SpamAssassin client on a defined port and answers them with the help of the SpamAssassin protocol returning an additional header is returned which contains the e-mail category.

Since eXpurgate does not actively accept e-mails in this mode via SMTP, the scope of functionality depends very much on the protocol used. eXpurgate can only provide the categorization of an e-mail via the SpamAssassin interface or an e-mail header. All treatment rules must be defined in the e-mail server configuration. For further information, please refer to the eXpurgate Spamd manual.

### **eXpurgate as a Sendmail Milter**

As a Milter (Mail Filtering API) for Sendmail, eXpurgate functions similarly to the SpamAssassin mode. In this case, the Milter protocol specified by Sendmail is used as an interface between the mail servers and eXpurgate. The Milter protocol is only available with Sendmail (as from version 8.12). Since eXpurgate also does not actively accept e-mails in this mode the same limitations apply as in SpamAssassin mode. For further information, please refer to the eXpurgate Milter manual.

## **1.2. The eXpurgate principle**

eXpurgate is based on the unique bulkcheck technology for spam recognition and e-mail categorization developed by eleven. eXpurgate checks e-mails for the key characteristic of every spam e-mail: being part of a mass mailing. eleven has developed a check sum algorithm which permits the system to check a large number of e-mails for uniformity or sufficient similarity. This takes place by reducing each e-mail to a check sum which is only a few bytes in size and which permits no conclusions to be drawn about the e-mail content. The check sum is then compared to check sums stored in the central eXpurgate database (eXdb) for already received e-mails. The more frequently a similar e-mail has already been received, the higher the probability that the e-mail currently being checked is spam.

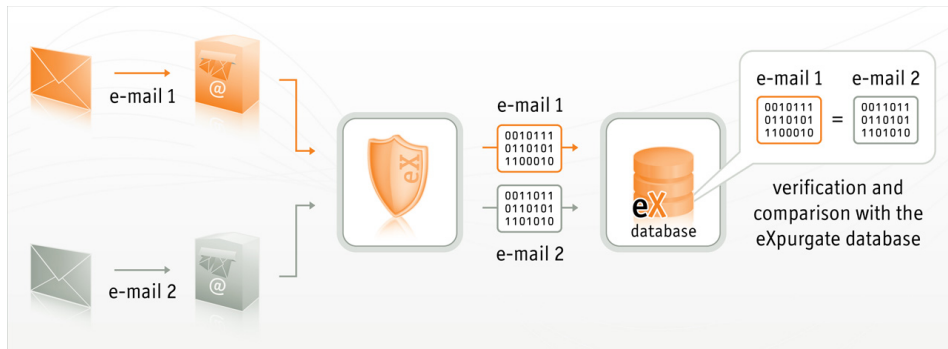


Figure 1.2.: All e-mails are allocated check sums which are collected in the eXpurgate database. Identification as spam takes place when an identical or similar check sum occurs a large number of times.

eXpurgate combines this test procedure with further evaluation methods and is therefore able to definitively place an e-mail in a category such as *clean*, *spam*, *bulk*, or *dangerous.virus*. This also allows eXpurgate to distinguish spam from legitimate mass mailings (e.g. newsletters). In addition, eXpurgate also recognizes dangerous e-mail content and attachments such as viruses and worms before they can cause system changes.

The self-learning bulkcheck technology developed by eleven does not normally delay e-mail delivery to the customer while maintaining confidentiality through encryption (TLS). Unlike conventional spam filters, the technology reduces the number of false positives (e-mails wrongly identified as spam) in individual e-mail communication to near zero.

Appropriate headers are added to the categorized e-mails, which permit automatic processing. These headers are:

- X-purgate-ID** with a unique ID.
- X-purgate-type** with the e-mail category.
- X-purgate-size** with the size of the e-mail.
- X-purgate-Ad** with a short string which points out the use of eXpurgate.

Notes on the configuration of your e-mail program are available on our support pages on the Internet at [www.eleven.de/support/](http://www.eleven.de/support/)



## 2. Installing eXpurgate

The following section describes the installation of eXpurgate.Inhouse on a Unix or Windows system. Both parts are adapted to the respective operating system so that just the section which deals with your operating system is relevant. In both cases you should, however, take note of the subsequent section on configuring eXpurgate. Since this is largely independent of the underlying operating system, we deal with it in a separate chapter.

Please note that to run eXpurgate you need a valid license from eleven or one of its partners. The license is a binary file that will be referred to as client.key below.

### 2.1. Installing eXpurgate SMTP on a Unix system

#### 2.1.1. Installation and removal of the packages

To install eXpurgate SMTP from a Debian package, use the following command:

```
# dpkg --install <package>.deb
```

**Note:** In some versions of debian can appear the following error message:

```
update-rc.d: warning: /etc/init.d/expurgate missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
expurgate: disabled, see /etc/default/expurgate
```

You can ignore the message.

To uninstall, use the following command:

```
# dpkg --remove expurgate
```

To install eXpurgate SMTP from an RPM package, use the following command:

```
# rpm --install <package>.rpm
```

To uninstall, use the following command:

```
# rpm --erase expurgate
```

To install eXpurgate SMTP from a TGZ archive, take the following steps:

Extract the archive.

```
# tar zxvf <package>.tar.gz
```

Change to the freshly created package sub-directory into which the files have been extracted.

```
# cd <package>
```

Install the binary and the configuration file (you need administrative privileges for this and the subsequent steps).

```
# mkdir /etc/expurgate
# cp bin/expurgate /usr/local/bin/
# cp etc/expurgate/expurgate.conf /etc/expurgate/
```

Install the init script and the file with the default settings.

```
# cp etc/init.d/expurgate /etc/init.d/
# cp etc/default/expurgate /etc/default/
```

Instead of the generic init script, which is suitable for all UNIX-like systems, you can choose to install one of the init scripts specific to Debian and RedHat based distributions as well as the SUSE Linux distribution. In this case, you must also use the corresponding default or sysconfig file.

Here is an example for a RedHat based distribution. Note that directory and file names differ from the preceding example.

```
# cp etc/init.d/expurgate.redhat /etc/init.d/expurgate
# cp etc/sysconfig/expurgate.redhat /etc/sysconfig/expurgate
```

Create the spool, run and log directories.

```
# mkdir /var/log/expurgate
# mkdir /var/run/expurgate
# mkdir /var/spool/expurgate
```

After installing the package, copy the license key<sup>1</sup> into the configuration directory:

```
# cp /path/to/your-license-key /etc/expurgate/client.key
```

To uninstall after installation from a TGZ archive, remove the files and directories from the filesystem which have been copied or created during installation.

To configure eXpurgate SMTP, edit the configuration file in */etc/expurgate/expurgate.conf*. You can also pass command line options to eXpurgate SMTP. For this, edit */etc/default/expurgate* which is read by the init script when the service is started. Command line options have priority over settings in the configuration file. Further information on configuration is in Section ??.

---

<sup>1</sup>The license key is a binary file which you will have received from your reseller or downloaded from the eleven website's customer area. If you do not have a license key, please contact support@eleven.de.

## 2.1.2. Activating and deactivating the service

The service is not automatically started after installation. The steps for activation depend on the chosen installation method:

If you have installed from a Debian package, edit `/etc/default/expurgate`. Set the `ENABLE` variable to `yes`.

If you have installed from an RPM package, execute the following command:

```
# /sbin/chkconfig expurgate on
```

If you have installed the SUSE RPM package, you should either use the YaST configuration tool or the following command:

```
# /sbin/insserv expurgate
```

If you have installed from a TGZ archive you should ensure that the init script is called on the respective run level. The precise steps for this depend on the platform.

Execute the following command on a Debian-based system:

```
# /usr/sbin/update-rc.d expurgate defaults
```

On a system such as Red Hat Enterprise Linux, Fedora or CentOS the command is:

```
# /sbin/chkconfig expurgate on
```

On a SUSE system use the following command:

```
# /sbin/insserv expurgate
```

To deactivate the service, perform the following steps:

If you have installed from a Debian package, set the `ENABLE` variable in `/etc/default/expurgate` back to `no`.

If you have installed from an RPM package, execute the following command:

```
# /sbin/chkconfig expurgate off
```

On a SUSE system use the following command:

```
# /sbin/insserv -r expurgate
```

If you have installed from a TGZ archive, the precise steps depend on the platform.

Execute the following command on a Debian-based system:

```
# /usr/sbin/update-rc.d expurgate remove
```

On a system such as Red Hat Enterprise Linux, Fedora, or CentOS the command is:

```
# /sbin/chkconfig expurgate off
```

On a SUSE system use the following command:

```
# /sbin/insserv -r expurgate
```

Deactivating the service does not stop an instance that is already running. See the next section for more on this.

### 2.1.3. Starting and stopping the service

If you have followed the steps described in the previous section, eXpurgate SMTP will be started automatically at the next reboot. This section describes how to start and stop the service manually.

Enter the following command to start eXpurgate SMTP with the init script:

```
# /etc/init.d/expurgate start
```

Use the following command to stop eXpurgate SMTP with the init script:

```
# /etc/init.d/expurgate stop
```

Further options are displayed if you call the init script without arguments:

```
# /etc/init.d/expurgate
```

Your platform may have a specialized command or program to start and stop services. Examples for this are `/usr/sbin/invoke-rc.d` on Debian-based systems and `/sbin/service` on Red Hat Enterprise Linux and Fedora.

For testing it often makes sense to call the eXpurgate SMTP binary directly. Enter the following command to start eXpurgate SMTP manually:

```
# expurgate --config /etc/expurgate/expurgate.conf
```

To stop eXpurgate SMTP manually:

```
# kill `pidof expurgate`
```

### 2.1.4. Connectivity test

eXpurgate requires a TCP connection to the networks 194.145.224.0/24 and 195.190.135.0/24, where port 55555 is used to communicate. Please verify if this connection is possible and pay attention to your firewall configuration. eXpurgate provides a command line option `--test-exdb`s to check reachability of the eXpurgate server (eXdb). When run with this option eXpurgate tries to contact every configured eXpurgate server, one by one, and gives a message whether the attempt was successful or not.

With the correct standard configuration you get the following output:

```
# expurgate -c <path-to-config> --test-exdb

exa.expurgate.de:55555 prio 10 OK
exb.expurgate.de:55555 prio 10 OK
exa.expurgate.net:55555 prio 20 OK
exb.expurgate.net:55555 prio 20 OK
```

**Note:** `<path-to-config>` is a placeholder to be replaced with the full path to the configuration file.

### 2.1.5. Further Remarks

A list of further options is available by calling `expurgate --help`.

Should problems occur when starting eXpurgate SMTP, you will find error messages in the log file. By default this is located in `/var/log/expurgate`.

eXpurgate re-reads changed configuration files if the HUP signal is received. If one of the options `chroot`, `uid` or `gid` is set eXpurgate will not update security-relevant files like license or TLS keys and certificates if the HUP signal is received. Please mind the option `--always-reload` in this context.

## 2.2. Installing eXpurgate on a Windows system

If you install eXpurgate under Microsoft Windows, the necessary parameters are requested during the installation process and eXpurgate is then installed and started as a service.

To start the installation, please double-click the eXpurgate installation file. An installation wizard appears that will guide you through the installation.



Figure 2.1.: Installation wizard start page

Click NEXT to begin the actual installation.

Please read the licence conditions with care. Click the I ACCEPT THE LICENCE AGREEMENT field and then NEXT.

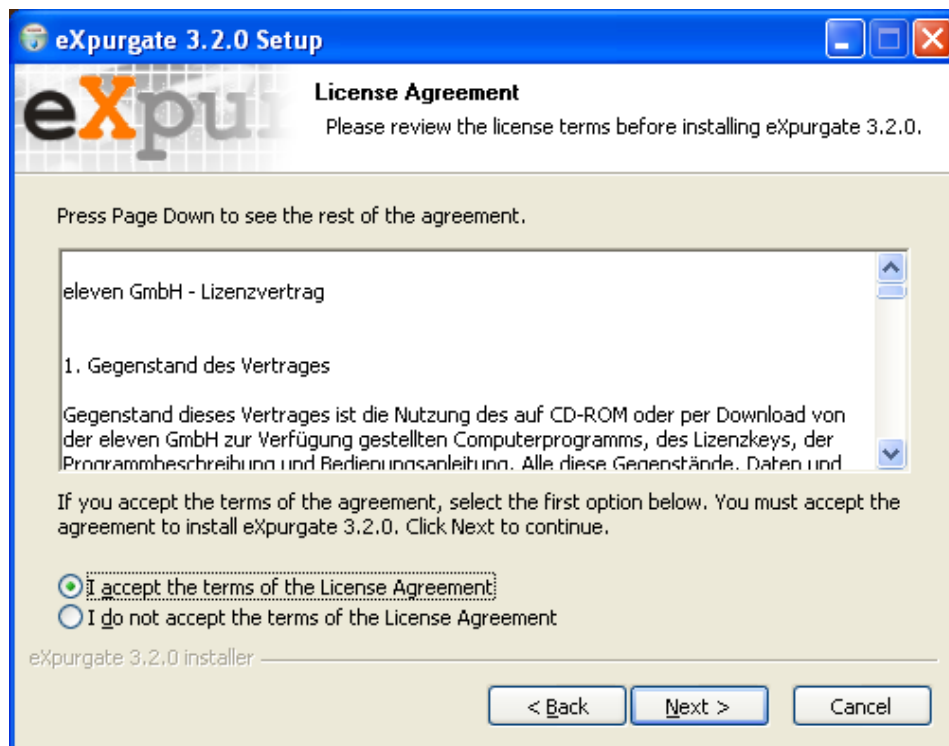


Figure 2.2.: Licence agreement

Now select the directory in which eXpurgate is to be installed. The default setting is the *eleven\exPurgate* directory below your programs directory (e.g. *C:\Program Files\eleven\exPurgate*). You can change this to suit your installation requirements. Click NEXT.

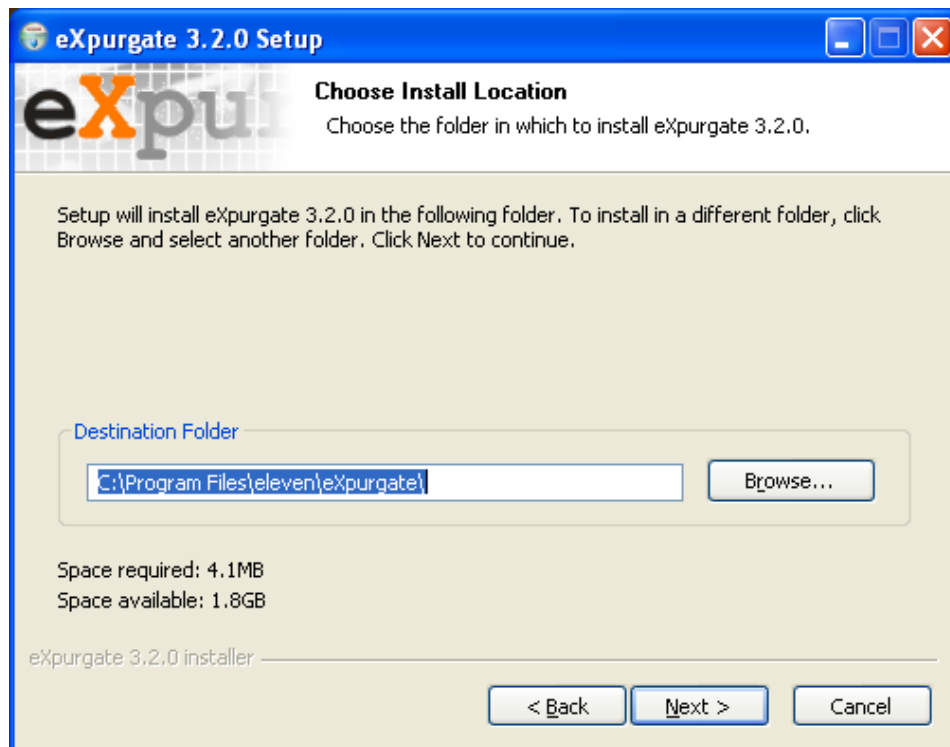


Figure 2.3.: Selecting the target directory



Specify where eXpurgate should be listed in the Windows Start menu and then click NEXT.

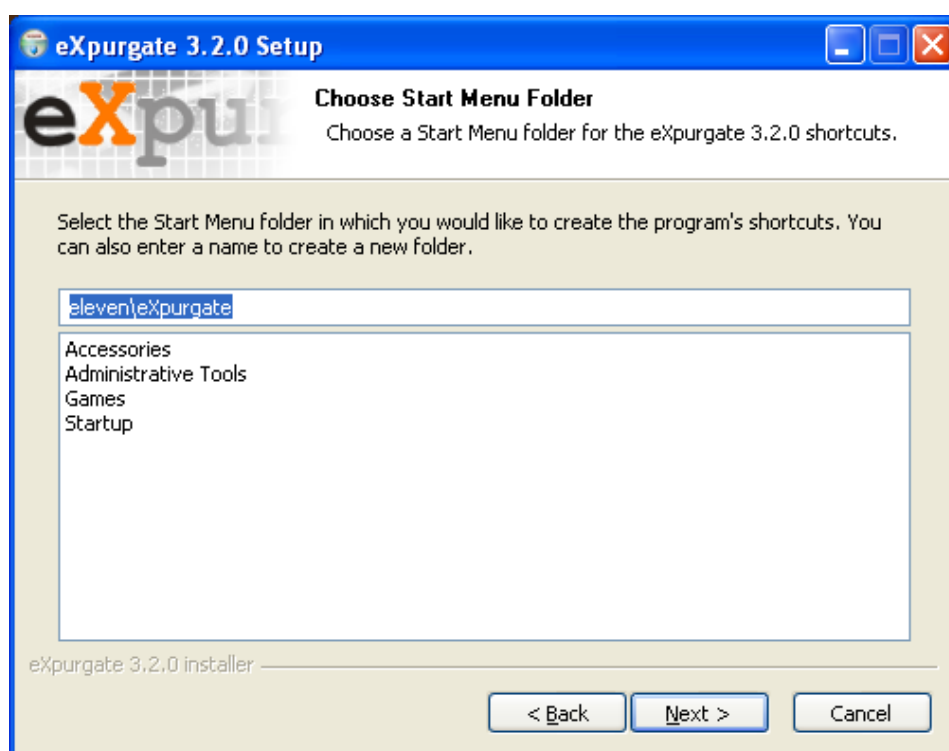


Figure 2.4.: Inserting eXpurgate into the Start menu

Under the connection options you must specify via which network interface and port eXpurgate should receive incoming e-mails (Default: 0.0.0.0:25).

Under MailServer Host and MailServer TCP/IP Port you should specify the server address and which port eXpurgate can contact your existing e-mail server. Should eXpurgate and the existing server be running on the same machine you must change its port to one which is not being used. Otherwise, enter the name of the other machine and the mailer port on it.

After you have specified the path to the eXpurgate licence file and confirmed the information by clicking NEXT, eXpurgate attempts to communicate with your existing e-mail server on the specified port. If it is available, proceed to the next window HOW TO HANDLE SPAM E-MAILS by clicking NEXT.

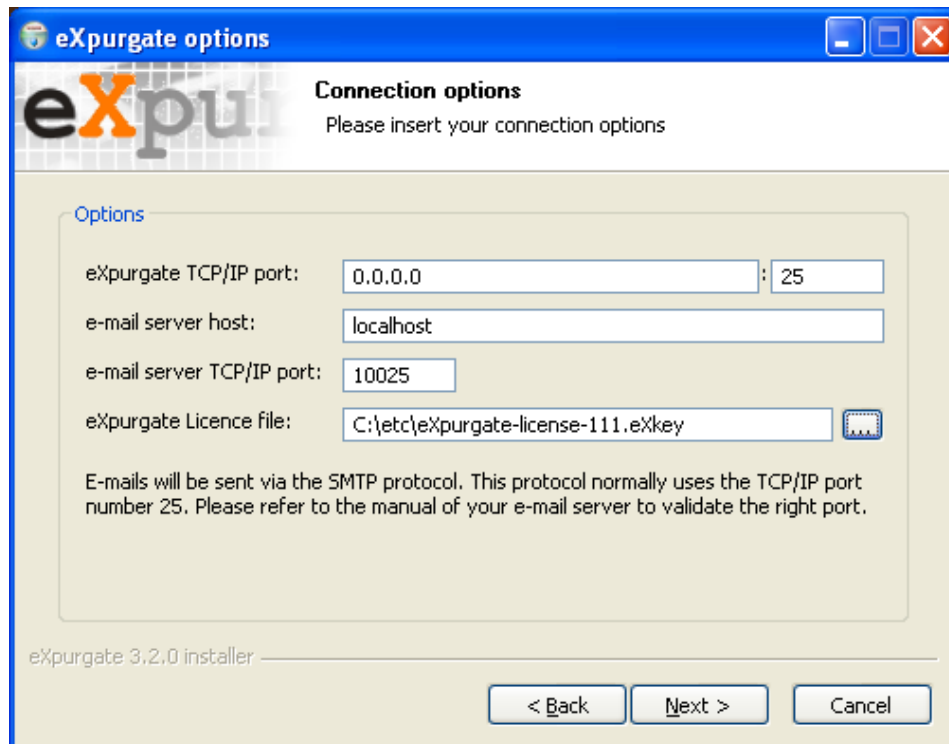


Figure 2.5.: Connection options

In the HOW TO HANDLE SPAM E-MAILS window you can specify how spam e-mails should be dealt with. Here you can determine if spam should be merely tagged with a header and delivered to its recipient or another address such as a collective address (catchall). Alternatively, eXpurgate can reject Spam already on delivery, or accept and subsequently delete it.

Click NEXT.

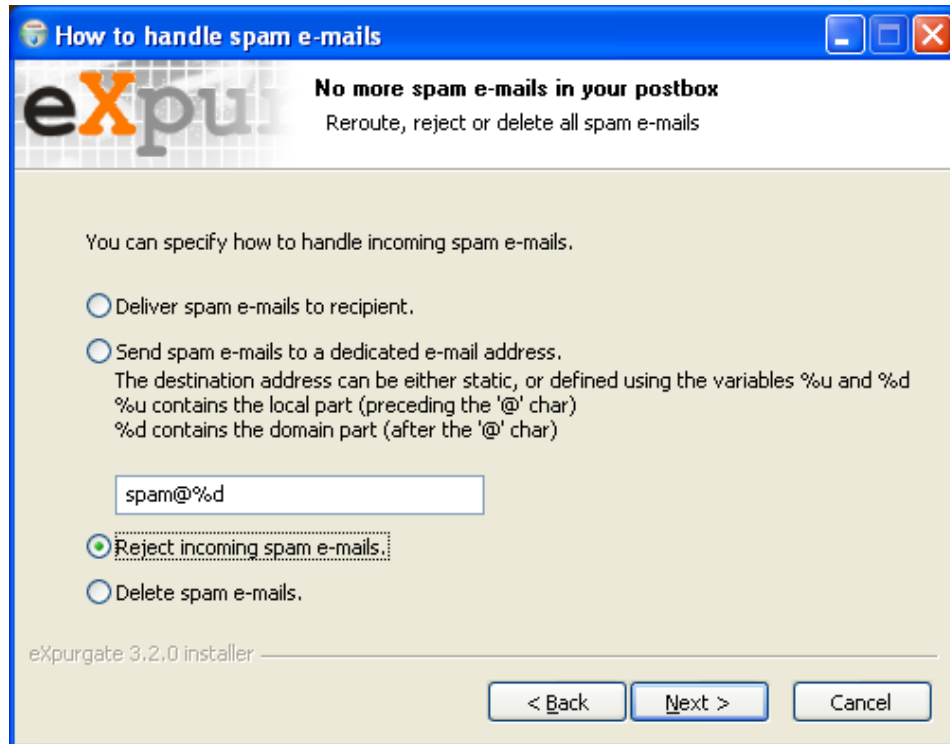


Figure 2.6.: Further treatment for spam e-mails

With the **CHANGE THE SUBJECT HEADING** option you can have the subject heading changed for categorized mass mails. This gives you a rapid overview of what type of e-mail it is and whether it would be wise or even dangerous to open the mail. This procedure is especially suitable if the mail is to be checked manually after it has been categorised by eXpurgate.

For the *spam*, *bulk* and/or *dangerous* type you can define with which schema the subject heading is to be replaced. The default [%t] %s, for example, changes the subject heading of an incoming spam e-mail that reads *Hi Allen, make money fast* to *[spam] Hi Allen, make money fast* and thus makes it quicker to classify.

Click **NEXT** to reach the **SSL/TLS OPTIONS**.

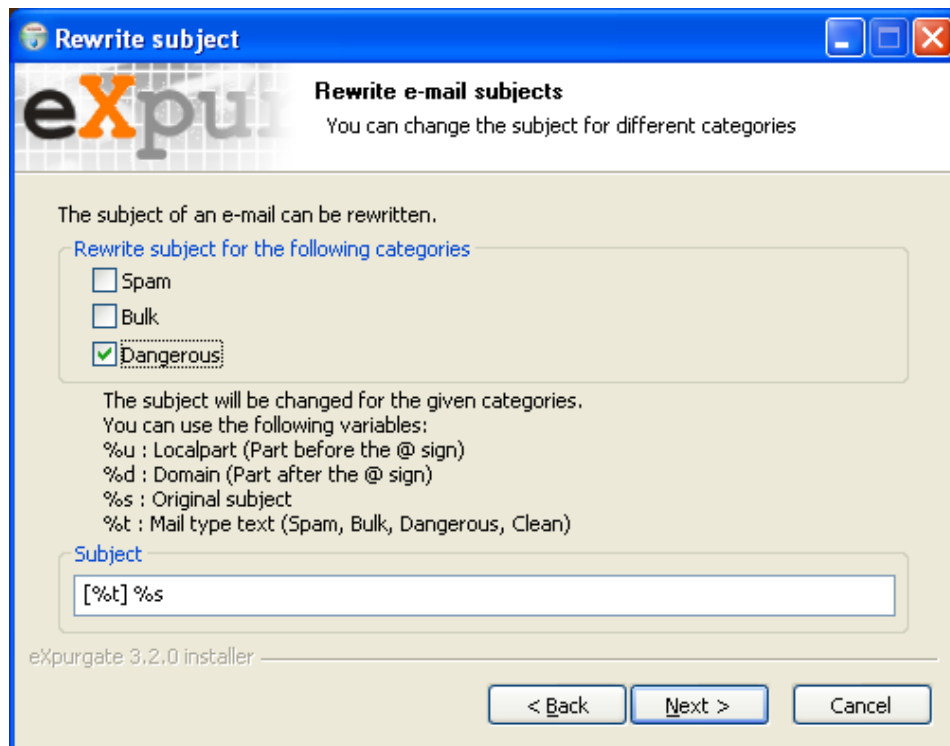


Figure 2.7.: Changing the mail subject header

The SSL/TLS options securely encrypt the transmission route between suitable servers. If you do not use this relatively new and uncommon procedure you should not make any changes here and click **NEXT**.

Further information on the SSL/TLS procedure is available in section 3.2.5 of this documentation. This option is not essential for either e-mail transmissions via the usual Internet SMTP procedure or the functional capability of eXpurgate and can remain inactive in most cases.

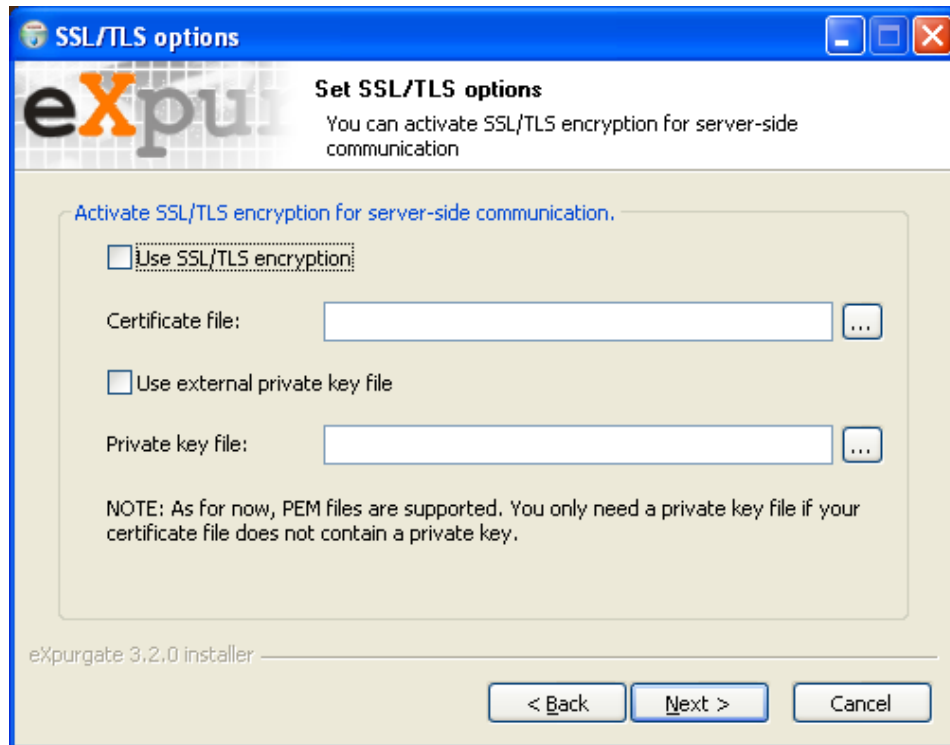


Figure 2.8.: Selecting SSL/TLS options

Your input is summarised at the end of the installation. Please check and correct it if necessary. Then click INSTALL.

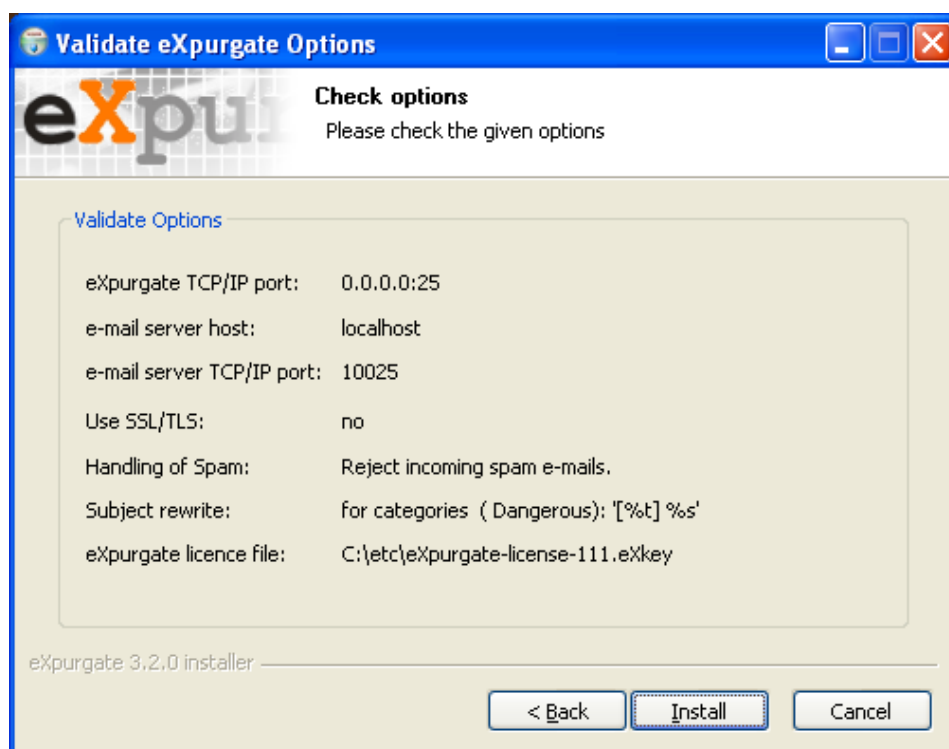


Figure 2.9.: Checking the data entered

eXpurgate will now be installed on your computer in accordance with your specifications, added as a Windows service and started.

At the end of the installation, the connection to the eXpurgate servers (eXdb Server) at eleven is checked. You arrive at the last screen if the installation was successful.

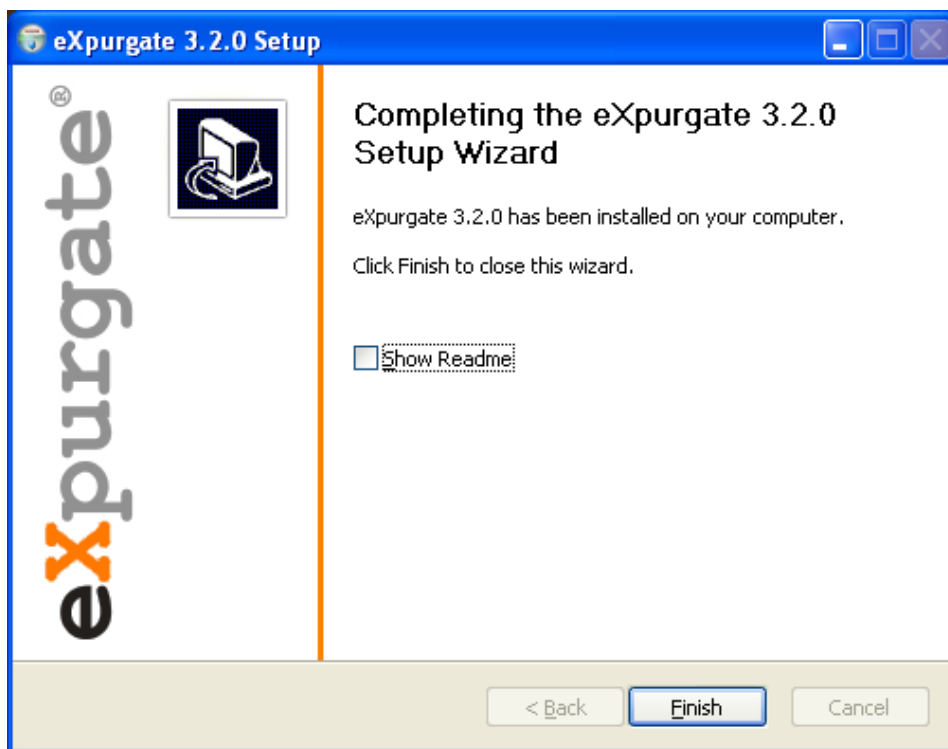


Figure 2.10.: Final installation screen

To end the installation wizard please click **FINISH**. The eXpurgate installation is now operational. eXpurgate logs its starts including the command line options used in the Windows Event Log (to be found via **START/PROGRAM FILES/ADMINISTRATION/EVENT LOG**). You also receive information on possible errors here.

### 2.2.1. Windows service commands

eXpurgate is installed as a service in Microsoft Windows so that eXpurgate is started automatically — without user log-in — after the system is booted. You can check this under **START/PROGRAM FILES/ADMINISTRATION/SERVICES**.

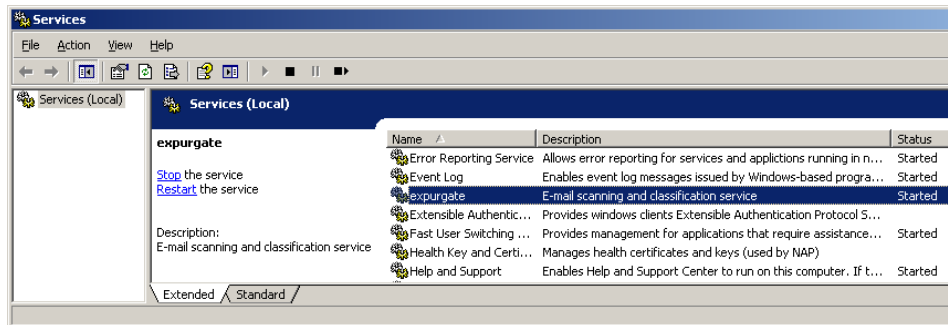


Figure 2.11.: eXpurgate entered as a service in the Microsoft Management Console

The following command line parameters are available for controlling eXpurgate as a Windows service:

|              |   |
|--------------|---|
| install      | Installs eXpurgate as a Windows service without starting it. The start parameters must be specified subsequently. |
| remove       | Uninstalls eXpurgate as a Windows service.  |
| start        | Starts the already installed eXpurgate service.   |
| stop         | Ends the installed eXpurgate service.   |
| isinstalled  | Checks whether eXpurgate has been installed as a service.   |
| isrunning    | Checks whether eXpurgate is currently running as a service.   |
| getparameter | Returns the parameters with which the service is started.   |
| setparameter | Sets new start parameters (identical to install).   |

### 2.2.2. Changing the TCP port with Microsoft Exchange 5.5

If you wish to operate eXpurgate together with Microsoft Exchange 5.5 on the same server you must ensure that Exchange receives e-mails on a port other than port 25. The Exchange 5.5 SMTP Connector takes over the port to which it binds itself from the *services* file which is to be found in your Windows directory (*%SystemRoot%* or *C:\WINNT*) in *system32\drivers\etc*. You can edit this for example as follows:

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

The services file is based on the following schema:

```
Service Port/Protocol [Alias...] [\'#Comment]
```



The entry for the SMTP protocol typically looks like this:

```
smtp 25/tcp mail #Simple Mail Transfer Protocol
```

Please change the value for the service smtp (default: 25/tcp) to a new, free port on which your Exchange should now receive mails, for example 10025. The modified entry in the services file must look like this:

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

The service must then be rebooted for the change to take effect. You can test this with the help of telnet.

### 2.2.3. Changing the TCP port with Microsoft Exchange 2000 or 2003

The option of changing the port through which Exchange receives external mails is already provided for in Exchange 2000 or 2003. In order to reach it, please proceed as follows:

- Open the Exchange System Manager (normally in the Start menu under Program Files/Microsoft Exchange/System Manager).
- Click in the System Manager on Server, then on the relevant server and under /Protocols/SMTP with the right mouse button on virtual default server for SMTP; finally, click on Properties in the menu which opens.

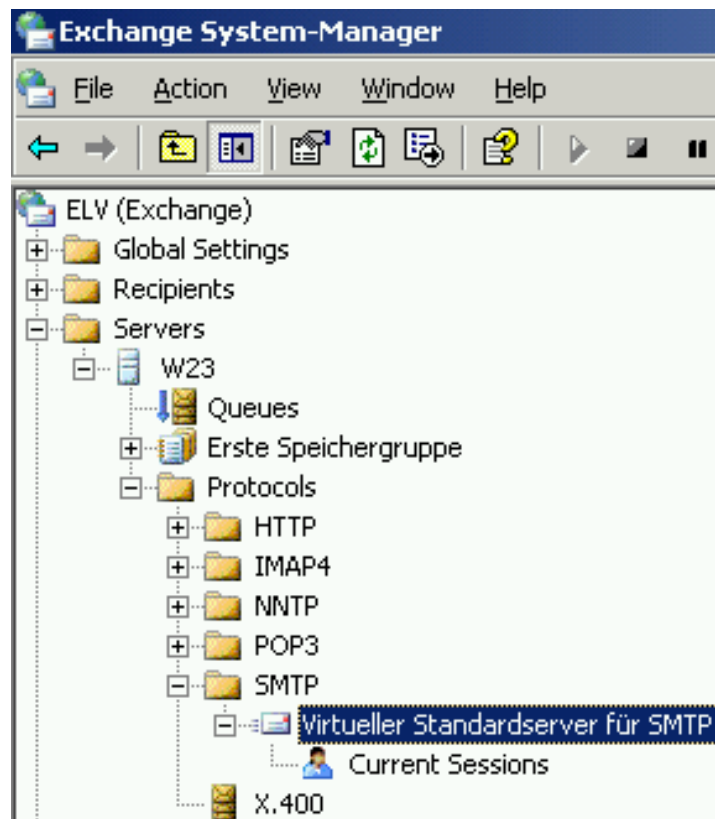


Figure 2.12.: Exchange system manager

On the GENERAL tab, select the IP address of the server and then click ADVANCED.

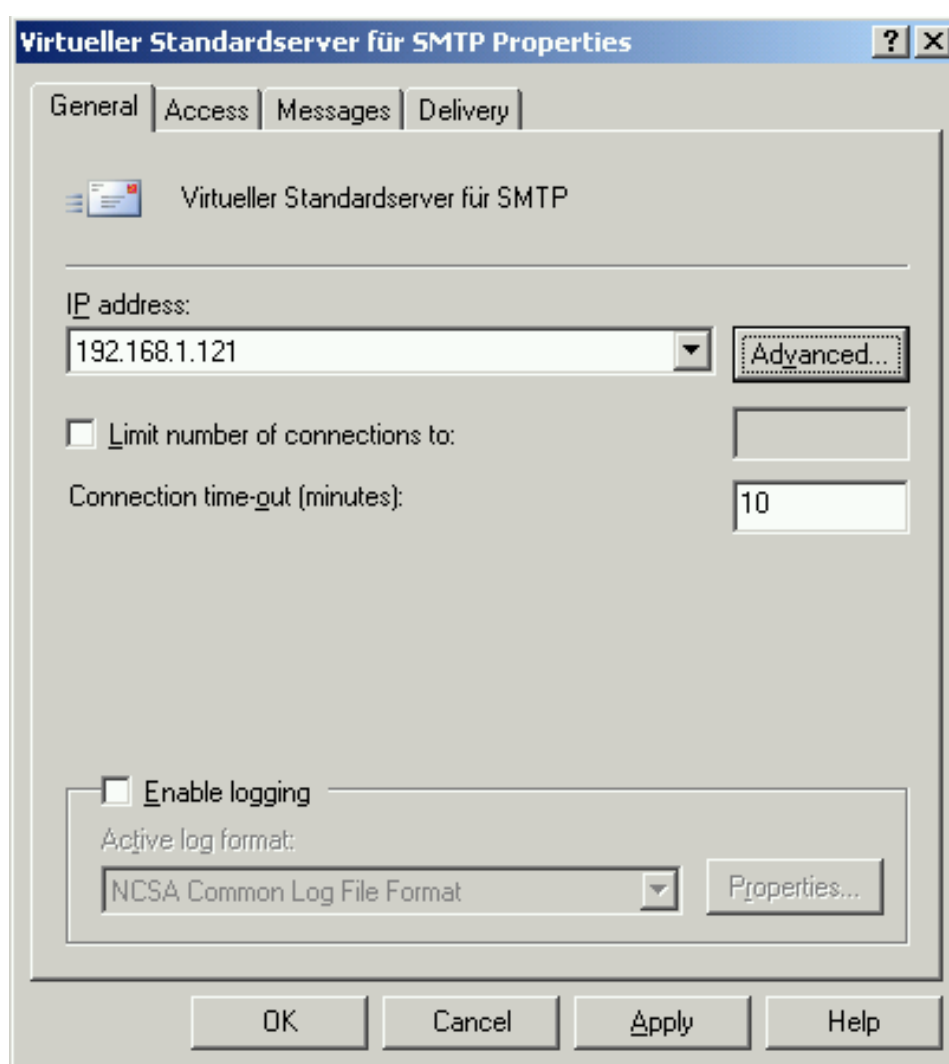


Figure 2.13.: Virtual default server

Click **EDIT** to edit this virtual server's properties.

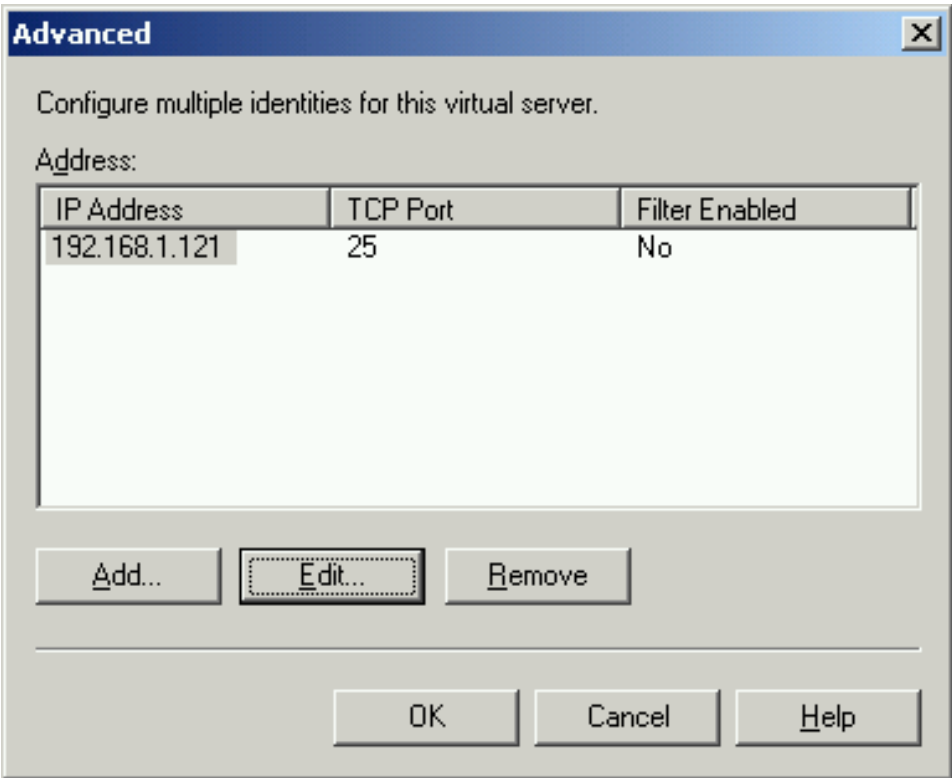


Figure 2.14.: Advanced

Here you can change the TCP port through which Exchange receives incoming e-mails. Enter a different, unused port such as 10025 and confirm with OK.

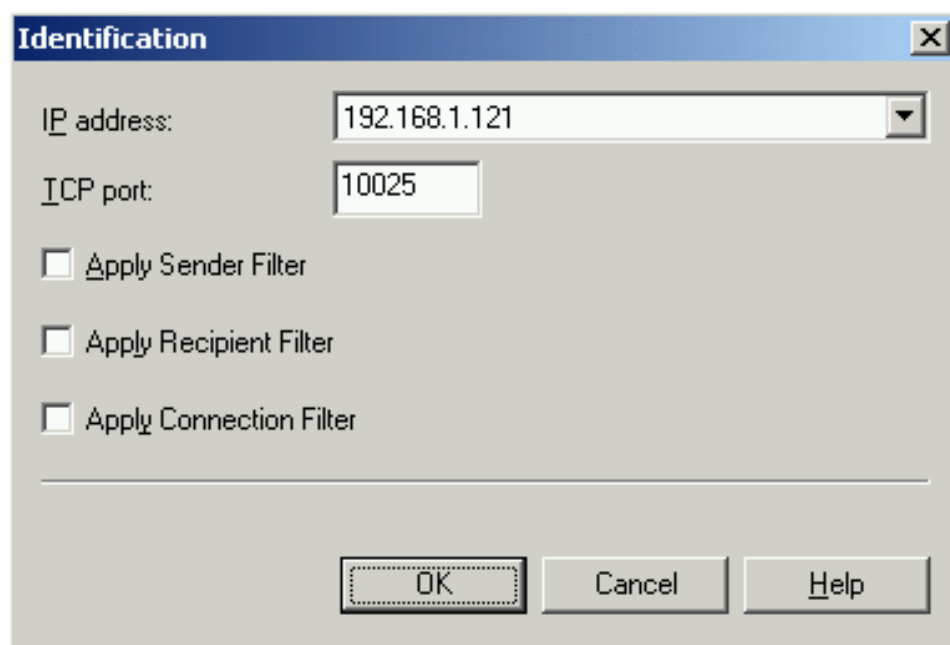


Figure 2.15.: Identification

With a further OK you return to the Exchange system manager. Now stop the virtual server and restart it. Your Exchange should now be accessible on port 10025. Please read the following section to test whether the change was successful.

#### 2.2.4. Test whether Exchange responds to a port

If you wish to test whether your Exchange server has accepted the port change you can do this with the help of telnet. Open a command line and enter the following command:

```
telnet 192.168.1.121 10025
```

Use your Exchange server's IP address instead of 192.168.1.121. The new port is 10025. Your Exchange should greet you as follows after a successful change and a reboot of the virtual SMTP server:

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

End the SMTP dialog with Exchange by entering quit. If this test was successful you can now start eXpurgate on port 25 so that it can forward incoming mail to Exchange following classification.

## 3. Configuring eXpurgate

eXpurgate is configured with the *expurgate.conf* configuration file. Some settings can also be set directly via the command line. Both configuration options are explained in the sections of this chapter. Command line settings have priority over settings in the configuration file. This also applies to settings that are typically used several times.

**Example:** If eXpurgate servers are defined both on the command line and in the configuration file (with the `--exdb` option or the server in the `SpamEngine` section of the configuration file) only those servers named on the command line apply.

The configuration file and all referenced files are loaded before switching to the configured user- and group-id or changing the root directory. This facilitates keeping security-relevant files, like license or SSL keys and certificates, outside the configured root directory or readable by privileged users only.

If you plan to use eXpurgate in a changeroot environment, the *Avira AntiVir* ("savapi") service must be running within the same environment.

**Note:** Most settings are pre-initialized with realistic defaults; typically these do not need to be changed. However, eXpurgate requires the following obligatory settings to be able to startup:

**The working directory** This can be set in the configuration file using the `WorkingDirectory` directive or on the command line using the `--working-dir (-w)` option.

**The license file** This file can also be set in the configuration file using the `LicenseFile` directive or on the command line using the `--license (-l)` option.

eXpurgate can handle IPv4 and IPv6 addresses. If an IPv6 address is used in combination with a port number, it is necessary to put the address into squared brackets. If using IPv6 addresses please note to use only IPv6 addresses in other options referring to IP addresses like `Permissions` or `UserSettings` of the configuration file. Furthermore, the public eXpurgate servers are only accessible via IPv4.

### 3.1. Command line options

eXpurgate can be configured with the following command line options. You will also find an overview of the possible options if you enter `expurgate --help`.

In the following section the name of the option is stated first, then possible arguments and finally a short description of how it works. Arguments follow the option separated by a space. The options are specified with two preceding dashes. If an option can be used several times this is expressly stated below. If an option cannot be used several times, only the last time the option is specified is recognised.

**Example:** If the `--exdb` option (specification of an eXpurgate server) is used several times, all specified eXpurgate servers are recorded. If, however, the `--listen` option (specification of the SMTP server interface and port) is used several times, eXpurgate only listens on the last specified address.

Options which expect no arguments are available in a negated form, whereby the option name is preceded by a `no-`. This is useful for changing deviating settings in the configuration file or in a preceding option.

**Example:** Virus scanner activation in the configuration file can be switched off again with the `--no-antivir` option.

### 3.1.1. Information output options

By specifying the following command line options you can retrieve information on the eXpurgate SMTP mode of operation and version. The program ends directly after the output without starting the eXpurgate SMTP service.

| Option                           | Description  |
|----------------------------------|--|
| <code>--help</code>              | Outputs the possible options.                                  |
| <code>--version</code>           | Outputs the program version.                                   |
| <code>--vcsid</code>             | Outputs the program's internal version number.                 |
| <code>--compiler</code>          | Outputs the program name and the version of the compiler used. |
| <code>--show-license FILE</code> | Outputs license information for the specified license file.    |

### 3.1.2. Options for operation on Unix

The following options are available if eXpurgate SMTP is running in a Unix environment.

| Option                          | Description  |
|---------------------------------|--|
| <code>--daemonize</code>        | Detaches eXpurgate SMTP from the terminal and starts it as a background process (daemon). Use <code>--no-daemonize</code> to disable this functionality. |
| <code>--pidfile FILE</code>     | Writes the process ID in the specified file.   |
| <code>--chroot DIRECTORY</code> | Changes the eXpurgate SMTP root directory to the specified path and starts eXpurgate SMTP in this directory in an isolated environment.                  |
| <code>--uid USER-ID</code>      | Changes the effective user to the specified (non-privileged) user ID once eXpurgate SMTP has been initialized.   |
| <code>--gid GROUP-ID</code>     | Changes the effective group to the specified (non-privileged) group ID once eXpurgate SMTP has been initialized.   |

### 3.1.3. Options for logging of log messages

The following command line options define which events are logged for particular log targets. Each option follows a specification of log levels which define which log messages are written in the respective log target.



The log targets are log files, the standard error output, the system logger (Unix), the system console (Unix) and the event log (Microsoft Windows).

**Example:** With the `--log-file ERROR-EMERGENCY:/var/log/expurgate/error.log` option all error messages are written in the `/var/log/expurgate/error.log` file.

| Option                                     | Description   |
|--|---|
| <code>--log-file MIN-MAX:FILE</code>       | Log levels and log file name. This option may be specified multiple times, e.g. to use separate log files for different log levels. |
| <code>--log-stderr MIN-MAX</code>          | Log levels for the standard error output.   |
| <code>--log-syslog MIN-MAX:FACILITY</code> | Log levels for the system logger on Unix systems.   |
| <code>--log-console MIN-MAX</code>         | Log levels for the system console ( <code>/dev/console</code> ) on Unix systems.  |
| <code>--log-event MIN-MAX</code>           | Log levels for the event log on Microsoft Windows systems.  |

**Note:** The `--log-file` option can be specified several times, e.g. to log events with different levels of importance in different files.

The importance levels for log messages are listed in the following.

**DEBUG** Internal log message with low priority.

**INFO** Information on normal functioning.

**NOTICE** Message about specific events.

**WARNING** Warning in case of unusual events.

**ERROR** Message about non-critical error messages.

**CRITICAL** Message about critical error states.

**ALERT** The error state requires immediate intervention .

**EMERGENCY** The system is no longer functional.

Both the lower and upper limits can be dispensed with; in this case, the level is amended downward to the lowest or upward to the highest importance level.

**Example:** The `--log-stderr -NOTICE` option sends only log messages to the standard error output below the **WARNING** level of importance.

If just one importance level is specified this is interpreted as the lower limit.

**Example:** The `--log-console CRITICAL` option outputs all critical error messages on the system console including **ALERT** and **EMERGENCY** level messages.

Please note that both limits must not be omitted. Simply passing the `--log-stderr` option without argument results in an error during startup.

The **FACILITY** field in the `--log-syslog` option specifies a logging section that can be used by the system logging daemon to filter log messages into different files. The value **MAIL** is typically used. Legal values are:

- **AUTHPRIV**

- CRON
- DAEMON
- FTP
- KERN
- LOCAL0 to LOCAL7
- LPR
- MAIL
- NEWS
- SYSLOG
- USER
- UUCP

**Example:** With the `--log-syslog NOTICE:MAIL` option all log messages of a purely informative nature are logged by the system logger with the facility MAIL.

### 3.1.4. Options for testing eXpurgate

Use the following options to check various eXpurgate settings.

| Option                        | Description  |
|-------------------------------|--|
| <code>--test-config</code>    | Checks the configuration file (loaded with <code>--config</code> ) settings.                 |
| <code>--test-exdb</code>      | Checks if the configured eXpurgate servers are available.                                    |
| <code>--test-relays</code>    | Checks if all configured relay servers are available.  |
| <code>--test-tls</code>       | Checks the TLS configuration, more specifically the specified private keys and certificates. |
| <code>--test-ensurance</code> | Checks the enSurance configuration.  |

### 3.1.5. General functionality options

The following command line options generally affect the functionality of eXpurgate.

| Option                               | Description   |
|--------------------------------------|---|
| <code>--config FILE</code>           | Loads the configuration file. If this file is not located in the current working directory, its full path must be specified — it is not automatically searched below <code>/etc/expurgate</code> .  |
| <code>--working-dir DIRECTORY</code> | Defines the eXpurgate working directory for storing run-time data.  |
| <code>--license FILE</code>          | Loads the specified eXpurgate licence.  |
| <code>--always-reload</code>         | Tells eXpurgate to reload security-relevant files like license or TLS keys and certificates when receiving the HUP signal, although one of the options <code>--uid</code> , <code>--gid</code> or <code>--chroot</code> is set. Without this option eXpurgate will not update the license and TLS files when the HUP signal is received, even if changed in the configuration file. |

### 3.1.6. SMTP server options

The following SMTP server settings are available on the command line.

| Option                                       | Description   |
|--|---|
| <code>--listen <i>PORT:HOST</i></code>       | Sets the IP address and port on which the SMTP server listens for incoming connections.   |
| <code>--max-connections <i>NUMBER</i></code> | Limits the maximal number of concurrent connections.  |
| <code>--tls-certificate <i>FILE</i></code>   | Loads the TLS server certificate from the specified file.   |
| <code>--tls-private-key <i>FILE</i></code>   | Loads the private key for TLS encryption from the specified file.   |
| <code>--tls-on-connect</code>                | Enables/disables the TLS support, if a SMTP client connects to the SMTP server. This option may be disabled with <code>--no-tls-on-connect</code> . |
| <code>--local-domain <i>DOMAIN</i></code>    | Considers the specified domain as local. E-mails for this domain are always accepted. This option may be specified multiple times.                  |

### 3.1.7. Options for downstream SMTP relays

Use the following option to configure the downstream SMTP relays. Please note that the configuration file allows for a much more detailed configuration of relays.

| Option                                   | Description  |
|--|--|
| <code>--smtp-out <i>HOST:PORT</i></code> | Defines a downstream SMTP relay through which e-mails may be delivered. This option may be specified multiple times. |

### 3.1.8. Options for the Spam-Engine

This section describes options regarding the internal processing of e-mails.

| Option                                    | Description   |
|---|---|
| <code>--exdb <i>HOST:PORT</i></code>      | Host and port of an eXpurgate Server to be used. Caution: If this option is used, any entries in the configuration file are ignored. This option may be specified multiple times. |
| <code>--socks <i>HOST:PORT</i></code>     | Use the specified SOCKS-Proxy for communication to the eXpurgate servers.   |
| <code>--socks-user <i>USERNAME</i></code> | Username used by the SOCKS proxy server.  |
| <code>--socks-pass <i>PASSWORD</i></code> | Password used by the SOCKS proxy server.  |
| <code>--threads <i>NUMBER</i></code>      | Number of concurrent threads classifying e-mails. This value is typically much smaller than the value of the <code>--max-connections</code> option.                               |

### 3.1.9. Virus scanner configuration options

The following command line options permit the AntiVir virus scanner to be activated and its mode of operation to be set.

| Option                                  | Description   |
|---|---|
| <code>--antivir</code>                  | Switches the virus scanner on. This option may be disabled with <code>--no-antivir</code> . |
| <code>--antivir-port <i>PORT</i></code> | Virus scanner port.   |

### 3.1.10. Options for the Simple Network Management Protocol

The following section describes the configuration of SNMP to monitor eXpurgate by a network management software. There are more options if you configure eXpurgate via the config file. Please refer to Section 3.2.8 for more information on this.

| Option  | Description  |
|---|--|
| <code>--snmp</code>                           | Enables/disables SNMP of eXpurgate. This option may be disabled with <code>--no-snmp</code> .  |
| <code>--snmp-address <i>HOST:PORT</i></code>  | Hostname and port defines the SNMP interface of eXpurgate.   |
| <code>--snmp-community <i>PASSWORD</i></code> | You have the possibility to assign a password to query data from eXpurgate. Caution: The password of eXpurgate and the network management software have to be equal. |

### 3.1.11. Freezing options

Using the following options freezing may be configured, i.e. the delayed delivery of e-mails. Extended settings are available in the configuration file.

| Option                                     | Description  |
|--|--|
| <code>--freezing</code>                    | Enable freezing. To explicitly disable freezing, use the <code>--no-freezing</code> option.  |
| <code>--fridge-dir <i>DIRECTORY</i></code> | Defines the directory used to store frozen e-mails. This directory may not be the working directory and must be located on the same storage medium as the working directory. |

## 3.2. The configuration file

eXpurgate is configured by the *expurgate.conf* configuration file. It is located in */etc/expurgate* on Unix systems and below the directory *C:\Program Files\eleven\expurgate\etc* on Microsoft Windows systems. The name of the configuration file is specified via the `--config (-c)` command line option. Most configuration

settings are pre-initialized with sensible defaults. As a consequence, the majority of settings do not need to be manually changed.

**Note:** Please note, that by default no mails are filtered. To prevent spam mails from being delivered you have to adapt the settings in the <UserSettings> section (See "4.4 Define e-mail processing").

The eXpurgate configuration file is sub-divided into sections. Each section begins with a name in angled brackets and ends with the same name preceded by a forward slash, also in angled brackets.

**Example:**

```
<General>
  Options
</General>
```

Each section can contain a series of configuration instructions and possibly further sections. Capitals are ignored in section names and the name of configuration instructions.

The configuration file is sub-divided into the following sections:

- General
- Logging
- SmtplibServer
- SmtplibRelay
- Tls
- SpamEngine
- Freezing
- UserSettings
- Snmp

Comments begin with a hash (#) and stretch to the end of the line. Further files can be bound into the configuration with Include commands. This permits the configuration to be divided up into several individually maintainable files. Each Include directive expects either a file name for inclusion of a single file or a *glob*-compatible search pattern to include multiple files. Include commands can only be used outside sections. The included files must in turn correspond to the full configuration syntax, i.e. they need to define at least one of the sections listed above.

**Example:** (expurgate.conf)

```
<General>
  WorkingDirectory "/var/spool/expurgate"
  LicenseFile "/etc/expurgate/client.key"
</General>
Include "/etc/expurgate/logging.conf"
```

(logging.conf)

```
<Logging>
  FileLog DEBUG-EMERGENCY "/var/log/expurgate.log"
</Logging>
```

It is possible to define one section multiple times. This is a useful technique when Include directives are used. This makes it possible to treat particular aspects of a section separately (e.g. the recipient-specific exceptions in the UserSettings) and does not necessarily result in conflicting section definitions.

It is also possible to use a single directive multiple times. In this case, as a general rule, the last definition simply overrides all others (e.g. WorkingDirectory). However, for a setting, which makes sense to be used multiple times (e.g. Server in the SpamEngine section), the result is the sum of all definitions.

In the following sections below some directives are mentioned which require an argument of the type bool. These directives may be followed by any of the following values:

- Yes, On, True, or 1 to enable the setting
- No, Off, False, or 0 to disable the setting

The various notations are interchangeable.

### 3.2.1. General settings

General settings for the eXpurgate service are specified in the General section.

#### WorkingDirectory

Specification of a working directory for temporarily storing e-mails and other working files.

**Syntax:** WorkingDirectory *path*  
**Example:** WorkingDirectory "/var/spool/expurgate"  
**Default:** *empty*

#### LicenseFile

Specification of the eXpurgate licence file.

**Syntax:** LicenseFile *path*  
**Example:** LicenseFile "/etc/expurgate/client.key"  
**Default:** *empty*

### Sublicense

Specification of the eXpurgate sub-licence key.

**Syntax:** Sublicense *string*

**Example:** Sublicense "abc-123"

**Default:** *empty*

### SublicenseFile

Specification of the eXpurgate sub-licence file.

**Syntax:** SublicenseFile *path*

**Example:** SublicenseFile "/etc/expurgate/client.subkey"

**Default:** *empty*

**Note:** The directives SubLicense and SublicenseFile are alternative ways to specify the sublicense. If both are specified, the last specified overwrites the first.

### Daemonize

Specification as to whether eXpurgate SMTP should change to the background.

**Syntax:** Daemonize *bool*

**Example:** Daemonize Yes

**Default:** No

### UserId

Specification of a user and optionally a group ID under which eXpurgate SMTP is to run. This option can be used if eXpurgate SMTP is to run with a non-privileged user ID but must be started with the root user ID (e.g. to set the incoming port to '25').

**Syntax:** UserId *user[:group]*

**Example:** UserId mail:mail

**Default:** *empty*

### ChangeRoot

Specification of a new root directory into which eXpurgate SMTP should change after starting.

**Syntax:** ChangeRoot *path*

**Example:** ChangeRoot "/opt/expurgate"

**Default:** *empty*

**PidFile**

Specification of a file in which eXpurgate SMTP should write its PID (process ID).

**Syntax:** PidFile *path*

**Example:** PidFile "/var/run/expurgate.pid"

**Default:** *empty*

**Example:**

```
<General>
  WorkingDirectory "/var/spool/expurgate"
  LicenseFile      "/etc/expurgate/client.key"
  PidFile          "/var/run/expurgate.pid"
  UserId           mail:mail
  Daemonize        True
</General>
```

**3.2.2. Logging**

All logging settings are specified in the Logging section. This section permits log messages to be distributed amongst different log files according to their importance.

A range of log levels is defined by specifying the lowest and highest loglevel: ERROR-EMERGENCY includes all log levels from ERROR to EMERGENCY. Lower or upper boundaries can be left out, in case the range starts at the lowest level or ends at the highest. So -NOTICE specifies all levels from DEBUG up to and including NOTICE, whereas ERROR defines the range including all levels higher or equal to ERROR.

The importance levels for log messages are listed in the following.

**DEBUG** Internal log message with low priority.

**INFO** Information on normal functioning.

**NOTICE** Message about specific events.

**WARNING** Warning in case of unusual events.

**ERROR** Message about non-critical error messages.

**CRITICAL** Message about critical error states.

**ALERT** The error state requires immediate intervention .

**EMERGENCY** The system is no longer functional.

As a default, all logs are disabled.

**DefaultTimestamp**

Defines the default timestamp format in a strftime() compatible notation.

**Syntax:** DefaultTimestamp *format*

**Example:** DefaultTimestamp "%Y-%m-%d %H:%M:%S"

**Default:** "[%H-%m-%d %H:%M:%S]"



## FileLog

Write log messages in the given range to the indicated file. The filename may contain `strftime` compatible format strings which are replaced by the current system time when writing a message. By providing a timestamp in `strftime` compatible notation the default timestamp format can be overwritten for this log target.

If the file does not exist, it will be created when the first log message is produced. The same applies for all parent directories. If the file does exist, it is appended to and must be writeable by the user as which `eXpurgate SMTP` is running.

**Syntax:** `FileLog range file [timestamp timestamp]`

**Example:** `FileLog NOTICE "/var/log/expurgate-%Y-%m.log" timestamp "%H:%M:%S"`

## ErrorLog

Write log messages in the given range to the standard error. Optionally the format of the timestamps can be specified in `strftime` compatible notation.

**Syntax:** `ErrorLog range [timestamp timestamp]`

**Example:** `ErrorLog -ERROR timestamp "%c"`

## SysLog

Write log messages in the given range to the system logger. This directive is available on UNIX operating systems only.

Valid facility values are:

- AUTHPRIV
- CRON
- DAEMON
- FTP
- KERN
- LOCAL0 to LOCAL7
- LPR
- MAIL
- NEWS
- SYSLOG
- USER
- UUCP

**Syntax:** `SysLog range facility`

**Example:** `SysLog WARNING-EMERGENCY MAIL`

### ConsoleLog

Write log messages in the given range to the system console. Optionally the format of timestamps can be specified in strftime compatible notation. This directive is available on UNIX operating systems only.

**Syntax:** ConsoleLog *range* [timestamp *timestamp*]

**Example:** ConsoleLog EMERGENCY

### EventLog

Write log messages in the given range to the event log. This directive is available on Windows operating systems only.

**Syntax:** EventLog *range*

**Example:** EventLog ERROR-EMERGENCY

### Example:

```
<Logging>
  FileLog NOTICE "/var/log/expurgate.log"
  Syslog WARNING-EMERGENCY MAIL
</Logging>
```

### Formatted log messages

Individual messages can be modified or deactivated in the Messages sub-section. Each log event can be allocated a format string with different variables. Variables are replaced with concrete values before a log message is output. Empty log messages are suppressed. Variables are referenced within the log messages via a name enclosed in round brackets and preceded by a percent symbol.

### Example:

```
eXpurgate V%(version) starting
```

Every line within the Messages sub-section consists of the name of a log message and the format string to be used.

```
event string
```

All modifiable log messages are output with the NOTICE importance level. No message is output in this level that is not modifiable. A list of all modifiable log messages can be found in section A.5 Log messages.

### Example:

```
<Logging>
  <Messages>
    ARBITER-SCAN "message %(id) recognized as %(type)"
    ARBITER-ACTION "%(action) message %(id) for %(rcptto)"
  </Messages>
</Logging>
```

### 3.2.3. SMTP server

Settings for eXpurgate's SMTP server interface can be specified in the `SmtServer` section.

#### ListenAddress

Specifies the network address and the port for the SMTP interface. This option can be used to receive SMTP data by several network addresses simultaneously.

**Syntax:** `ListenAddress ip[:port]`  
**Example:** `ListenAddress 0.0.0.1:10025`  
**Default:** `0.0.0.0:25`

#### HeloHostname

Specifies the host name in the BANNER and HELO/EHLO response.

**Syntax:** `HeloHostname domain`  
**Example:** `HeloHostname mail.example.com`  
**Default:** `localhost`

#### ReceivedHeader

Defines the format of the Received header inserted by eXpurgate.

**Syntax:** `ReceivedHeader string`  
**Example:** `ReceivedHeader "from %(peer-ip) for <%(rcptto)>"`  
**Default:** `(from %(peer-ip) (helo=%(helo)))\r\n  
 \tbody %(domain) with %(protocol) (eXpurgate %(version))\r\n  
 \t(envelope-from <%(mailfrom)>)\r\n  
 \tfor<%(rcptto)>; %(date))`

#### Extension

Enables or disables supported SMTP extensions. Supported extensions are VRFY, 8BITMIME, XCLIENT, and XFORWARD, AUTH, PIPELINING and DSN. If an extension is not explicitly enabled, it is by default disabled.

**Syntax:** `Extension identifier bool`  
**Example:** `Extension 8BITMIME On`

**Note:** If the PIPELINING extension is disabled, eXpurgate will terminate connections to clients which act not protocol compliant and use PIPELINING even if it is not available.

**Note:** DSNs are not handled by eXpurgate. The DNS parameter are only forwarded to the relay server. eXpurgate will never send delivery status notifications to clients. More information on how to configure SMTP-AUTH could be found in chapter 3.2.3.6.

### TlsOnConnect

Enables or disables TLS support for incoming connections via SMTP.

**Syntax:** TlsOnConnect *bool*

**Example:** TlsOnConnect Yes

**Default:** No

### MailBufferSize

Defines the limit up to which e-mails are buffered in memory. E-mails smaller than the indicated size are processed in memory where possible without being stored in the spool directory.

**Syntax:** MailBufferSize *number*

**Example:** MailBufferSize 0

**Default:** 8192

### ValidateAddresses

Defines whether the relay server validates the sender and the recipient addresses before the e-mail is delivered.

**Syntax:** ValidateAddresses *bool*

**Example:** ValidateAddresses Yes

**Default:** No

### AllowRelayAddresses

Defines whether typical relay addresses are accepted.

Relay addresses are:

- Addresses which contain a complete e-mail address as the local part (e.g. "john@example.com"@company.com)
- Addresses which contain a percent symbol and a domain in the local part (e.g. john%example.com@company.com)
- Addresses which contain one or several exclamation marks (e.g. example.com!john@company.com)

**Syntax:** AllowRelayAddresses *bool*

**Example:** AllowRelayAddresses No

**Default:** No

### MaxConnections

Specifies the maximum number of open connections.

**Syntax:** MaxConnections *number*

**Example:** MaxConnections 5000

**Default:** 0 (*unlimited*)

### MaxInvalidCommands

Specifies the maximum number of unknown commands or syntactical errors in an SMTP connection. Setting this value to zero results in no limit being imposed.

**Syntax:** MaxInvalidCommands *number*

**Example:** MaxInvalidCommands 5

**Default:** 5

### MaxRecipients

Specifies the maximum number of recipients per e-mail. Setting this value to zero results in no limit being imposed on the number of recipients.

**Syntax:** MaxRecipients *number*

**Example:** MaxRecipients 100

**Default:** 100

### MaxMailSize

Specifies the maximum size of an e-mail. Setting this value to zero results in no limit being imposed on the e-mail size.

**Syntax:** MaxMailSize *number*

**Example:** MaxMailSize 10000000

**Default:** 262144000 (*250MB*)

### ConnectionTimeout

Specifies the maximum duration of a connection (0 disables the timeout).

**Syntax:** ConnectionTimeout *seconds*

**Example:** ConnectionTimeout 3600

**Default:** 3600

### DataTimeout

Specifies the maximum time between two commands (0 disables the timeout).

**Syntax:** DataTimeout *seconds*

**Example:** DataTimeout 60

**Default:** 300

### AddStandardHeaders

If this option is enabled, eXpurgate will add any missing standard headers. The added headers conform to the requirements of *RFC 5322*.

**Syntax:** AddStandardHeaders *bool*

**Example:** AddStandardHeaders yes

**Default:** No

### Example:

```
<SmtpServer>
  ListenAddress 0.0.0.0:25
  HelloHostname example.com
  MaxConnections 5000
  MaxMailSize 262144000 # 250 MB
  ConnectionTimeout 3600 # 1 Hour
</SmtpServer>
```

#### 3.2.3.1. Local domains

In the LocalDomains section a list of domains can be specified which are regarded as local. E-mails to local domains are always accepted. E-mails to non-local domains are only accepted if relaying is permitted for the sending server. See the next section.

For each LocalDomains sections can be specified how to handle sub-domains. Therefore the option UseWildCards is available. If this option is missing or set to off, each entry is valid for the domain itself and all sub-domains. If UseWildCards is set to on, it is possible to differentiate between using sub-domains or not. The entry example.com is only valid for e-mails from this domain. Only valid for sub-domains of the domain example.com is the entry \*.example.com. If you want to regard mails as local from the domain itself and including all sub-domains use can use \*example.com.

If the LocalDomains section is empty or missing all domains are considered local.

**Attention:** An open relay can easily be configured if you are careless during configuration.

**Example:**

```
<LocalDomains>
  UseWildCards On
  example.com
  *.example.de
  *example.net
</LocalDomains>
```

### 3.2.3.2. Access control

Authorisations for delivering servers can be defined in the Permissions section. This section consists of a series of sub-sections for various privileges. Each sub-section consists of a list of Allow or Deny instructions with a network mask.

```
Allow netmask
Deny netmask
```

The Connect section regulates which servers may deliver e-mails. All servers are accepted if this section is empty or missing.

The Relay section regulates which servers may deliver e-mails to non-local domains. All servers are rejected if this section is empty or missing.

The XClient and XForward sections regulate which servers may use the XCLIENT and XFORWARD commands. All servers are rejected if these sections are empty or missing.

Please note that the sections Connect, Relay, XClient and XForward are interpreted separately. For instance, to grant relay permission to a subnet, you need to ensure the subnet is also granted connect permission. If this is not the case, a client will be rejected before its relay permission is even checked.

**Example:**

```
<Permissions>
  <Connect>
    Allow 0.0.0.0/0
  </Connect>
  <Relay>
    Allow 192.168.0.0/24
    Deny 0.0.0.0/0
  </Relay>
</Permissions>
```

### 3.2.3.3. Querying DNS Blacklists

eXpurgate is able to check client IPs against one or more DNS blacklists and if necessary terminate the connection to clients. Different blacklists could be weighted in a different way. If a client IP reaches a configurable score, eXpurgate terminates the connection to this client.

The simplest way to configure a DNS blacklist works as follows:

```
<Dnsbl>
  <Blacklist>
    Zone example-dnsbl.net
    Zone example-dnsbl.org
  </Blacklist>
</Dnsbl>
```

In this case eXpurgate will terminate a connection if the client IP address is listed on this list.

The effect of a Blacklist section could be limited to appropriate replies of the blacklist. Therefore you can use the Reject keyword to define an IP address or a range of IP addresses.

You can weight each Blacklist section in a different way by assigning a Score to each section. A connection will be terminated, if the client IP address reaches the value of RejectScore.

```
<Dnsbl>
  RejectScore 2

  <Blacklist>
    Score 2
    Zone example1-dnsbl.net
    Reject 127.0.0.2 - 127.0.0.9
  </Blacklist>

  <Blacklist>
    Score 1
    Zone example2-dnsbl.net
  </Blacklist>

  <Blacklist>
    Score 1
    Zone example3-dnsbl.net
  </Blacklist>
</Dnsbl>
```

In this example a connection will be rejected if the client IP address appears either on example1-dnsbl.net or on both lists example2-dnsbl.net and example3-dnsbl.net.

### 3.2.3.4. Bounce Address Tag Validation (BATV)

eXpurgate offers the possibility to check incoming bounce messages whether they were triggered by an e-mail of the local e-mail system. Previously the local e-mail system has to sign the envelope sender address of the e-mail with a BATV tag. eXpurgate recognizes later the tag in the bounce message and checks whether the BATV tag is valid. If the BATV tag is invalid eXpurgate will reject this message.



It is an important precondition that the local e-mail system uses the *Simple Private Signature (prvs)* for creating the signature. Only this signature is supported by eXpurgate.

You enable BATV by setting the parameter `Enable` to `Yes` in the `Batv` section. Additionally you have to insert a keyword after the parameter `Key` which is used by the local e-mail system for creating the BATV tags. If the local e-mail system uses different keys you can insert several lines in the configuration file.

The parameter `BounceSender` additionally names sender local parts for which to enable the BATV check. If the parameter `BounceSender` is not used, eXpurgate will only check messages without a sender address. This parameter can be used several times.

The parameter `Domain` limits the validation of bounce messages to specific recipient domains. If the parameter `Domain` is not used BATV will be enabled for all recipients. Additionally it is possible to set the values `Optional` or `Enforced` behind the recipient domains. `Optional` means that eXpurgate delivers bounce messages for this recipient domain although they don't have a BATV tag. The value `Enforced` means that eXpurgate rejects bounce messages without a BATV tag for this recipient domain. The value `Enforced` is set by default.

In the `Exceptions` section you can define recipients and clients which may get bounce messages without a BATV tag. For every recipient has to be specified the `Recipient` parameter followed by the e-mail address. If several recipients shall be defined they can be named within the `Recipients` section. For every client has to be specified the `ClientIp` parameter followed by the network. If several clients shall be specified they can be named within the `ClientIps` section.

If an e-mail has an invalid BATV tag and shall be rejected when DATA is received by eXpurgate, the parameter `DelayReject` have to be set.

#### Example:

```
<Batv>
  Enable Yes
  Key "secret"

  BounceSender MailerDaemon
  Domain example.com
  Domain *.example.de
  Domain *example.net Enforced
  Domain example.de Optional

  <Exceptions>
    Recipient foobar@example.com
    ClientIp 172.16.0.0/12

    <Recipients>
      john@example.com
      jane@example.com
    </Recipients>

    <ClientIps>
      10.0.0.0/8
      192.168.0.1/32
    </ClientIps>
  </Exceptions>

  DelayReject Yes
</Batv>
```

The Domain entries have the following meaning in the example above: The entry `example.com` enables the BATV check to this domain, but not its sub-domains. The entry `*.example.de` enables BATV checks for sub-domains of the domain `example.de` only. The entry `*example.net` enables the BATV check for the domain itself and all its sub-domains. The value `Optional` is set for domain `example.de` to accept e-mails to this recipient domain without a BATV tag. Bounce messages to the recipients `foobar@example.com`, `john@example.com`, `jane@example.com` and bounce messages from the clients `172.16.0.0/12`, `10.0.0.0/8`, `192.168.0.1/32` do not have a BATV tag. They will be passed by the BATV check of eXpurgate.

### 3.2.3.5. Sender Policy Framework (SPF)

eXpurgate offers the possibility to check inbound e-mails by the SPF method. For it eXpurgate checks the HELO and MAIL FROM identity of the SMTP client by requesting a SPF rule from the DNS. eXpurgate processes the received SPF rule and checks whether the SMTP client is authorized to use the sender domain. If not the e-mail will be rejected.

In the current version, eXpurgate requests only TXT records from the DNS to obtain the SPF rules. If no SPF rule was found the SPF check is not performed for this e-mail.

You enable the SPF check by setting the parameter `Enable` in the `Spf` section. Additionally you have the possibility to switch the HELO check on by setting the parameter `HeloCheck` to `Yes`. The SPF check of MAIL FROM is not configurable and will be executed every time.

The parameter `HostDomain` sets the name of your host. If necessary the value of `HostDomain` is required for generating SMTP responses. If no value is specified eXpurgate uses the value of `HeloHostname` in the `SmtptServer` section by default.

Sometimes it is required that several e-mail clients shall be excepted by the SPF check. Use the `NoCheck` sub-section to specify these e-mail clients.

#### Example:

```
<Spf>
  Enable Yes

  HeloCheck Yes
  HostDomain example.com

  <NoCheck>
    127.0.0.1/32
    192.168.0.0/16
  </NoCheck>
</Spf>
```

### 3.2.3.6. Authentication via SMTP AUTH

SMTP Clients may be authenticated using the *SMTP AUTH* protocol extension (RFC 4954). Authentication is done via the downstream server using the PLAIN mechanism (RFC 4616). This requires the protocol extension to be activated using the *Extension* directive. Detailed settings may be configured in the *Authentication* section.

#### Example:

```
Extension AUTH on

<Authentication>
  Disabled 127.0.0.1/32
  Optional 192.168.0.0/16
  Enforced 0.0.0.0/0

  RequireTls yes
</Authentication>
```

The *Disabled*, *Optional*, and *Enforced* directives are each followed by a netmask. The *Optional* directive is the default setting: This makes authentication available for the specified subnet, but does not require it. Using *Disabled* authentication is disabled for the specified subnet. Using *Enforced* all SMTP commands except HELO, EHLO, NOOP, RSET, and AUTH are denied until the client is authenticated successfully. The *Disabled*, *Optional*, and *Enforced* directives may be used multiple times.

The *RequireTls* directive results in authentication to not be made available until the connection is secured via TLS.

### 3.2.3.7. SMTP protocol messages

All SMTP server responses can be freely configured. A *Messages* section must be created similar to the log messages in which every SMTP response is allocated to a format string. A list of all SMTP protocol messages can be found in section A.6.

#### Example:

```
<Messages>
  banner "%(domain) eXpurgate ESMTP ready"
  quit "Bye Bye"
</Messages>
```

### 3.2.4. SMTP relay

eXpurgate attempts to use stable connections for e-mails processed for dispatch to its relay server. It is also possible to specify several relay servers and prioritise them.

Servers which belong together are grouped together in a so-called pool. Each pool is defined by a `Pool` sub-section. All relay servers grouped in a pool are regarded as equivalent apart from their priority and use the same settings.

Which of the defined pools is used to send an e-mail can be specified via the `UserSettings` section. See also Section 4.

At least one pool always exists, the so-called default pool. This pool is always used if another pool has not been specifically designated for dispatch.

#### AutoXforward

Defines whether eXpurgate will pass the IP address of the submitting client to the relay server using the `XFORWARD` command.

This option has global scope and can not be defined separately per pool.

**Syntax:** `AutoXforward bool`  
**Example:** `AutoXforward On`  
**Default:** `Off`

#### AutoXclient

Defines whether eXpurgate will pass the attributes of the submitting client to the relay server using the `XCLIENT` command.

This option has global scope and can not be defined separately per pool.

**Syntax:** `AutoXclient bool`  
**Example:** `AutoXclient On`  
**Default:** `Off`

#### Name

Defines the name with which a pool can be selected. This directive is only usable in a `Pool` sub-section. Please note that the name "Quarantine" has a special meaning and is used for e-mails that should be quarantined.

**Syntax:** `Name identifier`  
**Example:** `Name "VIP-Customers"`  
**Default:** `empty`

### MaxPoolSize

Specifies the maximum number of simultaneously open connections in this pool.

**Syntax:** MaxPoolSize *number*

**Example:** MaxPoolSize 50

**Default:** 0 (*unlimited*)

### DataTimeout

Specifies the maximum time period between two commands or two chunks of data. Zero (0) deactivates the timeout.

**Syntax:** DataTimeout *number*

**Example:** DataTimeout 60

**Default:** 600

### MaxMailsPerConnection

Specifies the maximum number of e-mails that may be sent via a connection before it is closed (0 = unlimited).

**Syntax:** MaxMailPerConnection *number*

**Example:** MaxMailsPerConnection 50

**Default:** 50

### Helo

Specifies the domain name used in HELO/EHLO. The Pass-through value ensures that the domain name used when the mail was delivered is used.

**Syntax:** Helo *domain*

**Example:** Helo example.com

**Default:** *HeloHostname from SmtplibServer*

**Attention:** If the Passthrough value is used, eXpurgate sends HELO/EHLO several times on one outgoing connection. This can lead to problems on some mailservers, for example Sendmail.

### Server

Specifies an SMTP relay server for this pool.

**Syntax:** Server *host[:port]* [*prio number*]

**Example:** Server 127.0.0.1:25

**Default:** *empty*

### AsciiConversion

If set to yes, eXpurgate will convert the mail body to *US-ASCII*, if the recipient does not support the *8BITMIME* extension. If this option is disabled, eXpurgate sends all mails without conversion to the relay server. If the relay server does not support *8BITMIME*, non-*US-ASCII* characters will be destroyed during transmission.

**Syntax:** AsciiConversion *bool*

**Example:** AsciiConversion yes

**Default:** No

### Encryption

Use the Encryption directive to determine whether TLS is Optional or Enforced, or whether the *common name* (CN) is Verified. If the Verified keyword is followed by a string argument, the peer certificates' *common name* (CN) must match this argument. Otherwise the *common name* must match the hostname obtained through a reverse DNS lookup.

**Syntax:** Encryption Optional|Enforced|Verified [*string*]

**Example:** Encryption Verified

**Default:** Optional

### TrustedCertificate

Defines the contained certificates as trustworthy for outgoing connections.

**Syntax:** TrustedCertificate *path*

**Example:** TrustedCertificate "/etc/ssl/ca.cert"

**Default:** *empty*

### TrustedCertificateDirectory

Defines all certificates in a directory as trustworthy for outgoing connections. The certificate files must be named after the hash of the contained certificate.

**Syntax:** TrustedCertificateDirectory *path*

**Example:** TrustedCertificateDirectory "/etc/ssl/certs"

**Default:** *empty*

### Example:

```
<SmtpRelay>
  <Pool>
    Default
    Helo passthrough
    Server 127.0.0.1:25
  </Pool>
</SmtpRelay>
```

**Note:** You can define the default settings for the SMTP relay either directly in the `SmtptRelay` section (as done in the sample configuration included at the end of this manual), or in a `Pool` sub-section with the special keyword `Default` (as shown in the example above). Both configurations have the same effect.

### 3.2.5. TLS

The eXpurgate software permits the reception and dispatch of e-mails via TLS-encrypted connections. Apart from encryption of the communication it is also possible to verify the authenticity of the respective communication partner.

A private key and a certificate to X.509 are required for encrypted reception. eXpurgate can deal with self-signed certificates and certificates from a Certificate Authority.

Neither a certificate nor a key is required for dispatch. If a certificate exists, this is also used for identification when dispatching. Certificates and keys can be in DER or PEM format. The PEM format permits the keys and the certificate to be stored in the same file and a certificate to be defined.

All options concerning encrypted incoming connections communication are defined in the section `Tls`. Options to handle TLS for outgoing connections are configured in Section 3.2.4.

#### Certificate

Specifies the certificate file.

**Syntax:** `Certificate path`

**Example:** `Certificate "/etc/expurgate/server.crt"`

**Default:** `empty`

#### PrivateKey

Specifies the private key.

**Syntax:** `PrivateKey path`

**Example:** `PrivateKey "/etc/expurgate/server.key"`

**Default:** `empty`

#### TrustedCertificate

Defines the contained certificates as trustworthy.

**Syntax:** `TrustedCertificate path`

**Example:** `TrustedCertificate "/etc/ssl/ca.cert"`

**Default:** `empty`

### TrustedCertificateDirectory

Defines all certificates in a directory as trustworthy. The certificate files must be named after the hash of the contained certificate.

**Syntax:** `TrustedCertificateDirectory path`

**Example:** `TrustedCertificateDirectory "/etc/ssl/certs"`

**Default:** `empty`

**Note:** If private key and certificate are stored in the same file, both options, `Certificate` and `PrivateKey`, have to be provided, nevertheless.

**Note:** The directives `TrustedCertificate` and `TrustedCertificateDirectory` are also usable in the sub-section `Policy`.

All further TLS settings are based on the sender- and recipient domain or on the client IP address. This is done recipient-based and are defined in `Policy` sections. A `Policy` section can either refer to one or more target domains or be a default for all domains not specifically named.

### Subsection Policy

A `Policy` section can either refer to one or more target domains or be a default for all domains not specifically named.

### Default

Defines the section as the default policy. That means, this sections is valid vor all domains not specifically named.

### Domain

Defines the section as the policy for a specific recipient domain.

**Syntax:** `Domain domain`

**Example:** `Domain example.com`

### Refinement of rules and using Validation

Individual encryption and authentication rules can be defined for different sender domains or client IP addresses within a `Policy` section. This is done via `Validation` sections.



## Default

Defines these validation rules as the default. That means, this section is valid for all incoming connections which are not covered by other Validation sections.

## Sender

Allocates the validation rules to a sender domain.

**Syntax:** Sender *domain*

**Example:** Sender random.com

## ClientIp

Allocates the validation rule to a range of client IP addresses.

**Syntax:** ClientIp *netmask*

**Example:** ClientIp 192.168.0.0/24

## Encryption

Use the Encryption directive to determine whether TLS is optional or enforced, or whether the *common name* (CN) is verified. If the Verified keyword is followed by a string argument, the peer certificates' *common name* (CN) must match this argument. Otherwise the *common name* must match the hostname obtained through a reverse DNS lookup.

**Syntax:** Encryption Optional|Enforced|Verified [*string*]

**Example:** Encryption Verified

**Default:** Optional

Default Policy and default Validation section settings can also be placed outside the relevant sections.

## Example:

```
<Tls>
  <Validation>
    Default
    Encryption Optional
  </Validation>

  <Policy>
    Domain example.com
    TrustedCertificateDirectory "/etc/ssl/certs"

    <Validation>
      Sender trusted.com
      Encryption Enforced
    </Validation>
```

```

    <Validation>
      ClientIp 192.168.0.0/24
      Encryption Verified "HighSec Inc."
    </Validation>
  </Policy>
</Tls>

```

### 3.2.6. Spam recognition

All general spam recognition and e-mail categorisation settings are defined in the SpamEngine section.

#### Server

Specifies an eXpurgate server for the categorization of e-mails.

**Syntax:** Server *host[:port]* [*prio number*]

**Example:** Server exa.expurgate.net:55555 prio 0

**Default:** All public eleven eXpurgate Server

#### SocksProxy

Specifies a SOCKS5 proxy for the connection to the eXpurgate servers. Optionally a username and password can be specified for the SOCKS server.

**Syntax:** *host[:port]* [*user string*] [*password string*]

**Example:** SocksProxy proxy.intern:1080 user "proxyuser" password "secret"

**Default:** empty

#### DangerousExtensions

Defines the list of file extensions considered to be dangerous.

**Syntax:** DangerousExtensions *string*

**Example:** DangerousExtensions "exe,com,scr,vbs"

**Default:** "ade, adp, app, asp, bas, bat, bhx, cab, ceo, chm, cmd, com, cpl, crt, csr, der, exe, fxp, hlp, hta, inf, ins, isp, its, js, jse, lnk, mad, maf, mag, mam, mar, mas, mat, mde, mim, msc, msi, msp, mst, ole, pcd, pif, reg, scr, sct, shb, shs, vb, vbe, vbmacros, vbs, vsw, wmd, wmz, ws, wsc, wsf, wsh, xxe"

### EnableGtube

Defines whether the GTUBE test signature leads to a spam classification. Activating this option can lead to a decrease in performance.

**Syntax:** `EnableGtube bool`

**Example:** `EnableGtube Off`

**Default:** `No`

### Threads

Defines how many e-mails can be processed in parallel. A high value can increase performance but leads to increased use of resources.

**Syntax:** `Threads number`

**Example:** `Threads 64`

**Default:** `32`

### TempRejectOnError

Defines if a communication error occurs with the eXpurgate servers, then E-Mail is either temporarily delayed, or classified as 'clean'.

**Syntax:** `TempRejectOnError bool`

**Example:** `TempRejectOnError On`

**Default:** `Yes`

### Example:

```
<SpamEngine>
  Threads 64
  DangerousExtensions "exe,com,pif"
  EnableGtube Yes
</SpamEngine>
```

#### 3.2.6.1. Subsection Antivir

Settings for the AntiVir virus scanner are specified in the Antivir sub-section.

### Enable

Defines whether the AntiVir virus scanner should be used.

**Syntax:** `Enable bool`

**Example:** `Enable Yes`

**Default:** `No`

## Port

Specifies the port via which the virus scanner is to be addressed.

**Syntax:** Port *number*

**Example:** Port 55556

**Default:** 55556

## MaxPoolSize

Specifies the maximum number of parallel connections to the virus scanner.

**Syntax:** MaxPoolSize *number*

**Example:** MaxPoolSize 20

**Default:** 3

## Extensions

Defines the list of all file types that should be examined by the virus scanner.

**Syntax:** Extensions *string*

**Example:** Extensions "exe,com,cmd"

**Default:** "ade, adp, bas, bat, bhx, ceo, chm, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mde, mim, msc, msi, msp, mst, ole, pcd, pif, reg, scr, sct, shb, shs, vb, vbe, vbs, wmd, wmz, wsc, wsf, wsh, xxe, cla, class, dll, drv, fon, ocx, sys, vxd, doc, docm, docx, dot, dotm, dotx, mda, mdb, pot, potm, potx, pps, ppsm, ppsx, ppt, pptm, pptx, ppo, rtf, xls, xlsb, xlsx, xlt, emf, flt, jfif, jif, jng, jp2, jpe, jpeg, jpg, png, swf, wmd, wmf ace, arj, bz2, cab, cpio, gz, gzip, jar, lha, lzh, rar, rpm, tar, tbz2, tgz, zip, zoo"

## MaxScanDepth

Specifies the maximum recursion depth when scanning archives or similar types of nested files. If the value is set to zero, the scanning of archives is disabled.

**Syntax:** MaxScanDepth *number*

**Example:** MaxScanDepth 10

**Default:** 5

## MaxScanSize

Specifies the maximum size of the files to be scanned.

**Syntax:** MaxScanSize *number*

**Example:** MaxScanSize 100000000

**Default:** 0 (*unlimited*)

### Example:

```
<Antivir>
  Enable Yes
  Port 55556
  MaxPoolSize 20
  AntivirExtensions "exe,com,cmd"
  MaxScanDepth 10
</Antivir>
```

### 3.2.6.2. Subsection NoFilter

Local e-mails can be exempted from categorisation by eXpurgate with the NoFilter sub-section. E-mails, which have only a limited number of received lines of a defined value, count as local.

## Enable

Activates the exemption of local e-mails.

**Syntax:** Enable *bool*

**Example:** Enable Yes

**Default:** No

## Network

Defines a network whose e-mails will be exempted from categorisation.

**Syntax:** Network *netmask*

**Example:** Network 10.0.0.0/8

**Default:** *empty*

## MaxReceivedHeaders

Defines the maximum number of Received headers in local e-mails.

**Syntax:** MaxReceivedHeaders *number*

**Example:** MaxReceivedHeaders 2

**Default:** 0 (*none*)

### ReceivedHeaderRegex

Defines the format of permitted Received lines in the form of a Perl-compatible regular expression.

**Syntax:** ReceivedHeaderRegex *pattern*

**Example:** ReceivedHeaderRegex /from 192\..168\./

**Default:** /\[10(\.[0-9]{1,3}){3}\]  
|\[127(\.[0-9]{1,3}){3}\]  
|\[172\..16(\.[0-9]{1,3}){2}\]  
|\[169\..254(\.[0-9]{1,3}){2}\]  
|\[192\..168(\.[0-9]{1,3}){2}\]/

#### Example:

```
<SpamEngine>
  <NoFilter>
    Enable Yes
    MaxReceivedHeader 1
    ReceivedHeaderRegex /from 127\..0\..0\..1/
  </NoFilter>
</SpamEngine>
```

### 3.2.7. Freezing

With the help of the Freezing functionality, e-mails which already fulfil the mass mail criterion but which have not yet been identified as spam can be briefly delayed and examined again at a later point in time. This leads to even better spam recognition.

All settings to do with this functionality are specified in the Freezing section.

#### Enable

Defines whether the Freezing functionality should be activated.

**Syntax:** Enable *bool*

**Example:** Enable Yes

**Default:** No

#### FridgeDirectory

Defines the directory in which delayed e-mails are stored. This directory may not be the working directory and must be located on the same storage medium as the working directory.

**Syntax:** FridgeDirectory *path*

**Example:** FridgeDirectory "/var/spool/expurgate-fridge"

**Default:** *empty*

### CheckInterval

Defines at what intervals delayed e-mails should be examined.

**Syntax:** CheckInterval *seconds*

**Example:** CheckInterval 60

**Default:** 30

### DayTime

Defines which period of time counts as daytime and which as nighttime. Different maximum freezing times can apply during the day and night periods.

**Syntax:** DayTime *from to*

**Example:** DayTime 7:00 20:00

**Default:** 7:00 2:30

### MaxFreezingTime

Defines the maximum delay for an e-mail in seconds during daytime and nighttime. The second argument is optional — if omitted, the first argument is valid for both daytime and nighttime.

**Syntax:** MaxFreezingTime *day night*

**Example:** MaxFreezingTime 300 3600

**Default:** 1200 7200

### InvalidRecipientLimit

Defines the number of invalid recipients to trigger freezing. The value 0 disables this functionality.

**Syntax:** InvalidRecipientLimit *number*

**Example:** InvalidRecipientLimit 1

**Default:** 0

### MaxThawTasks

Defines the number of tasks responsible for examining delayed e-mails.

**Syntax:** MaxThawTasks *number*

**Example:** MaxThawTasks 2

**Default:** 20

### MaxFrozenMails

Defines the maximum number of frozen e-mails.

**Syntax:** MaxFrozenMails *number*

**Example:** MaxFrozenMails 500

**Default:** 10000

#### Example:

```
<Freezing>
  Enable Yes
  FridgeDirectory "/var/spool/expurgate/fridge"
  Daytime 7:30 21:00
  MaxFreezingTime 180
  CheckInterval 10
</Freezing>
```

### 3.2.8. Simple Network Management Protocol (SNMP)

eXpurgate supports the Simple Network Management Protocol (SNMP) with which it can be monitored by a network management software. A precondition is that the network management software knows the data it can be queried from eXpurgate. This information is stored in MIB files (ELEVEN-MIB.mib and ELEVEN-EXPURGATE-MIB.mib) which are provided by the eleven GmbH. They are located in `/usr/share/doc/expurgate` on Unix systems and in `C:\Programme\eleven\eXpurgate\doc` on Microsoft Windows. The MIB files require the standard MIBs SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, SNMP-FRAMEWORK-MIB, INET-ADDRESS-MIB and HCNUM-TC which have to be installed on your system.

Currently eXpurgate supports the SNMP version 2c.

All SNMP settings are defined in the `Snmp` section of configuration file.

#### Enable

Enables or disables SNMP support of eXpurgate.

**Syntax:** Enable *bool*

**Example:** Enable Yes

**Default:** No

#### ListenAddress

Specifies the network interface and the port for the SNMP interface.

**Syntax:** ListenAddress *ip[:port]*

**Example:** ListenAddress 0.0.0.1:161

**Default:** 0.0.0.0:161



## UseTcp

eXpurgate uses the User Datagram Protocol (UDP) for communication via SNMP by default. Alternatively the Transmission Control Protocol (TCP) can be enabled by setting the parameter `UseTcp` to `Yes`.

**Syntax:** `UseTcp bool`

**Example:** `UseTcp Yes`

**Default:** `No`

## Community

You have the possibility to assign a password to query data from eXpurgate. Caution: The password of eXpurgate and the network management software have to be equal.

**Syntax:** `Community string`

**Example:** `Community "public"`

**Default:** `empty`

## Example:

```
<Snmp>
  Enable Yes
  ListenAddress 0.0.0.0:161
  UseTcp No
  Community "public"
</Snmp>
```

The data are arranged in tables and they can be viewed with a MIB browser. The following tables will be shown:

| Table                                 | Description  |
|---------------------------------------|--|
| <code>expurgateGlobal</code>          | Contains general informations about eXpurgate.   |
| <code>exServiceInTable</code>         | Shows the current data of the inbound network service.   |
| <code>exServiceOutTable</code>        | Stores the current data of the outbound network service.   |
| <code>exSmtpServiceInTable</code>     | Contains the data about the SMTP communication between the inbound e-mail servers and eXpurgate. |
| <code>exSmtpServiceOutTable</code>    | Contains the data about the SMTP communication between eXpurgate and the local e-mail servers.   |
| <code>exSmtpConnectionInTable</code>  | Shows informations about the current SMTP connections of inbound e-mail servers.                 |
| <code>exSmtpConnectionOutTable</code> | Shows informations about the current SMTP connections to the local e-mail servers.               |
| <code>exMessageTypeInTable</code>     | Stores data about the categorization of inbound e-mails.   |
| <code>exSmtpErrorInTable</code>       | Stores informations about SMTP rejects.  |
| <code>expurgateFridge</code>          | Contains informations about the fridge in eXpurgate.   |

### 3.2.9. Lightweight Directory Access Protocol (LDAP)

eXpurgate offers the possibility to delegate parts of its configuration to an external server using the LDAPv3 protocol. LDAP settings are defined in the Ldap section of the configuration file.

Currently, only recipient validation may be delegated to an LDAP server.

#### Enable

Enables or disables LDAP support of eXpurgate.

**Syntax:** Enable *bool*  
**Example:** Enable Yes  
**Default:** No

#### Library

This option sets the library which is necessary for the communication via LDAP. You can specify a path to the library or the name of the library. If the library name is used without a path the library is searched by a standard search strategy in the filesystem.

**Syntax:** Library *path*  
**Example:** Library "/usr/local/lib/libldap\_r.so"  
**Default:** "libldap\_r.so" (*unix*)  
**Default:** "wldap32.dll" (*windows*)

#### Server

Specifies the LDAP server. This option can be used multiple times.

**Syntax:** Server "*uri*" [*prio number*]  
**Example:** Server "ldap://ldap-server1.here.it.is:3456" prio 0  
**Default:** *empty*

#### MaxConnections

The maximal number of connections to an LDAP server is set by this option.

**Syntax:** MaxConnections *number*  
**Example:** MaxConnections 10  
**Default:** 2

## Bind

The Bind option defines how eXpurgate authenticates against the LDAP server by specifying an authentication method and optionally a username and password.

eXpurgate supports the authentication methods basic, simple, and authentication via SASL. The simple and basic authentication methods require a Bind DN and a password to be specified. The SASL authentication method may not require a username or password to be specified, depending on the SASL mechanism negotiated with the LDAP server.

You can limit the available SASL mechanisms by specifying a list of allowed mechanisms.

**Syntax:** Bind [*auth*] ["dn" [Password "*string*"]]

**Syntax:** Bind sasl[=*mechanisms*] ["dn" [Password "*string*"]]

**Example:** Bind simple "cn=expurgate,ou=users,c=de,o=company" Password "secret"

**Example:** Bind sasl=plain,digest-md5 "cn=expurgate,ou=users,c=de,o=company"  
Password "secret"

**Default:** Bind SASL

### Example:

```
<Ldap>
  Enable Yes
  Library "/usr/lib/libldap_r.so"

  Server "ldaps://ldap1.server:3456" prio 0
  Server "ldaps://ldap2.server:3456" prio 1

  MaxConnections 10

  Bind sasl=PLAIN,CRAM-MD5 "cn=expurgate,ou=users,c=de,o=company" Password "secret"

  <Query>
    QueryType Recipients
    Search "ou=users,c=de,o=company" Filter "(proxyAddresses=smtp:%(recipient))"
  </Query>
</Ldap>
```

#### 3.2.9.1. Queries for an LDAP server

eXpurgate uses the LDAP connection to send queries to a server. These queries can be configured in the configuration file. If you want to use the recipient validation via LDAP the query type Recipients is available.

Generally it is defined that a query overwrites a section in the configuration file which has the same functionality. This means for the recipient validation that the Recipients query overwrites the Recipients sub-section of the SmtServer section.

All query options are defined in the Query section.

### QueryType

Specifies which query shall be send to the LDAP server.

**Syntax:** QueryType *string*

**Example:** QueryType Recipients

**Default:** *empty*

### Search

The Search option assigns the position in the LDAP directory tree where to start the search for an object. The Filter defines a criterion of an object that have to be added to the result. Additionally the placeholder `%(recipient)` is available for the recipient validation. It replaces the e-mail address of a recipient.

**Syntax:** Search "*baseDn*" Filter "*string*"

**Example:** Search "ou=users,c=de,o=company" Filter "(proxyAddresses=smtp:%(recipient))"

**Default:** *empty*

### Example:

```
<Query>
  QueryType Recipients

  Search "ou=users,c=de,o=company" Filter "(mail:\%(recipient))"
</Query>
```

## 3.2.10. eXelerate

eXpurgate can delegate parts of its configuration to the eleven eXelerate middleware server.

### Server

Specifies the eXelerate server address.

**Syntax:** Server *host[:port]* [*prio number*]

**Example:** Server exelerate.example.com:11223 prio 0

**Default:** *none*

### DataTimeout

Defines the response timeout in seconds when querying an eXelerate server.

**Syntax:** DataTimeout *number*

**Example:** DataTimeout 5

**Default:** 30

## MaxConnections

Specifies the maximum number of open connections.

**Syntax:** MaxConnections *number*

**Example:** MaxConnections 5

**Default:** 2

## Query

Defines which parts of the configuration should be delegated to eXelerate.

**Syntax:** Query *query-type* *boolean*

**Example:** Query Recipients On

**Default:** *all off*

### Example:

```
<Exelerate>
  Server x11.example.com prio 0
  Server x12.example.com prio 1

  DataTimeout 5
  MaxConnections 10

  Query LocalDomains on
  Query Recipients on
  Query Blacklists on
</Exelerate>
```

All available eXelerate queries are defined in the file *exelerate-expurgate.conf*. Skeleton implementations for the eXelerate query functions are provided in the file *exelerate-expurgate.lua*. Both files are located in the package documentation directory after installation.

### 3.2.10.1. Local Domains Query

The Local Domains Query is used to determine whether a domain is considered local. This query replaces the <LocalDomains> section in the configuration file.

#### Query Identifier

```
Query LocalDomains On
```

### Request Structure

```
<Struct ExLocalDomainRequest>  
  Domain domain  
</Struct>
```

domain    The domain part of a recipient e-mail address.

### Response Structure

```
<Struct ExLocalDomainResponse>  
  Bool islocal  
</Struct>
```

islocal    Whether the domain is considered a local domain.

#### 3.2.10.2. Recipient Validation Query

The Recipient Validation Query is used to determine whether a recipient e-mail address exists. This query replaces the <Recipients> section within the <SmtpServer> section in the configuration file.

### Query Identifier

```
Query Recipients On
```

### Request Structure

```
<Struct ExRecipientValidationRequest>  
  EmailAddress recipient  
</Struct>
```

recipient    The recipient e-mail address.

### Response Structure

```
<Struct ExRecipientValidationResponse>  
  Bool exists  
</Struct>
```

exists    Whether the e-mail address is a valid recipient address.

### 3.2.10.3. Blacklist Query

The Blacklist Query is used to determine whether an IP address or mail-from address is blacklisted in general or for a particular recipient e-mail address. This query replaces the <Blacklists> section within the <SmtpServer> section in the configuration file.

#### Query Identifier

```
Query Blacklists On
```

#### Request Structure

```
<Struct ExBlacklistRequest>
  IPAddress    client
  EmailAddress sender
  EmailAddress recipient
</Struct>
```

client     The IP address of the submitting server.

sender     The envelope mail-from address.

recipient   The recipient e-mail address.

#### Response Structure

```
<Enum ExBlacklistReason>
  Ok      0
  Ip      1
  Email   2
</Enum>

<Struct ExBlacklistResponse>
  ExBlacklistReason reason
</Struct>
```

reason     The blacklist reason. Ip if the submitting server's IP address is blacklisted Email if the sender email address is blacklisted or Ok if neither is blacklisted.

### 3.2.10.4. BATV Policy Query

The BATV Policy Query is used to determine whether BATV checks apply for a given SMTP transaction. This query replaces parts of the <Batv> section within the <SmtpServer> section in the configuration file.

**Query Identifier**

```
Query Batv On
```

**Request Structure**

```
<Struct ExBatvPolicyRequest>
  IPAddress    client
  EmailAddress sender
  EmailAddress recipient
</Struct>
```

client     The IP address of the submitting server.

sender     The envelope mail-from address.

recipient   The recipient e-mail address.

**Response Structure**

```
<Enum ExBatvPolicy>
  Optional 0
  Enforced 1
</Enum>

<Struct ExBatvPolicyResponse>
  ExBatvPolicy policy
</Struct>
```

policy     Whether bounce messages require BATV tags.

**3.2.10.5. TLS Policy Query**

The TLS Policy Query is used to determine which TLS/SSL policy applies to a given SMTP transaction. This query replaces the Validation section within the <Tls> section in the configuration file.

**Query Identifier**

```
Query TlsPolicy On
```



**Request Structure**

```
<Struct ExTlsPolicyRequest>
  IPAddress    client
  EmailAddress sender
  EmailAddress recipient
</Struct>
```

client     The IP address of the submitting server.

sender     The envelope mail-from address.

recipient   The recipient e-mail address.

**Response Structure**

```
<Enum ExTlsPolicy>
  Optional 0
  Enforced 1
  Validated 2
</Enum>

<Struct ExTlsPolicyResponse>
  ExTlsPolicy policy
  Text subject
  Text store
</Struct>
```

policy     Whether TLS/SSL encryption is required and how a the client certificate is to be validated.

subject     The expected subject field of the client certificate. Used only when policy is Validated.

store       Identifier for the store of trusted certificates to validate against. Used only when policy is Validated.

**3.2.10.6. TLS Store Query**

The TLS Store Query is used to retrieve certificate stores for client certificate verification. This query replaces the TrustedCertificate and TrustedCertificateDirectory settings in the <Tls> section in the configuration file.

**Query Identifier**

```
Query TlsPolicy On
```

### Request Structure

```
<Struct ExCertificateStoreRequest>  
  Text identifier  
</Struct>
```

identifier The certificate store identifier as specified by the store field in the TLS Policy Response.

### Response Structure

```
<Struct ExCertificateStoreResponse>  
  List(Binary) certificates  
</Struct>
```

certificates The list of all certificates in the store. The certificates can be encoded in any format supported by OpenSSL.

#### 3.2.10.7. User Feature Query

The User Feature Query is used to configure the classification engine. This query replaces the Feature setting in the <UserSettings> section in the configuration file.

### Query Identifier

```
Query Features On
```

### Request Structure

```
<Struct ExUserFeatureRequest>  
  EmailAddress recipient  
</Struct>
```

recipient The recipient e-mail address.

**Response Structure**

```

<Enum ExUserFeature>
  Spam      0
  Virus     1
  Outbreak  2
  Freezing  3
</Enum>

<Struct ExUserFeatureResponse>
  List(ExUserFeature) features
</Struct>

```

features The list of enabled features for the queried recipient.

**3.2.10.8. Mail Action Query**

The Mail Action Query is determines how to treat a message after classification. This query replaces the <MailAction> section in the <UserSettings> section in the configuration file.

**Query Identifier**

```
Query MailActions On
```

**Request Structure**

```

<Enum ExMajorMailType>
  Clean      0
  Spam       1
  Bulk       2
  Dangerous  3
</Enum>

<Enum ExMinorMailType>
  Normal      0

  Empty       1
  AlmostEmpty 2
  EmptyBody   3
  Bounce      4

  Advertising 5
  Porn        6

  Virus       7
  Attachment  8
  Code        9
  Iframe      10
  Outbreak    11
</Enum>

<Struct ExMailType>
  ExMajorMailType major

```

```

    ExMinorMailType minor
</Struct>

<Enum ExProcessingStage>
    BeforeQueue 0
    AfterQueue 1
</Enum>

<Struct ExMailActionRequest>
    IPAddress      client
    EmailAddress   sender
    EmailAddress   recipient
    ExMailType     type
    ExProcessingStage stage
</Struct>

```

client     The IP address of the submitting server.

sender     The envelope mail-from address.

recipient   The recipient e-mail address.

type       The classification of the message.

stage       Indicates whether the message has been frozen.

### Response Structure

```

<Enum ExMailActionType>
    AddHeader      0
    RemoveHeader   1
    RewriteSubject 2
    Deliver         3
    Delete          4
    Reject          5
    Forward         6
    Redirect        7
    HandleAs        8
</Enum>

<Struct ExMailAction>
    ExMailActionType type
    Text parameter
</Struct>

<Struct ExMailActionResponse>
    List(ExMailAction) actions
</Struct>

```

actions     A list of actions to be executed for this message.

## 4. Fine tuning e-mail handling

### 4.1. Processing rules

The `UserSettings` section specifies how incoming e-mails are to be treated before and after categorization. A differentiation is made between global actions, which apply for all recipients of a mail and domain, and recipient-specific settings.

Functions such as a filter exclusion for individual domains and recipients can be configured in this section, and also black- and whitelists based on the IP address of the sending host and the sender or receipt of an e-mail.

#### Global versus recipient-specific settings

In the `UserSettings` it is possible to define settings which apply for every recipient of a mail. It is also possible to apply settings just to domains and recipients.

If commands appear directly below the `UserSettings` section they initially apply globally for every recipient. Limitations are possible through embedding the commands in a `Recipient` section. In operation, eXpurgate first looks for as precise a match of the recipient as possible and uses their settings. If no recipient-specific setting is found, then the global settings are used.

#### Example:

```
<UserSettings>
  # Global directives
  <Recipient>
    # Directies apply only to defined recipients
  </Recipient>
</UserSettings>
```

### 4.2. Defining a recipient

Recipients are defined in `Recipient` sections in which limitations are specified by `Domain`, `Domains`, `Address` and `Addresses` commands.

### 4.2.1. Selecting by domains

A domain for which the settings are to apply can be defined with the `Domain` command.

**Example:**

```
<Recipient>
  Domain example1.com
  Domain *example2.com
  Domain *.example3.com
  # Further directives
</Recipient>
```

Here, a limitation for the following command for the named domains is specified with three `Domain` commands.

An asterisk `*` can also be used as a wildcard:

- `*example2.com` affects all sub-domains of `example2.com` including `example2.com` itself. This `Recipient` section would therefore apply for recipients with the `department1.example2.com` domains and also `example2.com`.
- `*example3.com` applies for all sub-domains but not the `example3.com` domain itself. E-mails to the `department1.example3.com` domain would be affected but not e-mail to `example3.com`. If a large number of domains are to be specified it is recommended to use a separate `Domains` section as an abbreviated form.

**Example:**

```
<Recipient>
  <Domains>
    example1.com
    *example2.com
    *.example3.com
  </Domains>
  # Further directives
</Recipient>
```

### 4.2.2. Selecting by recipients

The `UserSettings` in `eXpurgate` provide the `Address` and the `Addresses` sections in order to limit settings to individual recipients.

**Example:**

```
<Recipient>
  Address user1@example.com
  <Addresses>
    user2@abteilung1.example.com
    user2@abteilung2.example.com
  </Addresses>
  # Further directives
</Recipient>
```

Here also — as with `Domain` — an abbreviated style is possible through the use of an `Addresses` section.

## 4.3. Features

You can activate and deactivate certain individual eXpurgate functions in the `UserSettings` with `Feature` commands. Features can be activated and deactivated globally or user-specific.

The following features are currently defined.

### 4.3.1. Feature Spam

Activates the e-mail categorisation and also the spam detection.

#### Example:

```
<UserSettings>
  Feature Spam on
  <Recipient>
    Address i-want-spam@example.com
    Address abuse@example.com
    Feature Spam off
  </Recipient>
</UserSettings>
```

This switches on the eXpurgate spam detection globally. Detection is, however, switched off for individual recipients.

### 4.3.2. Feature Virus

Activates the integrated AntiVir virus scanner.

#### Example:

```
<UserSettings>
  Feature Virus on
  <Recipient>
    Address abuse@example.com
    Domain viruslab.example.com
    Feature Virus off
  </Recipient>
</UserSettings>
```

The virus scanner is thus switched on globally. A domain and one single recipient are, however, exempted from the detection and receive e-mails with viruses unfiltered.

### 4.3.3. Feature Outbreak

Activates the Virus Outbreak Detection feature in eXpurgate.

**Example:**

```
<UserSettings>
  Feature Outbreak on
</UserSettings>
```

Virus Outbreak Detection is thus switched on globally.

### 4.3.4. Feature Freezing

Activates Freezing in eXpurgate. See also Section 3.2.7 for further information about this feature.

**Example:**

```
<UserSettings>
  Feature Freezing on
  <Recipient>
    Address systemmonitor@example.com
    Address newsletters@example.com
    Feature Freezing off
  </Recipient>
</UserSettings>
```

This section globally activates Freezing. Two addresses are, however, exempted in order to guarantee e-mail delivery without a time lag for these recipients.

## 4.4. Define e-mail processing

It is possible to define how categorized e-mails should be treated in the MailActions section, in which rules for processing e-mails can be defined depending on their categorisation and the sender.

These processing rules can also be recipient specific and configured by embedding the MailActions section in a respective Recipient section.

E-mail processing is controlled by actions. There are final and non-final actions. Every processing rule can contain one final action and any number of non-final actions.

The following final actions are available:



**Deliver**

The e-mail is delivered to the original recipient. The standard SMTP server is used for transport.

**Syntax:** Deliver

**DeliverTo**

The e-mail is sent to a new recipient. The substitution variables (Substitutions) listed in Section 4.6 are available for this.

**Attention:** The DeliverTo action only changes the envelope recipient. This has no effect on the choice of relay server.

**Syntax:** DeliverTo *address*

**Example:** DeliverTo john@example.com

**Delete**

The e-mail is irreversibly deleted. It is not delivered and no warning or bounce is sent to the e-mail sender.

**Note:** Using Reject is often a better solution as in case of incorrect classification the sender then receives a bounce message with which to inform that the e-mail could not be delivered (False Positive).

**Syntax:** Delete

**Reject**

The e-mail is rejected with a permanent error code in the SMTP protocol. This generally means that the delivering e-mail server sends a bounce message to the sender, which informs that the e-mail could not be delivered.

**Syntax:** Reject

### HandleAs

The e-mail is handled in the same manner as another e-mail type and all actions defined for the other e-mail type are performed.

**Syntax:** `HandleAs type`

**Example:** `HandleAs Spam`

The following non-final actions are also available

### UseRelay

A special SMTP server or relay pool is used for delivering the e-mail. A host:port relay specification forces delivery to the named server. Alternatively, the name of one of the relay pools defined in the configuration can be specified. In this case, delivery is made to one of the associated servers. See Section 3.2.4.

**Syntax:** `UseRelay pool | host:port`

**Example:** `UseRelay prio-relay.example.com:25`

### AddHeader

This command adds a freely definable header to the e-mail. The command expects two parameters: the name of the header and its value (in inverted commas). The substitution variables introduced in Section 4.6 can be used for the value.

**Syntax:** `AddHeader header string`

**Example:** `AddHeader X-Spam-Level "0"`

### RemoveHeader

This command removes a header from the e-mail.

**Syntax:** `RemoveHeader header`

**Example:** `RemoveHeader X-Mailer`

### RewriteSubject

This overwrites the current subject header of an e-mail with another freely definable value. The documented substitution variables can also be used here.

The major advantage of overwriting the subject header is that users normally see the subject header directly in their mail program so that information and warnings can easily be placed there.

**Syntax:** `RewriteSubject string`

**Example:** `RewriteSubject "[Dangerous] %s"`

#### 4.4.1. Category-based rules

Actions are most frequently used subject to categorization by eXpurgate. Special treatment for individual e-mail types can be forced with the MailType section. Categories are selected with the Category command.

##### Example:

```
<UserSettings>
  <MailActions>
    <MailType>
      Category Spam
      Category Dangerous.Virus
      Reject
    </MailType>
    <MailType>
      Category Bulk.Advertisement
      HandleAs Spam
    </MailType>
  </MailActions>
</UserSettings>
```

That *spam* and *dangerous.virus* e-mail types should be rejected is defined here. The same treatment for *bulk.advertisement* is also forced with a HandleAs action. In the above example, global settings are defined for the e-mail types. If a MailActions section is embedded in a Recipient section the treatment for these e-mail types only applies for the respective recipients.

##### Example:

```
<UserSettings>
  <MailActions>
    <MailType>
      Category Spam
      Category Dangerous.Virus
      Reject
    </MailType>
    <MailType>
      Category Bulk.Advertisement
      HandleAs Spam
    </MailType>
  </MailActions>
  <Recipient>
    Domain marketing.example.com
    <MailActions>
      <MailType>
        Category Bulk.Advertisement
        Deliver
      </MailType>
    </MailActions>
  </Recipient>
</UserSettings>
```

The example from above is extended here: spam, viruses and advertising e-mails are rejected globally. Special treatment is defined for the marketing.example.com domain as this supposedly contains advertising e-mails.

### 4.4.2. Sender-based rules

Senders which can then, for example, be used for black- and whitelists are defined in `MailFrom` and `SenderId` sections within the `MailActions` section.

Envelope Mail From-based processing rules can be defined with the `MailFrom` section. As in the `Recipient` section, the `Domain`, `Domains` and `Addresses` commands are available to narrow down the sender.

**Example:**

```
<UserSettings>
  <MailActions>
    <MailFrom>
      Domain *partner.com
      Domain *partner.de
      HandleAs Clean
    </MailFrom>
  </MailActions>
</UserSettings>
```

This defines a sender, which includes the `partner.com` and `partner.de` domains and all their sub-domains. E-mails from these senders are regarded as *clean* (whitelisting).

IP-based processing rules can be defined with the `SenderId` section. One or more `Source` commands precisely specify the host.

**Example:**

```
<UserSettings>
  <MailActions>
    <SenderId>
      Source 10.10.1.100
      Source 10.10.0.0/24
      Reject
    </SenderId>
  </MailActions>
</UserSettings>
```

A host with the IP address `10.10.1.100` is defined here as well as a complete `10.10.0.0` network with a 24-bit network mask. Connection is generally rejected for these sender IP addresses (blacklisting).

IP addresses can also be included in a `Recipient` section. Special treatment for these addresses can be defined for each recipient.

### 4.4.3. Actions for IP addresses, senders and e-mail types

The efficiency of the processing rules results from the possibility of combining the actions with e-mail types, sending IP addresses and senders. These can in turn be applied to each recipient so that very finely granulated settings for e-mail processing can be defined.

The search for suitable actions for an e-mail begins with a search for as precise a match of the recipient as possible in a Recipient section. If no match is found the global settings are used.

A match for the current e-mail and appropriate actions are sought in this order: (1). SenderIp, (2). MailFrom, (3). MailType. The first match causes the respective actions to be performed. No further matches are then sought. The HandleAs action is an exception: it continues the search for a MailType section which matches the e-mail types specified as a parameter. SenderIp and MailFrom sections are then ignored.

## 4.5. Application examples

### 4.5.1. Whitelisting

The following configuration creates a whitelist for a certain recipient domain.

#### Example:

```
<UserSettings>
  Feature Spam On
  Feature Virus On
  <MailActions>
    <MailType>
      Category Spam
      Category Dangerous
      Reject
    </MailType>
    <MailType>
      Category Clean
      Category Bulk
      AddHeader X-Approved "Certified as %t"
      Deliver
    </MailType>
  </MailActions>
  <Recipient>
    Domain marketing.example.com
    <MailActions>
      <SenderIp>
        # Host belongs to a partner company
        Source 10.10.10.1
        HandleAs Clean
      </SenderIp>
      <MailFrom>
        # These senders are always accepted
        Domain *partner.com
        Address friend@reseller.com
        AddHeader X-Whitelisted "Whitelisting for partners"
        HandleAs Clean
      </MailFrom>
    </MailActions>
  </Recipient>
</UserSettings>
```

```

    </MailActions>
  <Recipient>
</UserSettings>

```

The spam and virus checks are switched on globally here. E-mails which have been detected to be *spam* or *virus* are rejected by default, i.e. the e-mail is rejected with a permanent error. E-mails which are recognized as *clean* or *bulk* contain an additional e-mail header which contains the e-mail type. The e-mail is ultimately delivered to the recipient. An exception rule is, however, introduced in the `Recipient` section for the `marketing.example.com` domain. This supplies an IP address, a sender domain and a sender with a `HandleAs Clean`. This means that all e-mails sent by these senders are treated as a *clean* e-mail and the appropriate actions are performed, i.e. the e-mail header `X-Whitelisted` is added and the e-mail is delivered, but the `AddHeader` command from the `MailFrom` section is also performed. The e-mails processed by whitelisting as such.

### 4.5.2. Blacklisting

A blacklist can also be configured via the `HandleAs` command and the use of `SenderId` and `MailFrom` sections.

#### Example:

```

<UserSettings>
  Feature Spam On
  Feature Virus On
  <MailActions>
    <MailFrom>
      # Never allow these senders
      Domain *annoying.com
      Reject
    </MailFrom>
  </MailActions>
</UserSettings>

```

This example realizes a simple blacklist. E-mails from the `annoying.com` domain are rejected.

## 4.6. Substitutions

Numerous variables are available which can replace text with current data from the e-mail processing procedure for the `AddHeader`, `RewriteSubject` and `DeliverTo` actions.

These are:

**%d** The part of the recipient's address after the @ symbol, in other words the domain.

**%s** The original e-mail subject heading.

**%t** The eXpurgate e-mail type following processing by `HandleAs`.

**%T** The original e-mail type before treatment by HandleAs.

**%u** The part of the recipient's address before the @ symbol (the local part).

**%v** The name of a possibly detected virus in the e-mail.

**%x** The eXpurgate ID of the e-mail. This is an ID assigned by eXpurgate which uniquely identifies the e-mail and is important in case of support queries.

**%z** The size of the e-mail after parsing of the MIME structure.

**%%** The percent symbol itself.

#### Example:

```
<UserSettings>
  <MailActions>
    <MailType>
      Category Dangerous.Virus
      RewriteSubject "%v: %s"
      UseRelay "Quarantine"
    </MailType>
  </MailActions>
</UserSettings>
```

The subject header for e-mails which are detected as *dangerous.virus* is modified here. The name of the detected virus is added to the beginning of the original subject heading. Delivery is also via the Quarantine pool.

#### Example:

```
<UserSettings>
  <MailActions>
    <MailType>
      Category Spam
      AddHeader X-Checked "%t / %T"
      Deliver
    </MailType>
    <MailType>
      Category Bulk.Advertisement
      HandleAs Spam
    </MailType>
  </MailActions>
</UserSettings>
```

A special header is added to e-mails which contain the original category as well as the category after treatment by HandleAs. In this example, e-mails which have been classified as *bulk.advertisement* are treated as *spam*. These rules mean that spam e-mails are marked with the header *spam / spam*. For *bulk.advertisement* e-mails, *spam / bulk.advertisement* is added.

## 4.7. Limits

There are no limitations as to the number of `Recipient`, `MailType`, `SenderId` or `MailFrom` sections that can be present in the `UserSettings`. You can define as many recipients as you like, create blacklists or whitelists and cover special cases during e-mail processing.

## 4.8. Default settings

eXpurgate performs a number of actions by default. These do not have to be explicitly listed in the `UserSettings`.

### 4.8.1. Adding a header

The following headers are added to each e-mail that is not deleted or rejected:

**X-purgate-ID** with a unique ID.

**X-purgate-type** with the type of the e-mail that is currently being processed.

**X-purgate-size** with the size of the e-mail.

**X-purgate-Ad** with a short string that points out the use of eXpurgate.

These headers permit a level of support by eleven which can also react to queries about individual e-mails. These changes therefore cannot be overwritten in the `UserSettings`.

### 4.8.2. Features

The anti-spam feature is activated by default. Anti-virus, Virus Outbreak Detection and Freezing are activated depending on the settings in the licence file. If this permits the use of a feature it is switched on automatically by eXpurgate for all recipients and incoming e-mails.

### 4.8.3. Delivery

Every e-mail is delivered by default after the aforementioned headers have been added. The standard SMTP relay is used which is defined in the `SmtRelay` section (3.2.4).



## 5. Testing eXpurgate

eXpurgate offers various options for testing the installation and settings. The eXpurgate binary with appropriate options for testing is called directly for this. After the configuration file has been adapted these settings can be checked with the `--test-config`.

### Example:

```
# expurgate -c expurgate.conf --test-config
```

The availability of the eXpurgate server specified in the configuration file is necessary for eXpurgate to function. This can be checked with the `--test-exdb` option. The defined servers are addressed in turn; the name of the server and the test result are output for each test.

### Example:

```
# expurgate -c expurgate.conf --test-exdb
```

With the `--test-relays` option you can check the availability of the configured SMTP relay servers.

### Example:

```
# expurgate -c expurgate.conf --test-relays
```

## 6. eXpurgate reporting

The eXpurgate reporting function offers the option of a statistical overview of the distribution of individual e-mail categories. For this, you must first log in under <https://my.eleven.de/> with your user name and password and then click in left menu **STATISTICS**

In the first field you can select the time frame and the domains that is to be displayed in the statistics. When selecting **LAST WEEK** or **LAST MONTH**, the time period selected will end on the current day, counting backwards. Therefore, if you choose the option **LAST MONTH** on the 21st of the current month, the statistics displayed will start on the 21st of the previous month. Alternatively You can *mark* a section in the diagram above to zoom in.

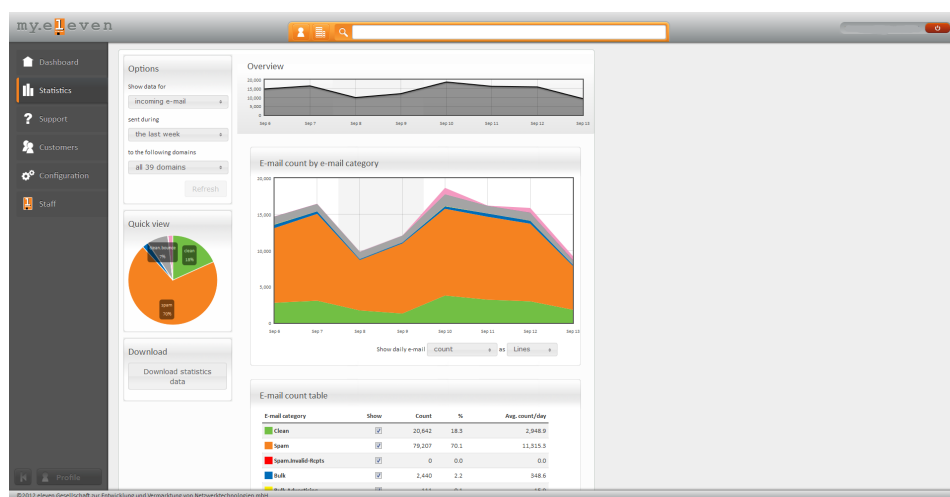


Figure 6.1.: Selecting the time frame for statistics

For the **SPECIFIC TIME FRAME** option you must specify a time frame (from/to). Please pay attention to the correct syntax. Years, months and dates must be separated by a minus sign. The 2nd of December 2008 would have the following format: 2008-12-02.

You receive the data on processed e-mails in three forms: in table form, as a pie chart and as a progression diagram. You can also download the data from the table as an Excel file for use in your own calculations or presentations.

The different display options have in common that they all display in color the absolute number of individual e-mail categories and their percentage share with regard to all e-mails. This gives you a quick overview of how high the share of clean e-mails is in relation to less desirable and completely unwanted e-mails.

# A. Appendix

## A.1. Best Practice Empfehlungen

To get a maximum level of protection for the user eleven advises the "best practice settings". To use the "best practice settings" you only have to adjust the rules for three categories. First the categories *spam*, *dangerous.virus-outbreak* and *dangerous.virus* should be set to *reject*. *df* in the table means default. If you have no AV licence, you don't need a configuration for *dangerous.virus* and *dangerous.virus-outbreak*. In this case choose the reject mode for the categorie *dangerous.attachment*.

| Kategorie                | Default                  | Business (BP) | Business      |
|--------------------------|--------------------------|---------------|---------------|
| Clean                    | deliver                  | deliver       | deliver       |
| Spam                     | tag & deliver            | reject        | tag & deliver |
| Bulk                     | deliver                  | df            | df            |
| Bulk.Advertising         | treat as Spam            | df            | df            |
| Bulk.Porn                | treat as Spam            | df            | df            |
| Clean.Empty              | treat as Spam            | df            | df            |
| Clean.Almost-empty       | treat as Clean           | df            | df            |
| Clean.Empty-body         | treat as Clean           | df            | df            |
| Clean.Bounce             | treat as Clean           | df            | df            |
| Clean.Whitelisted        | treat as Clean           | df            | df            |
| Suspect                  | treat as Clean           | df            | df            |
| Dangerous                | deliver                  | df            | df            |
| Dangerous.Virus          | tag & deliver            | reject        | reject        |
| Dangerous.Attachment     | tag & treat as Dangerous | df            | df            |
| Dangerous.Code           | treat as Dangerous       | df            | df            |
| Dangerous.Iframe         | treat as Dangerous       | df            | df            |
| Dangerous.Virus-Outbreak | tag & treat as Dangerous | reject        | reject        |

Table A.1.: Default settings and eleven recommendations for handling E-Mails

## A.2. Example file

```

<General>
    WorkingDirectory  "/var/spool/expurgate"
    LicenseFile       "/etc/expurgate/client.key"
    # SublicenseFile  "/etc/expurgate/license.subkey"
    # Sublicense      "this-string-is-a-sublicense-key"
    Pidfile           "/var/run/expurgate/expurgate.pid"
    UserId            mail:mail
    Daemonize         yes
    # Changeroot      "/var/spool/expurgate"
</General>

<Logging>
    FileLog NOTICE "/var/log/expurgate/expurgate.log"
    SysLog  WARNING-EMERGENCY MAIL

    <Messages>
        GENERAL-START          "Expurgate v%(version) starting"
        GENERAL-SHUTDOWN      "Shutting down "
        GENERAL-RECONFIGURE    "Received reconfigure request"

        SMTP-CONNECT           "Connect from %(peer)"
        SMTP-DISCONNECT        "Disconnect from %(peer)"

        SMTP-HELO              ""
        SMTP-MAILFROM          ""
        SMTP-RCPTTO            ""
        SMTP-DATA               ""
        SMTP-ENDOFDATA         ""
        SMTP-RESET             ""
        SMTP-QUIT               ""
        SMTP-XCLIENT           ""
        SMTP-XFORWARD          ""
        SMTP-STARTTLS          ""
        SMTP-TLSUPGRADED       ""
        SMTP-TLSUPGRADEFAILED   ""
    </Messages>
</Logging>

<SmtpServer>
    ListenAddress      0.0.0.0:25
    HelloHostname      example.com
    MaxConnections     5000
    ConnectionTimeout  3600
    DataTimeout        60
    MaxInvalidCommands 5
    MaxRecipients      1024
    MaxMailSize        250000000
    ValidateAddresses  No
    AllowRelayAddresses No

    Extension 8BITMIME On
    # Extension VRFY      On
    # Extension XCLIENT   On
    # Extension XFORWARD  On

    <LocalDomains>
        example.com
        example.de
    </LocalDomains>

    <Permissions>
        <Connect>
            Allow 0.0.0.0/0

```

```
</Connect>

<Relay>
    Allow 127.0.0.1/32
    Deny 0.0.0.0/0
</Relay>
</Permissions>
</SmtServer>

<SmtRelay>
    Server relay.example.com:25
    # Server relay-fallback.example.com:25 prio 1

    Helo          PASSTHROUGH
    MaxPoolSize 50
    MaxMailsPerConnection 500

    <Pool>
        Name "Quarantine"

        Server      quarantine.example.com
        Helo         example.com
        MaxPoolSize 50
        MaxMailsPerConnection 500
    </Pool>
</SmtRelay>

<Tls>
    Certificate "/etc/expurgate/certificate.pem"
    PrivateKey  "/etc/expurgate/private-key.pem"

    TrustedCertificate "/etc/expurgate/ca.pem"
    # TrustedCertificateDirectory "/etc/ssl/ca/"

    <Policy>
        Domain highsec.example.com
        Domain highsec.example.de

        <Validation>
            Default
            Encryption Enforced
        </Validation>

        <Validation>
            Sender trusted.com
            Encryption Verified "Trusted Inc."
        </Validation>
    </Policy>
</Tls>

<SpamEngine>
    Server exa.expurgate.net:55555 prio 0
    Server exb.expurgate.net:55555 prio 0
    Server exa.expurgate.de:55555 prio 1
    Server exb.expurgate.de:55555 prio 1

    Threads 128
    TempRejectOnError On

    <Antivir>
        Enable      yes
        Port        55556
        MaxPoolSize 20
    </Antivir>
</SpamEngine>
```

```
<Freezing>
  Enable          yes
  FridgeDirectory "/var/spool/expurgate/fridge"
  CheckInterval   300
  Daytime          7:00 2:30
  MaxFreezingTime 1200 7200
  MaxThawTasks     5
  MaxFrozenMails  1000
</Freezing>

<UserSettings>
  Feature Spam      on
  Feature Virus     on
  Feature Outbreak  on
  Feature Freezing  on

  <MailActions>
    <MailType>
      Category Clean.Empty
      Category Bulk.Porn
      Category Bulk.Adv
      HandleAs Spam
    </MailType>

    <MailType>
      Category Spam
      Reject
    </MailType>

    <MailType>
      Category Dangerous.Attachment
      RewriteSubject "[%t] %s"
    </MailType>

    <MailType>
      Category Dangerous.Virus
      Category Dangerous.Outbreak
      Quarantine
    </MailType>
  </MailActions>

  <Recipient>
    Domain vip.example.com
    Address cio@example.com

    Feature Freezing off
  </Recipient>
</UserSettings>
```

### A.3. eXpurgate categories

eXpurgate assigns all checked e-mails to one of the following categories:

**clean** E-mails which demonstrate no suspicious characteristics.

**bulk** E-mails sent in mass such as newsletters.

**spam** Uniquely identified spam and phishing e-mails.

**dangerous** E-mails which potentially contain dangerous executable code or corresponding attachments (file attachments).

**dangerous.attachment** E-mails which contain an executable attachment (file attachment). There are: ade, adp, app, asp, bas, bat, bhx, cab, ceo, chm, cmd, com, cpl, crt, csr, der, exe, fpx, hlp, hta, inf, ins, isp, its, js, jse, lnk, mad, maf, mag, mam, mar, mas, mat, mde, mim, msc, msi, msp, mst,ole, pcd, pif, reg, scr, sct, shb, shs, vb, vbe, vbmacros, vbs, vsw, wmd, wmz, ws, wsc, wsf, wsh, xxe

**dangerous.code** E-mails with potentially dangerous content such as links to local files.

**dangerous.iframe** E-mails which use the iframe feature. (An iframe embedded in an e-mail could for example be used to execute a script which has access to the local file system and can read or delete files.)

**dangerous.virus** E-mails which contain a virus. (This category is only available when the optional virus checker is activated.)

**dangerous.virus-outbreak** E-mails which very probably contain a virus but which due to its novelty can not yet be recognized as such by virus scanners. (This category is only available when the optional virus check is activated.)

**bulk.advertising** Advertising e-mails which are not typical spam but are still not wanted.

**bulk.porn** E-mails with pornographic content which are not *spam* (e.g. pornographic newsletter).

**clean.empty** E-mails which have neither a subject header nor a body and are thus completely empty.

**clean.empty-body** E-mails which have a subject header but no body.

**clean.almost-empty** E-mails whose body is almost empty.

**clean.bounce** E-mails which are returned to the sender due to a delivery error.

## A.4. Variables

**action** Final action for a single recipient.

**all-rcpttos** Comma-separated list of all e-mail recipient addresses.

**authcid** authentication identity (AUTH command).

**cipher** Employed cipher algorithm.

**cipher-bits** Key length of employed cipher algorithm.

**commands** List of all available SMTP commands.

**connection-id** Unique identification string of an SMTP connection.

**domain** SMTP domain for banner and HELO/EHLO responses. Configurable via the `HeloHostname` setting in the `SmtptServer` section.

**error** Error message.

**expurgate-id** Combination of id and reason.

**extensions** List of all supported SMTP extensions.

**helo** Parameters of the last HELO or EHLO command.

**issuer** Common name of the certificate issuer of the peer MTA.

**mailfrom** E-mail envelope sender address taken from SMTP MAIL FROM command.

**message** Relay server SMTP response.

**message-id** Unique identification string for an e-mail. Combination of `connection-id` and `message-number`.

**message-number** Running number of e-mail transactions inside an SMTP connection. The number is incremented by HELO, EHLO, and RSET commands, as well as completed message deliveries.

**original-rcptto** Original recipient before application of DeliverTo actions.

**peer** The delivering e-mail server's IP address and port.

**peer-ip** The delivering e-mail server's IP address.

**peer-port** The delivering e-mail server's port

**pool** Name of the relay pool or server used for despatch.

**protocol** Name of the used protocol.



**rcptto** E-mail recipient address or multiple recipients if several recipients exist.

**received** Timestamp of receipt of an e-mail.

**relay** The IP address and port of the relay server.

**relay-ip** The IP address of the relay server.

**relay-port** The port of the relay server.

**score** Sum of Score values of all DNS blacklists that list an IP address.

**subject** Common name of certificate subject of the peer MTA.

**tls-version** SSL/TLS protocol version.

**type** Classification of an e-mail.

**version** eXpurgate version in X.Y.Z format.

**zones** List of all matching DNS blacklist zones for an IP address.

## A.5. Log messages

| Keyword                             | Meaning   |
|-------------------------------------|---|
| <b>general-start</b>                | Message at service start-up<br><b>Variables:</b> version  |
| <b>general-shutdown</b>             | Message on service terminaton<br><b>Variables:</b> version  |
| <b>general-reconfigure</b>          | Message on receipt of a reconfigure signal<br><b>Variables:</b> version   |
| <b>smtp-connect</b>                 | Message for new SMTP connection<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port   |
| <b>smtp-disconnect</b>              | Message for end of an SMTP connection<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port   |
| <b>smtp-helo</b>                    | Message for HELO/EHLO<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo   |
| <b>smtp-mailfrom</b>                | Message for MAIL FROM<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom   |
| <b>smtp-rcptto</b>                  | Message for RCPT TO<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom, rcptto   |
| <b>smtp-data</b>                    | Message for DATA<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom  |
| <b>smtp-endofdata</b>               | Message at conclusion of delivery<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom   |
| <b>smtp-reset</b>                   | Message for RSET<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id  |
| <b>smtp-quit</b>                    | Message for QUIT<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id  |
| <b>smtp-xclient</b>                 | Message for XCLIENT<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id   |
| <b>smtp-xforward</b>                | Message for XFORWARD<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id  |
| <b>smtp-auth</b>                    | Message for AUTH<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, authcid   |
| <b>smtp-starttls</b>                | Message for STARTTLS<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id  |
| <b>smtp-tlsupgraded</b>             | Message following successful TLS upgrade<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, tls-version, cipher, cipher-bits, subject, issuer |
| <b>smtp-tlsupgradedfailed</b>       | Message on unsuccessful TLS upgrade<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, error  |
| <b>smtp-syntax-error</b>            | Message on syntactically invalid commands within an ongoing SMTP transaction<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message, error                            |
| <b>smtp-syntax-error-connection</b> | Message on syntactically invalid commands outside of an ongoing SMTP transaction<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message, error                        |

|  |   |
|--|---|
| <b>check-mailfrom-permanent-reject</b> | Message for permanent rejection of a sender by the relaying MTA<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message                                    |
| <b>check-mailfrom-temporary-reject</b> | Message for temporary rejection of a sender by the relaying MTA<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message                                    |
| <b>check-rcptto-permanent-reject</b>   | Message for permanent rejection of a recipient by the relaying MTA<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message                                 |
| <b>check-rcptto-temporary-reject</b>   | Message for temporary rejection of a recipient by the relaying MTA<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message                                 |
| <b>relay-address-denied</b>            | Message for a not permitted recipient with a relay mail address<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos   |
| <b>acl-connect-denied</b>              | Message for not permitted inbound connection establishment<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos  |
| <b>acl-relay-denied</b>                | Message for not permitted delivery of an e-mail server to non-local domains<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos                                 |
| <b>acl-xclient-denied</b>              | Message for not permitted execution of a XCLIENT command<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos  |
| <b>acl-xforward-denied</b>             | Message for not permitted execution of a XFORWARD command<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos   |
| <b>tls-not-encrypted</b>               | Message for missing encryption<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos  |
| <b>tls-verification-failed</b>         | Message for failed certificate verification<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message  |
| <b>auth-failed</b>                     | Message for failed authentication<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message  |
| <b>dnsbl-reject</b>                    | Message for rejection based of DNS blacklist results<br><b>Variables:</b> version, connection-id, message-number, message-id, peer, peer-ip, peer-port, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, score, zones  |
| <b>arbiter-scan</b>                    | Message on first scan of an e-mail<br><b>Variables:</b> connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type   |
| <b>arbiter-rescan</b>                  | Message on repeated scanning of an e-mail<br><b>Variables:</b> connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type  |
| <b>arbiter-action</b>                  | Message on definition of MailAction per recipient.<br><b>Variables:</b> connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type, action                                       |
| <b>relay-delivery</b>                  | Message on successful despatch of an e-mail.<br><b>Variables:</b> connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type, pool, relay, relay-ip, relay-port, original-rcptto |

|                              |   |
|------------------------------|---|
| <b>relay-delivery-failed</b> | Message upon rejection of an e-mail by the relay server.<br><b>Variables:</b> connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type, pool, relay, relay-ip, relay-port, original-rcptto |
| <b>batv-denied</b>           | Message for a not permitted e-mail because of an invalid BATV signature.<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos  |
| <b>batv-delayed-denied</b>   | Message at delayed rejection by an invalid BATV signature<br><b>Variables:</b> version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos   |

## A.6. SMTP replies

| Keyword                     | Meaning   |
|-----------------------------|---|
| <b>banner</b>               | SMTP banner at connection<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port              |
| <b>helo</b>                 | Response to HELO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, helo                 |
| <b>ehlo</b>                 | Response to EHLO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, helo, extensions     |
| <b>quit</b>                 | Response to QUIT<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                       |
| <b>rset</b>                 | Response to RSET<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                       |
| <b>mailfrom</b>             | Response to MAIL FROM<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, mailfrom        |
| <b>rcptto</b>               | Response to RCPT TO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, rcptto            |
| <b>xclient</b>              | Response to XCLIENT<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                    |
| <b>xforward</b>             | Response to XFORWARD<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                   |
| <b>starttls</b>             | Response to STARTTLS<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                   |
| <b>vrfy</b>                 | Response to VRFY<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                       |
| <b>help</b>                 | Response to HELP<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, commands             |
| <b>auth</b>                 | Response to AUTH<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, authcid              |
| <b>data</b>                 | Response to DATA<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                       |
| <b>not-available</b>        | Error message at Shutdown<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port              |
| <b>session-timeout</b>      | Error message at Session Timeout<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port       |
| <b>command-timeout</b>      | Error message at Command Timeout<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port       |
| <b>local-error</b>          | Error message to local errors<br><b>Variables:</b> domain, version, product-name, peer, peer-ip, peer-port          |
| <b>rcptto-too-many</b>      | Error message for too many RCPT TO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port     |
| <b>invalid-command</b>      | Error message for unknown commands<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port     |
| <b>syntax-error</b>         | Error message for syntax error<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port         |
| <b>not-implemented</b>      | Error message for unavailable commands<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port |
| <b>tls-failed</b>           | Error message for failed SSL handshake<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port |
| <b>helo-first</b>           | Error message at not used HELO/EHLO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port    |
| <b>mailfrom-nested-mail</b> | Error message for multiple MAIL FROMs<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |

|                                       |   |
|---------------------------------------|---|
| <b>rcptto-mailfrom-needed</b>         | Error message for RCPT TO without MAIL FROM<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>data-rcptto-needed</b>             | Error message for DATA without RCPT TO<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>data-size-exceeded</b>             | Error message for too large e-mails<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>xclient-in-progress</b>            | Error message for XCLIENT after MAIL FROM<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>auth-in-progress</b>               | Error message for AUTH after MAIL FROM<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>auth-already</b>                   | Error message for multiple AUTHs<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>auth-unsupported</b>               | Error message for invalid authentication mechanism<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>auth-cancelled</b>                 | Error message if authentication is cancelled by the client<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port                                     |
| <b>auth-failed</b>                    | Error message for invalid authentication credentials<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>auth-required</b>                  | Error message if authentication is obligatory<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>acl-connect-denied</b>             | Error message at rejection by connect ACL<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>acl-relay-denied</b>               | Error message at rejection by relay ACL<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>acl-xclient-denied</b>             | Error message at rejection by XClient ACL<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port  |
| <b>acl-xforward-denied</b>            | Error message at rejection by XForward ACL<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>tls-not-encrypted</b>              | Error message at rejection by TLS policy<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>tls-verification-failed</b>        | Error message at rejection by TLS policy<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port   |
| <b>check-mailfrom-temporary-error</b> | Error message at temporary MAIL FROM rejection by relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, message                        |
| <b>check-mailfrom-permanent-error</b> | Error message at permanent MAIL FROM rejection by relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, message                        |
| <b>check-rcptto-temporary-error</b>   | Error message at temporary RCPT TO rejection by relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, message                          |
| <b>check-rcptto-permanent-error</b>   | Error message at permanent RCPT TO rejection by relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, message                          |
| <b>endofdata-accept</b>               | Response on acceptance of an e-mail<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type                               |
| <b>endofdata-reject</b>               | Response on rejection of an e-mail<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type                                |
| <b>endofdata-temporary-error</b>      | Error message for temporary delivery problems on the relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type |
| <b>endofdata-permanent-error</b>      | Error message for permanent delivery problems on the relay server<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type |
| <b>batv-denied</b>                    | Error message at rejection by an invalid BATV signature<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, rcptto                                |
| <b>batv-delayed-deny</b>              | Error message at delayed rejection by an invalid BATV signature<br><b>Variables:</b> domain, product-name, version, peer, peer-ip, peer-port, rcptto                        |

## A.7. eXpurgate server IP ranges

The following networks are currently used by eleven GmbH for running the eXpurgate service and are documented as follows in the RIPE database:

```
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
```

## A.8. Licenses

eXpurgate uses the following licences:

**OpenSSL** Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

**PCRE** Copyright (c) 1997-2008 University of Cambridge. All rights reserved.

**c-ares** Copyright (c) 1998,2000 by the Massachusetts Institute of Technology.  
Copyright (c) 2004-2008 by Daniel Stenberg et al  
Copyright (c) 2005 by Dominick Meglio

**libjpeg** This software is based in part on the work of the Independent JPEG Group.

**libpng** Copyright (c) 2004, 2006-2008 Glenn Randers-Pehrson  
Copyright (c) 2000-2002 Glenn Randers-Pehrson  
Copyright (c) 1998, 1999 Glenn Randers-Pehrson  
Copyright (c) 1996, 1997 Andreas Dilger  
Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

**zlib** Copyright (C) 1995-2004 Jean-Loup Gailly and Mark Adler

# List of Figures

|  |    |
|--|----|
| 1.1. eXpurgate as in-house installation. E-mails are processed in the company network. Only the check sums are compared with the eXpurgate database. . . . .   | 6  |
| 1.2. All e-mails are allocated check sums which are collected in the eXpurgate database. Identification as spam takes place when an identical or similar check sum occurs a large number of times. . . . . | 8  |
| 2.1. Installation wizard start page . . . . .  | 14 |
| 2.2. Licence agreement . . . . .   | 15 |
| 2.3. Selecting the target directory . . . . .  | 16 |
| 2.4. Inserting eXpurgate into the Start menu . . . . .   | 17 |
| 2.5. Connection options . . . . .  | 18 |
| 2.6. Further treatment for spam e-mails . . . . .  | 19 |
| 2.7. Changing the mail subject header . . . . .  | 20 |
| 2.8. Selecting SSL/TLS options . . . . .   | 21 |
| 2.9. Checking the data entered . . . . .   | 22 |
| 2.10. Final installation screen . . . . .  | 23 |
| 2.11. eXpurgate entered as a service in the Microsoft Management Console . . . . .   | 24 |
| 2.12. Exchange system manager . . . . .  | 26 |
| 2.13. Virtual default server . . . . .   | 27 |
| 2.14. Advanced . . . . .   | 28 |
| 2.15. Identification . . . . .   | 29 |
| 6.1. Selecting the time frame for statistics . . . . .   | 90 |