

eleven Dokumentation

■ eXpurgate.Inhouse (SMTP)

eleven Support

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

eleven Vertrieb

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

Postanschrift

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

© eleven Gesellschaft zur Entwicklung und Vermarktung von
Netzwerktechnologien mbH.

Dieses Dokument enthält vertrauliche Informationen.
Alle Rechte vorbehalten. Wiedergabe, Vervielfältigung und
Weitergabe – auch auszugsweise – bedarf der vorherigen
schriftlichen Genehmigung von eleven.

Inhaltsverzeichnis

1. Einleitung	5
1.1. Die Funktionsweise von eleven Inhouse E-Mail Security	6
1.2. Das eXpurgate Prinzip	7
2. Installation von eXpurgate	9
2.1. Installation von eXpurgate SMTP auf einem Unix-System	9
2.1.1. Installation und Deinstallation der Pakete	9
2.1.2. Aktivieren und Deaktivieren des Dienstes	11
2.1.3. Starten und Beenden des Dienstes	12
2.1.4. Verbindungstest	12
2.1.5. Weitere Anmerkungen	13
2.2. Installation von eXpurgate auf einem Windows-System	14
2.2.1. Windows-Dienst-Kommandos	24
2.2.2. Ändern des TCP-Ports bei Microsoft Exchange 5.5	24
2.2.3. Ändern des TCP-Ports bei Microsoft Exchange 2000 bzw. 2003	25
2.2.4. Testen, ob Exchange auf einem Port antwortet	30
3. Die Konfiguration von eXpurgate	31
3.1. Die Kommandozeilen-Optionen	32
3.1.1. Optionen zur Ausgabe von Informationen	32
3.1.2. Optionen für den Betrieb unter Unix	32
3.1.3. Optionen zur Protokollierung von Log-Meldungen	33
3.1.4. Optionen zum Testen von eXpurgate	34
3.1.5. Optionen zur allgemeinen Funktionsweise	35
3.1.6. Optionen für den SMTP-Server	35
3.1.7. Optionen für nachgelagerte SMTP-Relays	35
3.1.8. Optionen für die Spam-Engine	36
3.1.9. Optionen zur Konfiguration des Virens scanners	36
3.1.10. Optionen für das Simple Network Management Protocol	36
3.1.11. Optionen für das Freezing	37
3.2. Die Konfigurationsdatei	37
3.2.1. Allgemeine Einstellungen	39
3.2.2. Logging	41
3.2.3. SMTP-Server	44
3.2.3.1. Lokale Domains	48
3.2.3.2. Zugriffskontrolle	48
3.2.3.3. Abfrage von DNS-Blacklists	49
3.2.3.4. Bounce Address Tag Validation (BATV)	50
3.2.3.5. Sender Policy Framework (SPF)	51
3.2.3.6. Authentifizierung via SMTP AUTH	52
3.2.3.7. SMTP-Protokoll-Meldungen	53
3.2.4. SMTP-Relay	53
3.2.5. TLS	56

3.2.6.	Spam-Erkennung	59
3.2.6.1.	Untersektion Antivir	61
3.2.6.2.	Untersektion NoFilter	62
3.2.7.	Freezing	64
3.2.8.	Simple Network Management Protocol (SNMP)	66
3.2.9.	Lightweight Directory Access Protocol (LDAP)	67
3.2.9.1.	LDAP-Server-Abfragen	69
3.2.10.	eXelerate	70
3.2.10.1.	Local Domains Query	71
3.2.10.2.	Recipient Validation Query	72
3.2.10.3.	Blacklist Query	73
3.2.10.4.	BATV Policy Query	73
3.2.10.5.	TLS Policy Query	74
3.2.10.6.	TLS Store Query	75
3.2.10.7.	User Feature Query	76
3.2.10.8.	Mail Action Query	77
4.	Finetuning der E-Mail-Behandlung	79
4.1.	Verarbeitungsregeln	79
4.2.	Empfänger definieren	79
4.2.1.	Nach Domains selektieren	80
4.2.2.	Nach Empfängern selektieren	80
4.3.	Features	81
4.3.1.	Feature Spam	81
4.3.2.	Feature Virus	81
4.3.3.	Feature Outbreak	82
4.3.4.	Feature Freezing	82
4.4.	E-Mail-Verarbeitung festlegen	83
4.4.1.	Kategoriebasierte Regeln	85
4.4.2.	Absenderbasierte Regeln	86
4.4.3.	Aktionen für IP-Adressen, Absender und E-Mail-Typen	87
4.5.	Anwendungsbeispiele	87
4.5.1.	Whitelisting	87
4.5.2.	Blacklisting	88
4.6.	Substitutionen	89
4.7.	Limits	90
4.8.	Standardeinstellungen	90
4.8.1.	Header hinzufügen	90
4.8.2.	Features	91
4.8.3.	Zustellung	91
5.	Testen von eXpurgate	92
6.	eXpurgate Reporting	93
A.	Anhang	95
A.1.	Best-Practice-Empfehlungen	95
A.2.	Beispieldatei	96
A.3.	eXpurgate Kategorien	99
A.4.	Variablen	100
A.5.	Log-Meldungen	102
A.6.	SMTP-Antworten	105
A.7.	IP-Bereiche der eXpurgate Server	108

A.8. Lizenzen	108
-------------------------	-----

Letzte Bearbeitung: 28. September 2012

1. Einleitung

Die vorliegende Dokumentation beschreibt die Installation, Konfiguration und den Betrieb von eXpurgate SMTP Version 4. eXpurgate kategorisiert eingehende E-Mails und reicht sie an einen nachgelagerten E-Mail-Server weiter. eXpurgate ist unbegrenzt skalierbar und ist somit in der Lage auch große E-Mail-Volumen sicher zu behandeln. In drei weiteren Varianten kann eXpurgate mit der Open-Source-Lösung SpamAssassin (Spamd-Protokoll) zusammenarbeiten, mit einer SendMail-Installation (Milter-Protokoll) oder als eigenständiger, text-basierter Daemon.

Um den vollen Funktionsumfang von eXpurgate nutzen zu können, empfiehlt eleven die Installation von eXpurgate SMTP. Die anderen oben genannten Varianten besitzen einen eingeschränkten Funktionsumfang. So kann die Freezing-Funktion nicht genutzt werden und es können keine Statistikdaten via SNMP erhoben und verarbeitet werden. Voraussetzung zum Betrieb von eXpurgate ist eine bestehende, permanente Internetverbindung. Diese dient dem Austausch der Fingerprints mit der eXpurgate Datenbank (eXdb).

Die Prüfung der E-Mails erfolgt ohne Analyse des Inhalts, so dass die Vertraulichkeit der E-Mail-Kommunikation gewahrt bleibt. Gleichzeitig sichert die Verwendung der Fingerprints höchste Geschwindigkeit bei der E-Mail-Verarbeitung, bei unerreicht niedriger False-Positive-Rate. Zusätzliche Feature wie beispielsweise: TLS-Verschlüsselung und Zertifikatsverwaltung sichern die Kommunikation in sensiblen Geschäftsbereichen. eXpurgate benötigt keinerlei Trainingsphasen und ist nach Installation und Konfiguration sofort einsatzbereit. Während des laufenden Betriebs sind, abgesehen von Updates, keine weiteren Wartungsarbeiten notwendig.

Neu in eXpurgate 4

Neben dem klassischen Fingerprint führt eleven mit eXpurgate 4 den Strukturfingerprint ein. Er ermöglicht eine Merkmalsabstraktion, so dass strukturgleiche oder strukturähnliche E-Mails zuverlässiger als bisher erkannt und zusammenfasst werden können. Verbesserte Hashbuster-Erkennung: Hashbuster sind Inhalts-Blöcke, die automatisch in Spam-E-Mails eingefügt werden, um die Ähnlichkeitsanalyse von eXpurgate zu erschweren. eXpurgate 4 verbessert die Spam-Erkennung solcher E-Mails, indem zur Berechnung der Prüfsumme nur noch der Text der "1. Seite" herangezogen und typische Hashbusterblöcke erkannt werden. Auch die Erstellung der klassischen Prüfsumme wurde gegenüber der Vorgängerversion optimiert. So werden Inhalte, die die Prüfsumme verschlechtern, wie beispielsweise rotierende Links, entfernt. Auch der HTML-Extractor wurde überarbeitet. Die Spam-Erkennungsleistung konnte mit eXpurgate 4 nochmals erhöht werden und liegt nun bei 99,8 Prozent oder mehr.

eXpurgate 4 ist für die folgenden Linux-Distributionen und Windows-Versionen verfügbar, sowie für FreeBSD und 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. Die Funktionsweise von eleven Inhouse E-Mail Security

eXpurgate arbeitet entweder als SMTP-Proxy (Relay), als SpamAssassin-Server (Spamd) oder als Militer-Plug-In für Sendmail. Jede dieser Varianten hat individuelle Vor- und Nachteile. Aufgrund von Einschränkungen der Militer- und SpamAssassin-Schnittstellen bietet der Einsatz von eXpurgate als SMTP-Proxy die größte Flexibilität. Der Einsatz als Militer-Plug-In oder SpamAssassin-Server kann hingegen Vorteile für die Integration in bestehende Infrastrukturen bieten.

eXpurgates Funktion besteht lediglich darin, E-Mails zu kategorisieren. Daher ist für die Verwaltung von Benutzern bzw. deren E-Mail-Konten immer ein weiterer E-Mail-Server erforderlich. Durch eXpurgates geringen Ressourcenbedarf ist für dessen Betrieb in der Regel jedoch keine separate Hardware erforderlich. Meist kann eXpurgate neben der vorhandenen E-Mail-Server-Software auf demselben Rechner betrieben werden.



Abbildung 1.1.: eXpurgate als Inhouse-Installation. Die Verarbeitung der E-Mails erfolgt im Unternehmensnetzwerk. Es werden nur Kontrollsummen mit der eXpurgate Datenbank ausgetauscht.

Alle Installationsarten basieren auf dem Bulkcheck als Grundprinzip von eXpurgate. Jede eingehende E-Mail wird von eXpurgate einer Analyse unterzogen, bei der eine kurze Kontrollsumme erstellt und verschlüsselt an die zentralen eXpurgate Server übertragen wird. Auf den eXpurgate Servern erfolgt dann der Vergleich mit den Kontrollsummen anderer E-Mails. Das Ergebnis wird an die anfragende eXpurgate Installation zurückgegeben.

Die eXpurgate Server sind redundant ausgelegt und auf mehrere Standorte verteilt, um eine höchstmögliche Verfügbarkeit zu gewährleisten. Für die Übermittlung der Kontrollsumme ist es erforderlich, dass eXpurgate.Inhouse eine Verbindung zu den eXpurgate Servern in den Netzen 194.145.224.0/24 und 195.190.135.0/24

auf Port 55555 aufbauen und von dort kommende Antworten annehmen kann. Sie müssen ggf. Ihre Firewall-Konfiguration entsprechend anpassen. Alternativ können Sie die Verbindungen auch mit Hilfe des SOCKS-Protokolls nach außen leiten. Die eXpurgate Server bauen selbst aktiv keine Verbindungen auf, sondern antworten lediglich auf Anfragen der eXpurgate Client-Installationen.

eXpurgate als SMTP-Proxy

Als SMTP-Proxy fungiert eXpurgate wie ein zusätzlicher, vorgeschalteter E-Mail-Server: eXpurgate nimmt eingehende E-Mails via SMTP (Simple Mail Transfer Protocol) an, um sie kategorisiert via SMTP an den eigentlichen E-Mail-Server weiterzureichen. Die Weiterleitung erfolgt dabei an in eXpurgate konfigurierte E-Mail-Server, wobei MX-Einträge im DNS unberücksichtigt bleiben.

Der SMTP-Proxy-Modus ist die flexibelste Einsatzmöglichkeit eXpurgates. Nur in diesem Modus steht der gesamte Funktionsumfang, wie der Reject-Modus, Empfänger-spezifische Verarbeitungsregeln oder die Integration der E-Mail-Firewall enSurance, zur Verfügung.

eXpurgate als SpamAssassin-Server (Spamd)

Als SpamAssassin-Server nimmt eXpurgate nicht selbständig von außen eingehende E-Mails an. Stattdessen nimmt es auf einem definierten Port Anfragen bzw. E-Mails von einem SpamAssassin-Client entgegen und beantwortet diese mit Hilfe des SpamAssassin-Protokolls. Dabei wird ein Header zurückgegeben, der die Kategorie der E-Mail enthält.

Da eXpurgate in diesem Betriebsmodus nicht selbständig E-Mails über SMTP annimmt, ist der gebotene Leistungsumfang stark vom eingesetzten Protokoll abhängig. eXpurgate kann lediglich die Kategorisierung einer E-Mail über die SpamAssassin-Schnittstellen bzw. einen E-Mail-Header bereitstellen. Alle Behandlungsregeln müssen in der Konfiguration des E-Mail-Servers definiert werden. Weitere Informationen finden Sie in der Dokumentation zu eXpurgate im Einsatz als SpamAssassin-Daemon.

eXpurgate als Sendmail Militer

Als Militer (Mail-Filtering-API) für Sendmail arbeitet eXpurgate ähnlich dem SpamAssassin-Modus. Als Schnittstelle zwischen E-Mail-Server und eXpurgate wird in diesem Fall das von Sendmail spezifizierte Militer-Protokoll verwendet. Das verwendete Militer-Protokoll steht nur unter Sendmail (ab Version 8.12) zur Verfügung. Da eXpurgate auch in diesem Modus nicht selbst E-Mails annimmt, gelten in etwa die gleichen Einschränkungen wie im SpamAssassin-Modus. Weitere Informationen finden Sie in der Dokumentation zu eXpurgate im Einsatz als Militer-Plug-In.

1.2. Das eXpurgate Prinzip

Die von eleven entwickelte eXpurgate Technologie zur Spam-Erkennung und E-Mail-Kategorisierung überprüft E-Mails auf das entscheidende Charakteristikum jeder Spam-E-Mail: Teil einer Massensendung zu sein. eleven hat dafür einen Fingerprint-Algorithmus entwickelt, der es dem System erlaubt, eine große Zahl E-Mails auf Gleichheit bzw. ausreichend große Ähnlichkeit zu überprüfen. Dies geschieht durch Reduzierung jeder E-Mail auf einen nur wenige Bytes großen Fingerprint(Prüfsumme), der keinerlei Rückschlüsse auf den Inhalt der E-Mail zulässt. Dieser wird dann in der zentralen eXpurgate Datenbank (eXdb) mit denen bereits geprüfter

E-Mails verglichen. Je häufiger eine E-Mail mit passendem Fingerprint empfangen wurde, desto höher ist die Wahrscheinlichkeit, dass es sich bei der gerade in der Prüfung befindlichen E-Mail um Spam handelt.

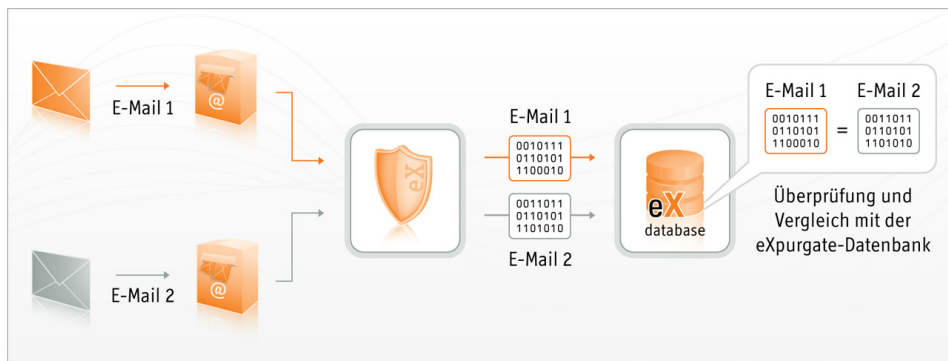


Abbildung 1.2.: Allen E-Mails werden Fingerprints zugeordnet, die in der eXpurgate Datenbank gesammelt werden. Die Identifizierung als *spam* erfolgt, wenn eine gleiche oder ähnliche Kontrollsumme massenhaft auftritt und über zusätzliche Prüfmethoden ausgeschlossen werden kann, dass es sich um eine legitime Massen-E-Mail (z. B. Newsletter) handelt.

eXpurgate kombiniert dieses Testverfahren mit weiteren Prüfmethoden und ist somit in der Lage, jede E-Mail eindeutig einer Kategorie zuzuordnen (z.B. *clean*, *spam*, *bulk*, *dangerous.virus*). Auf diese Weise wird beispielsweise Spam von legitimen Massen-E-Mails (z.B. Newsletter) unterschieden. Darüber hinaus erkennt eXpurgate gefährliche E-Mail-Inhalte und -Anhänge (Attachments) wie Viren und Würmer, bevor diese Systemveränderungen verursachen können.

Durch die von eleven entwickelte selbstlernende eXpurgate-Technologie verzögert sich die E-Mail-Zustellung in der Regel nicht, während die Vertraulichkeit durch Verschlüsselung jederzeit gewahrt wird. Zudem reduziert die Technologie im Gegensatz zu herkömmlichen Spam-Filtern das Auftreten eines False Positives (einer fälschlich als Spam erkannten E-Mail) in der individuellen E-Mail-Kommunikation auf nahe null.

Den E-Mails werden ihrer Kategorie entsprechende Header hinzugefügt, die deren automatische Verarbeitung ermöglichen. Diese Header sind:

- X-purgate-ID** mit einer eindeutigen ID
- X-purgate-type** mit der E-Mail-Kategorie
- X-purgate-size** mit der Größe der E-Mail
- X-purgate-Ad** mit einem kurzen Text, der die Benutzung von eXpurgate anzeigt

Hinweise zur Konfiguration Ihres E-Mail-Programms finden Sie auf unseren Support-Seiten im Internet unter <http://www.eleven.de/support/>

2. Installation von eXpurgate

Im folgenden Abschnitt möchten wir Ihnen die Installation von eXpurgate.Inhouse auf einem Unix- bzw. Windows-System erläutern. Beide Teile sind jeweils auf das Betriebssystem zugeschnitten, so dass für Sie lediglich der Abschnitt relevant ist, der sich mit Ihrem Betriebssystem befasst. In beiden Fällen sollten Sie jedoch den darauf folgenden Abschnitt über die Konfiguration von eXpurgate beachten. Da diese weitgehend unabhängig vom zugrundeliegenden Betriebssystem ist, behandeln wir sie in einem eigenen Kapitel.

Bitte beachten Sie, dass Sie für den Betrieb von eXpurgate eine Lizenzdatei benötigen, die Sie direkt von eleven oder einem Partner erhalten. Hierbei handelt es sich um eine binäre Datei, die im folgenden Text üblicherweise als *client.key* bezeichnet wird.

2.1. Installation von eXpurgate SMTP auf einem Unix-System

2.1.1. Installation und Deinstallation der Pakete

Um eXpurgate SMTP aus einem Debian-Paket zu installieren, benutzen Sie folgendes Kommando:

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

Anmerkung: Bei einigen Debian-Versionen kann folgende Fehlermeldung auftreten:

```
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
```

Sie können die Meldung ignorieren.

Die Deinstallation erfolgt mit dem Kommando:

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

Um eXpurgate SMTP aus einem RPM-Paket zu installieren, benutzen Sie folgendes Kommando:

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

Die Deinstallation erfolgt mit dem Kommando:

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

Um eXpurgate SMTP aus einem TGZ-Archiv zu installieren, befolgen Sie folgende Schritte:

Extrahieren Sie das Archiv.

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

Wechseln Sie in das neu angelegte Unterverzeichnis mit dem Namen *package*, in das die Dateien extrahiert wurden.

```
# cd <package>
```

Installieren Sie das Binary und die Konfigurationsdatei. (Für diesen und die folgenden Schritte benötigen Sie Administratorrechte.)

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

Installieren Sie das Init-Skript und die Datei mit den Default-Einstellungen.

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

Statt des generischen Init-Skripts, das sich für alle UNIX-ähnlichen Systeme eignet, können Sie eines der spezifischen Init-Skripte für eine Debian- oder RedHat-basierte Distribution oder für SUSE Linux installieren. In diesem Fall müssen Sie auch die dazugehörige Default-bzw. Sysconfig-Datei verwenden.

Das folgende Beispiel zeigt dies für eine RedHat-basierte Distribution. Beachten Sie, dass die Verzeichnis- und Dateinamen vom vorherigen Beispiel abweichen.

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

Legen Sie das Spool-, Run-, und Log-Verzeichnis an.

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

Nach der Installation des Pakets kopieren Sie die Lizenz-Key¹ in das Konfigurationsverzeichnis:

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

Zur Deinstallation einer Installation aus einem TGZ-Archiv entfernen Sie die oben kopierten Dateien und angelegten Verzeichnisse aus dem Dateisystem.

Um eXpurgate SMTP zu konfigurieren, editieren Sie die Konfigurationsdatei */etc/expurgate/expurgate.conf*. Zusätzlich können Sie eXpurgate SMTP auch Kommandozeilen-Optionen übergeben. Hierzu editieren Sie die Datei */etc/default/expurgate*, die vom Init-Skript beim Starten des Dienstes gelesen wird. Kommandozeilen-Optionen haben Vorrang vor Einstellungen in der Konfigurationsdatei. Nähere Informationen zur Konfiguration entnehmen Sie Abschnitt 3.

¹Die Lizenz-Key liegt als Binär-Datei vor, die Sie von ihrem Reseller bekommen oder aus dem Kundenbereich der eleven Website geladen haben. Sollten Sie keine Lizenz-Key besitzen, wenden Sie sich bitte an support@eleven.de.

2.1.2. Aktivieren und Deaktivieren des Dienstes

Der expurgate Dienst wird nicht automatisch gestartet, wenn Sie das Paket installieren. Die Schritte zur Aktivierung hängen von der von Ihnen gewählten Installationsmethode ab:

Wenn Sie von einem Debian-Paket installiert haben, editieren Sie die Datei `/etc/default/expurgate`. Setzen Sie dort die Variable `ENABLE` auf `yes`.

Wenn Sie von einem RPM-Paket installiert haben, führen Sie folgendes Kommando aus:

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

Wenn Sie das SUSE RPM-Paket installiert haben, sollten Sie entweder das YaST-Konfigurationstool verwenden, oder das folgende Kommando benutzen:

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

Wenn Sie von einem TGZ-Archiv installiert haben, sollten Sie sicherstellen, dass das Init-Skript auf den jeweiligen Run-Levels aufgerufen wird. Die genauen Schritte hierzu sind plattformabhängig.

Auf einem Debian-basierten System führen Sie folgendes Kommando aus:

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

Auf einem System wie Red Hat Enterprise Linux, Fedora oder CentOS lautet das Kommando:

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

Auf einem SUSE-System verwenden Sie folgendes Kommando:

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

Um den Dienst zu deaktivieren, führen Sie folgende Schritte aus:

Wenn Sie aus einem Debian-Paket installiert haben, setzen Sie in der Datei `/etc/default/expurgate` die Variable `ENABLE` wieder auf `no`.

Wenn Sie aus einem RPM-Paket installiert haben, führen Sie folgendes Kommando aus:

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

Auf einem SUSE-System verwenden Sie folgendes Kommando:

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

Wenn Sie von einem TGZ-Archiv installiert haben, sind die genauen Schritte plattformabhängig.

Auf einem Debian-basierten System führen Sie folgendes Kommando aus:

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

Auf einem System wie Red Hat Enterprise Linux, Fedora oder CentOS lautet das Kommando:

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

Auf einem SUSE-System verwenden Sie folgendes Kommando:

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

Durch die Deaktivierung des Dienstes wird eine bereits laufende Instanz nicht beendet. Lesen Sie hierzu den folgenden Abschnitt.

2.1.3. Starten und Beenden des Dienstes

Wenn Sie die im vorangehenden Abschnitt beschriebenen Schritte befolgt haben, wird eXpurgate SMTP beim nächsten Reboot automatisch gestartet. In diesem Abschnitt ist beschrieben, wie Sie den Dienst manuell starten und beenden.

Um eXpurgate SMTP durch das Init-Skript zu starten, geben Sie folgendes Kommando ein:

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

Um eXpurgate SMTP durch das Init-Skript zu beenden, benutzen Sie das folgende Kommando:

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

Weitere Optionen werden Ihnen angezeigt, wenn Sie das Init-Skript ohne Argumente aufrufen:

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

Ihre Linux-Distribution kann über ein spezialisiertes Kommando oder Programm zum Starten und Beenden von Diensten verfügen. Auf Debian-basierten Systemen ist dies zum Beispiel das Programm `/usr/sbin/invoke-rc.d`, auf Red Hat Enterprise Linux und Fedora das Programm `/sbin/service`.

Zum Testen ist es oft sinnvoll, das eXpurgate SMTP Binary direkt aufzurufen. Um eXpurgate SMTP manuell zu starten, ist folgende Kommandozeile einzugeben:

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

Um eXpurgate SMTP manuell zu beenden:

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

2.1.4. Verbindungstest

eXpurgate benötigt eine TCP-Verbindung zu den Netzen 194.145.224.0/24 und 195.190.135.0/24. Die Kommunikation erfolgt dabei über Port 55555. Bitte überprüfen Sie, ob diese Verbindung möglich ist. Beachten Sie dabei auch die Einstellungen Ihrer Firewall. Um die Erreichbarkeit der eXpurgate Server (eXdb) zu überprüfen, bietet eXpurgate die Kommandozeilen-Option `--test-exdbs`. Mit dieser Option aufgerufen versucht eXpurgate der Reihe nach jeden eingestellten eXpurgate Server zu kontaktieren und gibt eine Meldung aus, ob dies erfolgreich war.

Mit der korrekten Standard-Konfiguration erhalten Sie folgende Ausgabe:

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

```
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
```

Anmerkung: Für den Platzhalter `<path-to-config>` ist der absolute Pfad zur Konfigurationsdatei einzusetzen.

2.1.5. Weitere Anmerkungen

Eine Liste weiterer Optionen erhalten Sie durch Aufruf von `expurgate --help`.

Sollten beim Starten von eXpurgate SMTP Probleme auftauchen, finden Sie Fehlermeldungen in der Log-Datei. Standardmäßig befindet sich die Log-Datei in dem Verzeichnis `/var/log/expurgate`.

eXpurgate akzeptiert das HUP-Signal um während des Betriebs geänderte Konfigurationsdateien neu einzulesen. Wenn Sie eine der Optionen `chroot`, `uid` oder `gid` gesetzt haben, liest eXpurgate keine sicherheitsrelevanten Dateien wie Lizenz, TLS-Schlüssel und Zertifikate ein, wenn ein HUP-Signal empfangen wird. Beachten Sie in diesem Zusammenhang auch die Option `--always-reload`.

2.2. Installation von eXpurgate auf einem Windows-System

Wenn Sie eXpurgate unter Microsoft Windows installieren, werden die notwendigen Parameter bereits während des Installationsvorgangs abgefragt und eXpurgate anschließend als Dienst installiert und gestartet.

Um die Installation zu starten, doppelklicken Sie bitte auf die eXpurgate Installationsdatei. Es erscheint der Installationsassistent, der Sie durch die weitere Installation leitet.

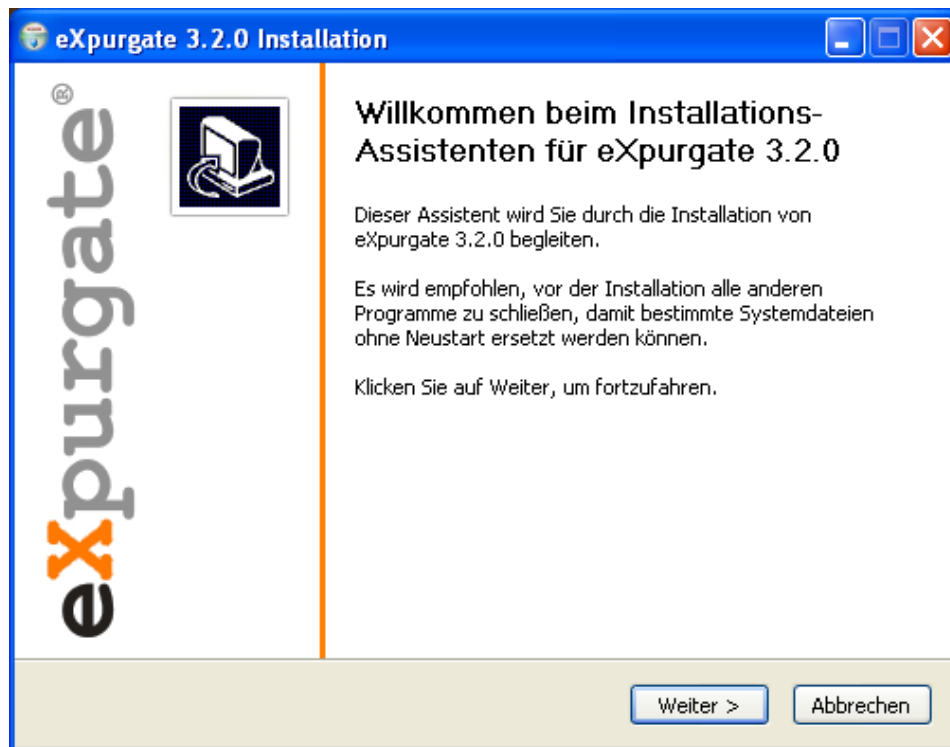


Abbildung 2.1.: Startseite des Installationsassistenten

Klicken Sie auf WEITER, um mit der eigentlichen Installation zu beginnen.

Bitte lesen Sie die Lizenzbedingungen aufmerksam durch. Klicken Sie in das Feld vor ICH AKZEPTIERE DAS LIZENZABKOMMEN, danach auf WEITER.

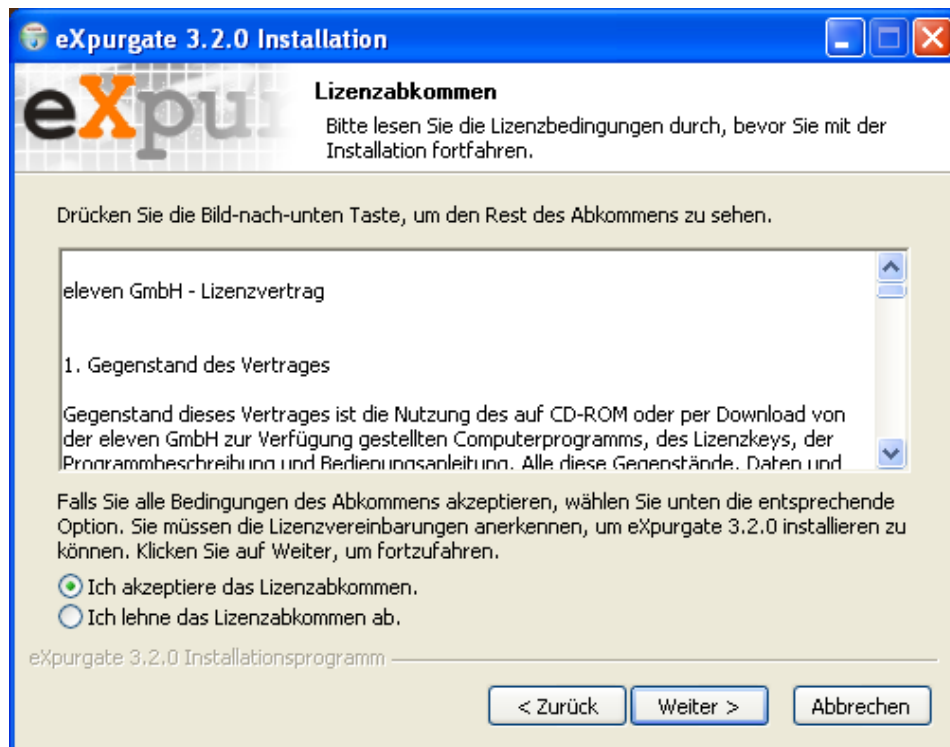


Abbildung 2.2.: Lizenzvereinbarung

Wählen Sie nun das Verzeichnis aus, in das eXpurgate installiert werden soll. Die Voreinstellung entspricht dem Verzeichnis *eleven*eXpurgate unterhalb Ihres Programmverzeichnisses (z.B. *C:\Programme\eleven*eXpurgate). Sie können dieses jedoch beliebig an Ihre Installationsvorgaben anpassen.



Abbildung 2.3.: Auswahl des Zielverzeichnisses

Geben Sie an, an welcher Stelle eXpurgate im Windows-Startmenü gelistet werden soll, und klicken Sie auf WEITER.

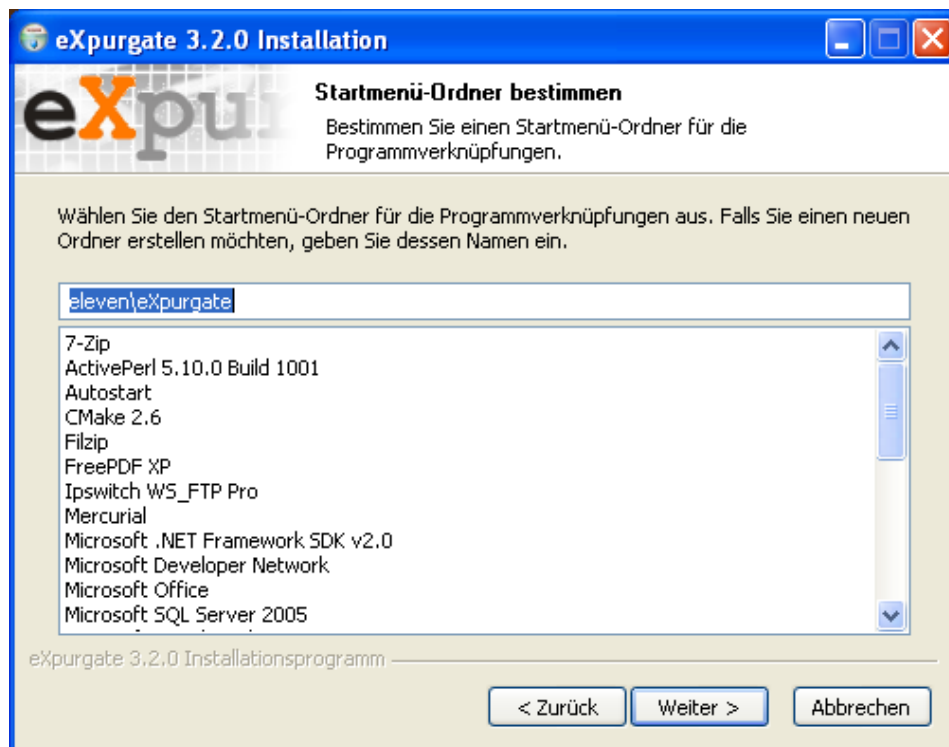


Abbildung 2.4.: Einfügen von eXpurgate in das Startmenü

Unter den Verbindungsoptionen müssen Sie angeben, auf welcher Netzwerkschnittstelle und Port eXpurgate eingehende E-Mails annehmen soll (Default: 0.0.0.0:25).

Als E-Mail-Server-Host und TCP/IP Port geben Sie an, unter welcher Adresse und welchem Port eXpurgate Ihren bestehenden E-Mail-Server erreichen kann. Sollen eXpurgate und der bestehende Server auf demselben Rechner laufen, müssen Sie Ihren E-Mail-Server umkonfigurieren, indem Sie dessen Port in einen bislang ungenutzten ändern. Anderenfalls tragen Sie hier den Namen der anderen Maschine und den Port des Mailers darauf ein.

Nachdem Sie die den Pfad zur eXpurgate Lizenzdatei angegeben und die Einträge mit einem Klick auf WEITER bestätigt haben, versucht eXpurgate Ihren bereits vorhandenen E-Mail-Server auf dem soeben angegebenen Port anzusprechen. Ist dieser erreichbar, gelangen Sie mit einem Klick auf WEITER zum nächsten Fenster BEHANDLUNG VON SPAM-E-MAILS.

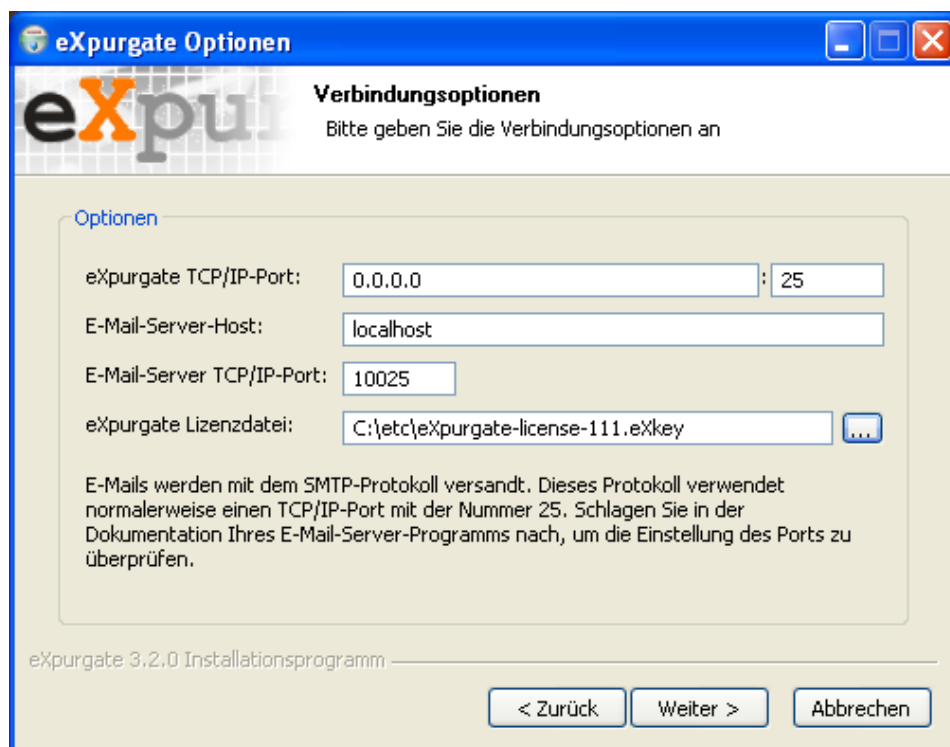


Abbildung 2.5.: Verbindungsoptionen

Im Fenster BEHANDLUNG VON SPAM E-MAILS können Sie festlegen, wie Spam-E-Mails behandelt werden sollen. Hier können Sie einstellen, ob diese lediglich mit einem Header-Eintrag versehen an den Empfänger zugestellt oder an eine (Sammel-) Adresse zugestellt werden. Alternativ können Sie hier einstellen, ob Spam bereits bei der Einlieferung zurückgewiesen (*reject*) oder angenommen und anschließend gelöscht werden soll.

Klicken Sie auf WEITER.

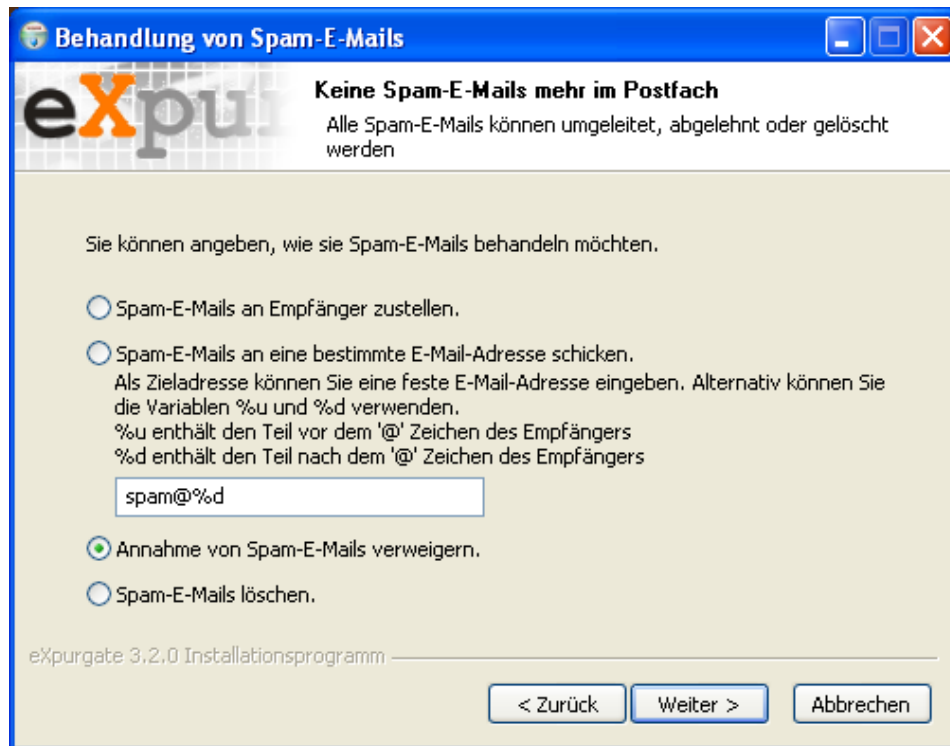


Abbildung 2.6.: Weitere Behandlung der Spam-E-Mails

Mit der Option **UMSCHREIBEN DER BETREFFZEILE** können Sie für kategorisierte Massen-E-Mails deren Betreffzeile (*Subject*) umschreiben lassen. Auf diese Weise erhalten Sie schnell einen Überblick, um welchen E-Mail-Typ es sich handelt und ob es sinnvoll oder gar gefährlich wäre, die E-Mail zu öffnen. Dieses Verfahren eignet sich besonders dann, wenn die E-Mail nach der Kategorisierung durch eXpurgate manuell geprüft werden soll.

Sie können für die Typen *spam*, *bulk* und/oder *dangerous* (gefährlich) festlegen, nach welchem Schema die Betreffzeile umgeschrieben werden soll. Die Voreinstellung [%t] %s bewirkt beispielsweise, dass die Betreffzeile einer eingehenden Spam-E-Mail mit dem Betreff *Hi Allen, make money fast* umgeschrieben wird zu *[spam] Hi Allen, make money fast* und somit schneller zu sortieren ist.

Klicken Sie auf **WEITER**, um zu den SSL/TLS-OPTIONEN zu gelangen.

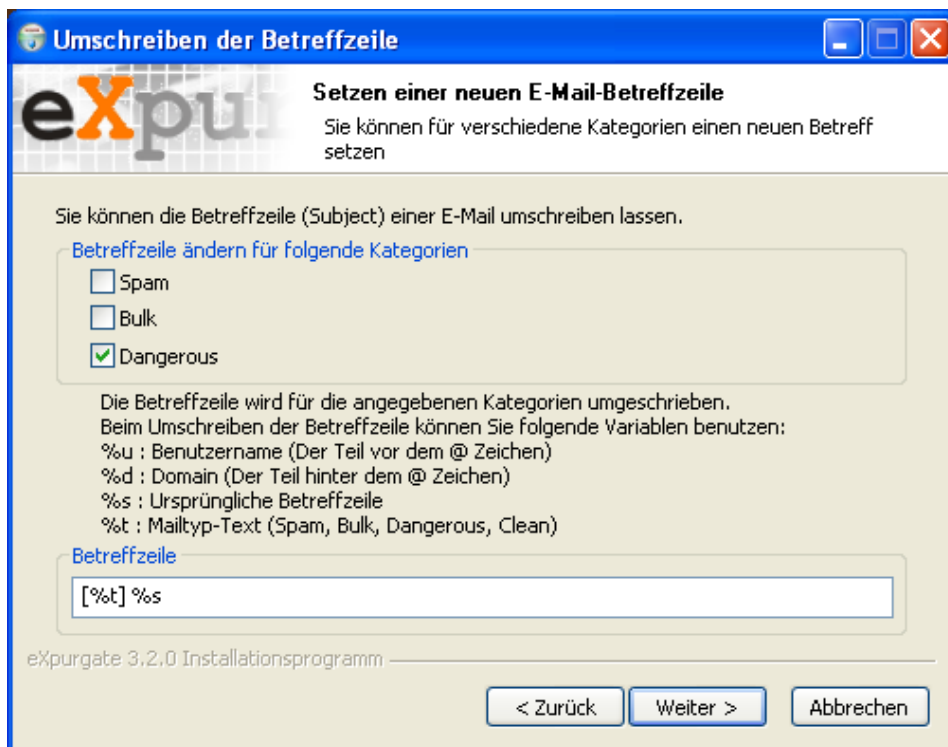


Abbildung 2.7.: Umschreiben der Betreffzeile

Die SSL/TLS-Optionen dienen der sicheren Verschlüsselung des Übertragungswegs zwischen geeigneten Servern. Falls Sie dieses Verfahren nicht verwenden, sollten Sie hier keine Änderungen vornehmen und auf WEITER klicken.

Nähere Informationen zum SSL/TLS-Verfahren erhalten Sie im Abschnitt 3.2.5 dieser Dokumentation. Für die im Internet übliche E-Mail-Übertragung mittels SMTP und das Funktionieren von eXpurgate ist diese Option nicht erforderlich, kann also in den meisten Fällen deaktiviert bleiben.

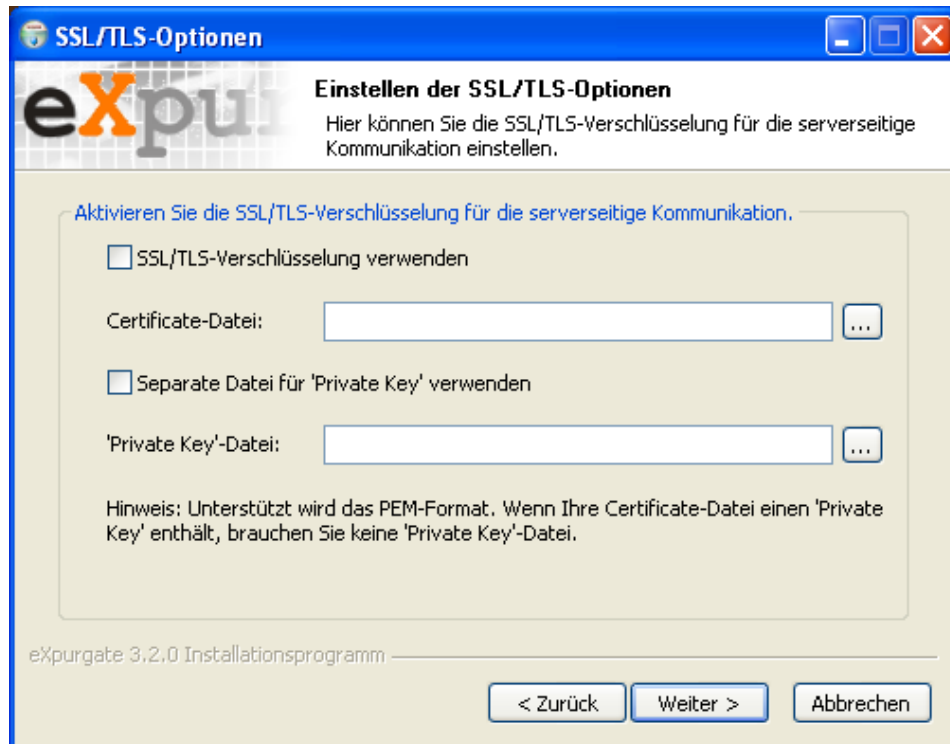


Abbildung 2.8.: Auswahl der SSL/TLS-Optionen

Zum Abschluss der Installation werden Ihre Angaben zusammengefasst. Bitte kontrollieren und korrigieren Sie sie falls nötig. Klicken Sie danach auf **INSTALLIEREN**.

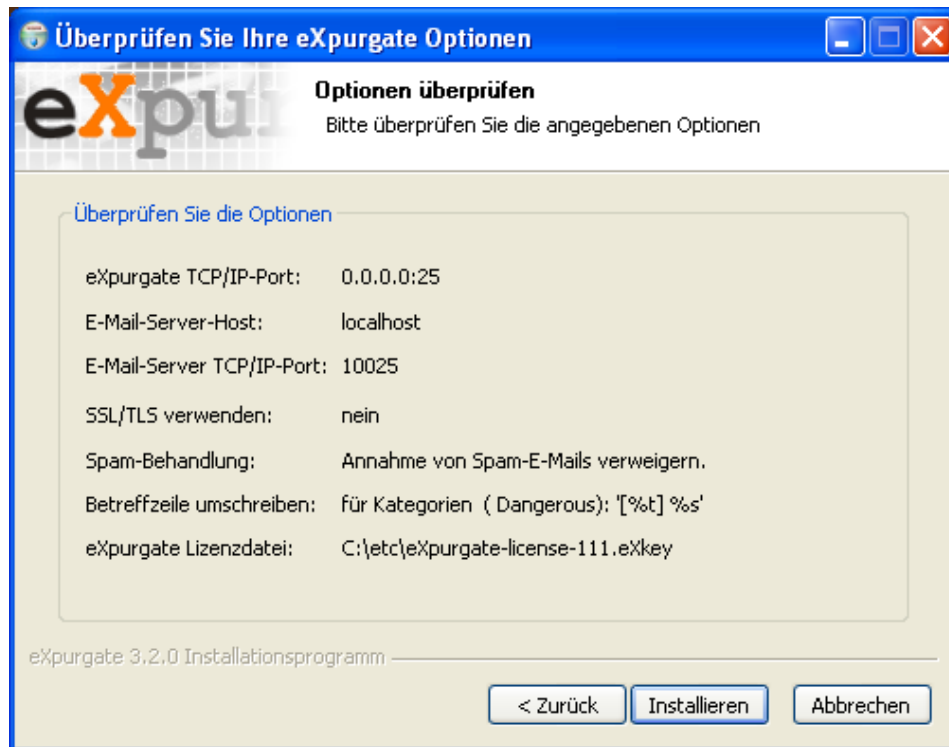


Abbildung 2.9.: Prüfen der eingegeben Daten

Nun wird eXpurgate gemäß Ihren Vorgaben auf Ihrem Rechner installiert, als Windows-Dienst hinzugefügt und gestartet.

Am Ende der Installation wird noch die Verbindung zu den eXpurgate Servern (eXdb Server) bei eleven geprüft. Wenn die Installation erfolgreich war, gelangen Sie zum letzten Bild.



Abbildung 2.10.: Abschlussbildschirm der Installation

Zum Beenden des Installationsassistenten klicken Sie bitte auf **FERTIGSTELLEN**. Die eXpurgate Installation ist nun betriebsbereit. eXpurgate protokolliert seine Starts zusammen mit den verwendeten Kommandozeilenoptionen in der Windows-Ereignisanzeige (Event Log, zu finden via **START/PROGRAMME/VERWALTUNG/EREIGNISANZEIGE**). Hier erhalten Sie auch erste Hinweise auf mögliche Fehler.

2.2.1. Windows-Dienst-Kommandos

eXpurgate wird unter Microsoft Windows als Dienst installiert, so dass eXpurgate automatisch — ohne Benutzeranmeldung — nach einem Systemstart gestartet wird. Sie können dies unter **START/PROGRAMME/VERWALTUNG/DIENSTE** überprüfen.

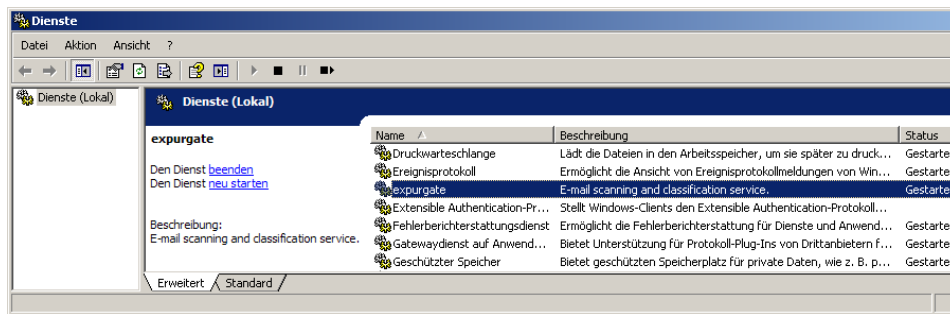


Abbildung 2.11.: Eintrag von eXpurgate als Dienst in der Microsoft-Dienste-Konsole

Für die Steuerung von eXpurgate als Windows-Dienst stehen Ihnen auf der Kommandozeile die folgenden Parameter zur Verfügung:

install	Installiert eXpurgate als Windows-Dienst, ohne ihn zu starten. Die Start-Parameter müssen folgend angegeben werden.
remove	Deinstalliert eXpurgate als Windows-Dienst.
start	Startet den bereits installierten eXpurgate Dienst.
stop	Beendet den installierten eXpurgate Dienst.
isinstalled	Überprüft, ob eXpurgate als Dienst installiert wurde.
isrunning	Überprüft, ob eXpurgate gegenwärtig als Dienst läuft.
getparameter	Gibt die Parameter zurück, mit denen der Dienst gestartet wird.
setparameter	Setzt neue Start-Parameter (analog zu install).

2.2.2. Ändern des TCP-Ports bei Microsoft Exchange 5.5

Wenn Sie eXpurgate mit Microsoft Exchange 5.5 auf demselben Server einsetzen wollen, müssen Sie dafür sorgen, dass Exchange E-Mails auf einem anderen Port als 25 entgegen nimmt. Der SMTP-Connector von Exchange 5.5 übernimmt dabei den Port, der in der Datei *services* definiert ist. Diese Datei befindet sich unterhalb Ihres Windows-Verzeichnisses (*%SystemRoot%* bzw. *C:\WINNT*) in *system32\drivers\etc*. Die Datei können Sie z.B. wie folgt editieren:

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

Der Datei *services* liegt folgendes Schema zugrunde:


```
Dienst Port/Protokoll [Alias...] [#Kommentar]
```

Der Eintrag für das SMTP-Protokoll sieht typischerweise wie folgt aus:

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

Ändern Sie bitte den Wert für den Dienst smtp (default: 25/tcp) auf einen neuen, freien Port, auf dem Ihr Exchange E-Mails entgegennehmen soll, wie z.B. 10025. Entsprechend müsste der geänderte Eintrag in der Datei *services* wie folgt aussehen:

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

Anschließend muss der Dienst neu gestartet werden, damit die Änderung wirksam werden kann. Sie können dies mit Hilfe von `telnet` testen.

2.2.3. Ändern des TCP-Ports bei Microsoft Exchange 2000 bzw. 2003

Die Möglichkeit den Port des Exchange zu ändern, auf dem E-Mails entgegengenommen werden, ist bei Exchange 2000 bzw. 2003 bereits vorgesehen. Deshalb gibt es innerhalb des Programms eine entsprechende Option. Um diese zu erreichen, gehen Sie bitte wie folgt vor:

- Öffnen Sie den Exchange-System-Manager (i.d.R. im Startmenü unter Programme/Microsoft Exchange/System-Manager).
- Klicken Sie im System-Manager auf `SERVER`, dann auf den betreffenden Server und unter `/PROTOKOLLE/SMTP` mit der rechten Maustaste auf `VIRTUELLER STANDARDSERVER FÜR SMTP`, um im dann aufgehenden Menü auf `EIGENSCHAFTEN` zu klicken.

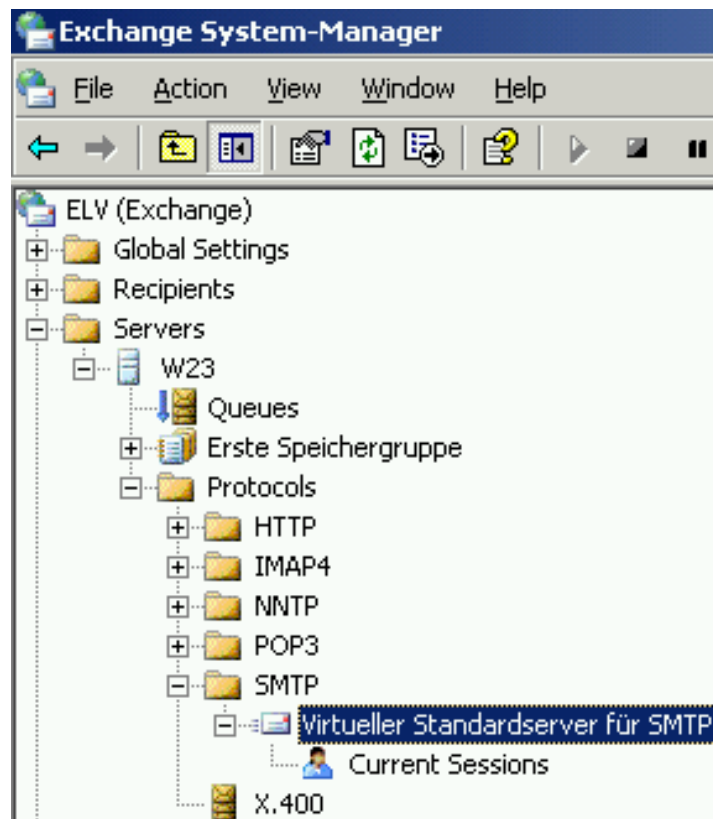


Abbildung 2.12.: Exchange-System-Manager

Wählen Sie auf der Registerkarte GENERAL die IP-Adresse des Servers aus und klicken Sie dann auf ADVANCED.

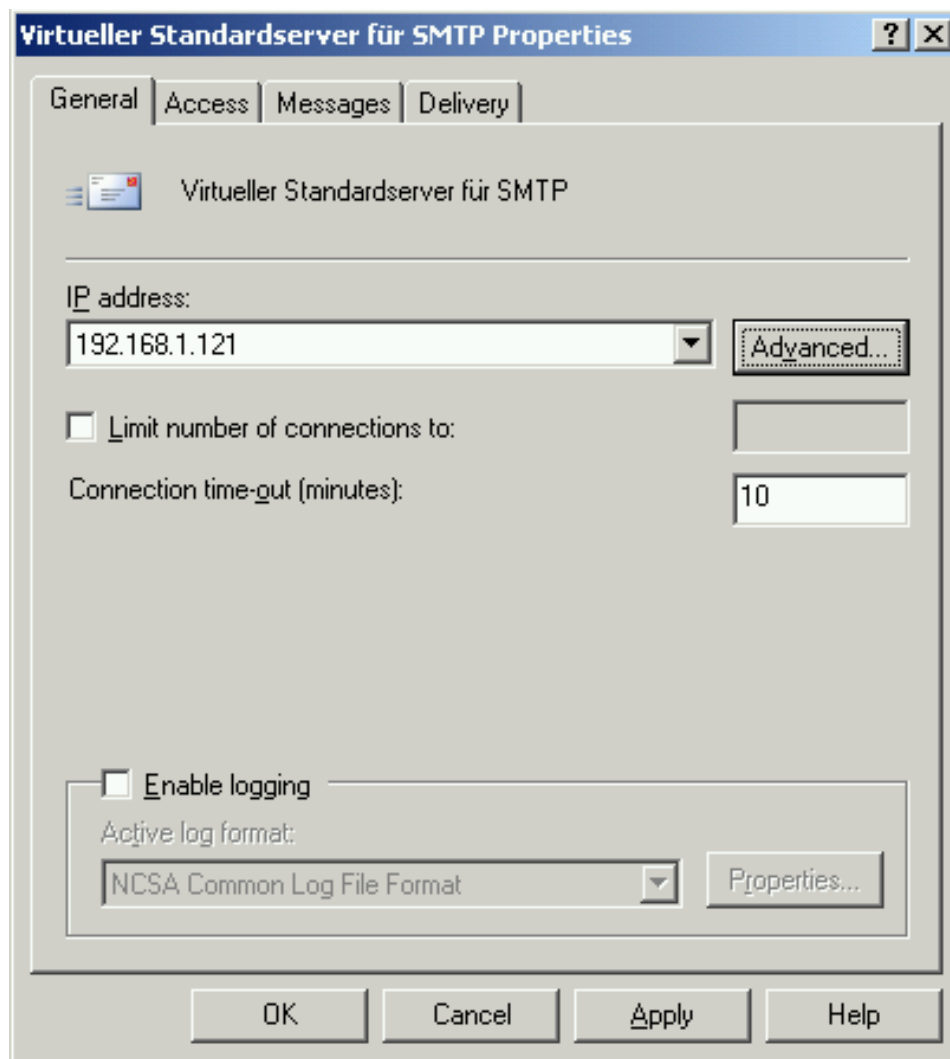


Abbildung 2.13.: Virtueller Standardserver

Klicken Sie auf **EDIT**, um die Eigenschaften dieses virtuellen Servers bearbeiten zu können.

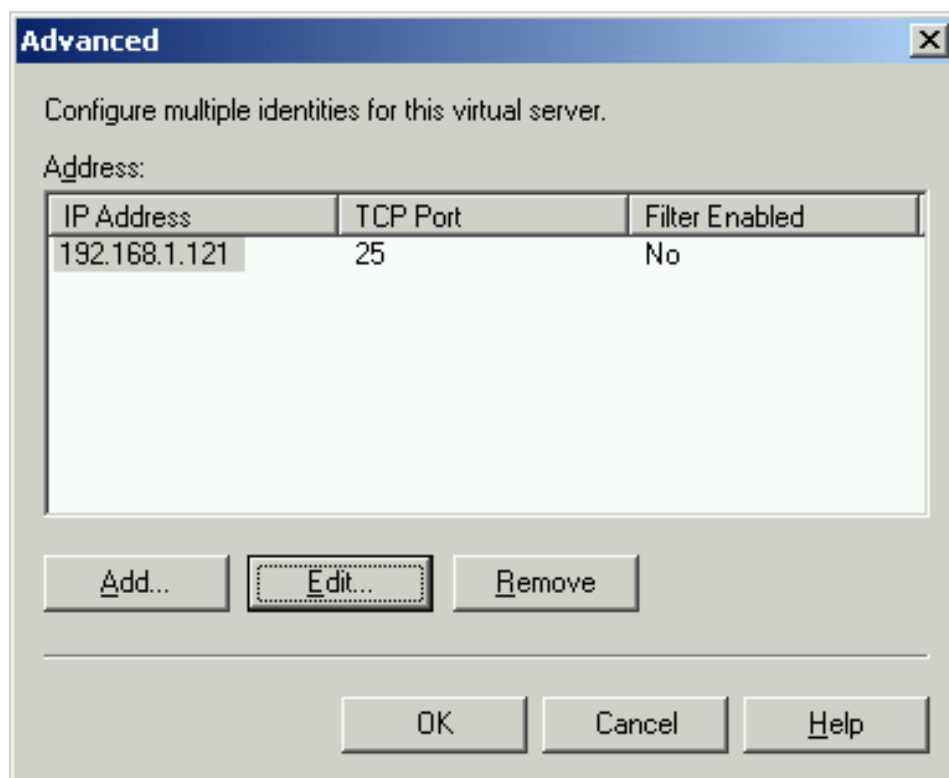


Abbildung 2.14.: Advanced

Hier können Sie unter TCP PORT den Port ändern, auf dem Ihr Exchange eingehende E-Mails entgegennehmen soll. Tragen Sie dort einen anderen, bislang ungenutzten Port ein (z.B. 10025) und bestätigen Sie die Änderung mit OK.

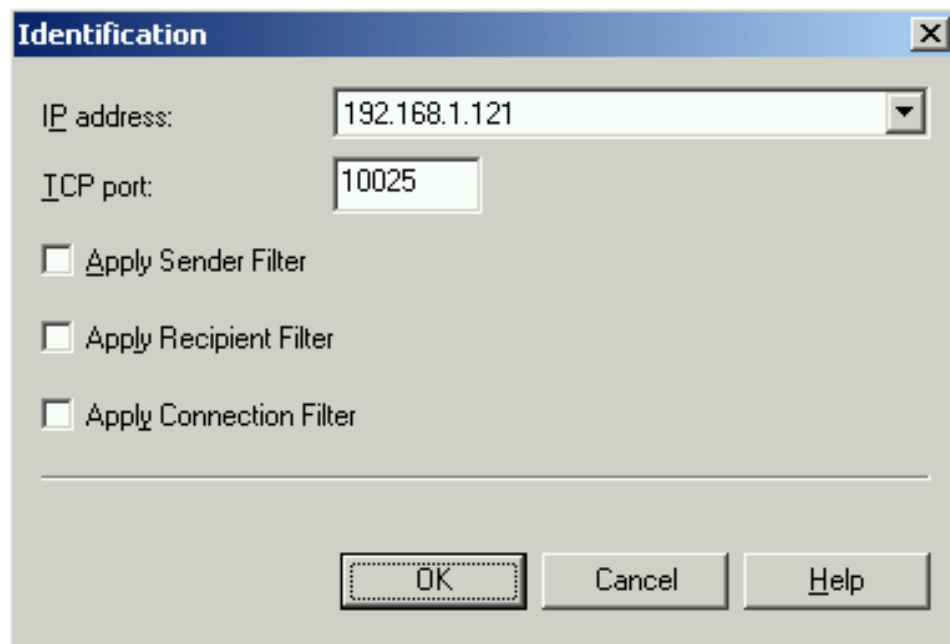


Abbildung 2.15.: Identifikation

Mit einem weiteren OK gelangen Sie zurück zum Exchange-System-Manager. Halten Sie anschließend den virtuellen Server an, um ihn dann neu zu starten. Nun sollte Ihr Exchange auf dem Port 10025 erreichbar sein. Lesen Sie bitte den folgenden Abschnitt, um zu testen, ob die Änderung erfolgreich war.

2.2.4. Testen, ob Exchange auf einem Port antwortet

Wenn Sie testen möchten, ob Ihr Exchange-Server die Änderung des Ports übernommen hat, können Sie dies mit Hilfe von `telnet` testen. Öffnen Sie dazu eine Kommandozeile und geben Sie folgendes Kommando ein:

```
telnet 192.168.1.121 10025
```

Dabei verwenden Sie statt 192.168.1.121 die IP-Adresse Ihres Exchange-Servers, wobei 10025 dem neuen TCP-Port entspricht. Ihr Exchange-Server sollte Sie nach erfolgreicher Änderung und Neustart des virtuellen SMTP-Servers etwa wie folgt begrüßen:

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

Beenden Sie den SMTP-Dialog mit dem Exchange-Server durch die Eingabe von `quit`. War dieser Test erfolgreich, können Sie eXpurgate auf Port 25 starten, damit eXpurgate eingehende E-Mails nach der Klassifizierung an den Exchange-Server weiterleitet.

3. Die Konfiguration von eXpurgate

Die Konfiguration von eXpurgate erfolgt durch die Konfigurationsdatei *expurgate.conf*. Alternativ können einige Einstellungen auch direkt über die Kommandozeile gesetzt werden. Beide Konfigurationsmöglichkeiten finden Sie in den Abschnitten dieses Kapitels erklärt. Einstellungen auf der Kommandozeile haben Vorrang vor Einstellungen in der Konfigurationsdatei. Dies gilt auch für solche Einstellungen, die typischerweise mehrfach verwendet werden.

Beispiel: Werden sowohl auf der Kommandozeile als auch in der Konfigurationsdatei eXpurgate Server definiert (durch die Option `--exdb` bzw. die `Server` in der `SpamEngine`-Sektion der Konfigurationsdatei), so gelten allein die auf der Kommandozeile genannten Server.

Die Konfigurationsdatei, sowie alle darin eingetragenen Dateien, werden eingelesen bevor der eXpurgate auf die konfigurierte User- und Group-ID, sowie in das neue Wurzelverzeichnis wechselt. Es ist somit möglich, sicherheitsrelevante Dateien, wie Lizenz, SSL-Schlüssel und Zertifikate, außerhalb des konfigurierten Wurzelverzeichnis bzw. nur für privilegierte Nutzer lesbar zu halten.

Falls eXpurgate zusammen mit *Avira AntiVir* ("savapi") laufen soll, so muss sich AntiVir in der gleichen Chroot-Umgebung befinden.

Anmerkung: Für die meisten Einstellungen sind bereits sinnvolle Werte eingetragen, diese brauchen daher nicht geändert zu werden. eXpurgate benötigt jedoch folgende obligatorische Einstellungen, damit der Dienst gestartet werden kann:

Das Arbeitsverzeichnis Dieses kann entweder in der Konfigurationsdatei unter `WorkingDirectory` oder als Kommandozeilenparameter `--working-dir (-w)` angegeben werden.

Die Lizenzdatei Diese Datei kann ebenfalls entweder über die Konfigurationsdatei unter `LicenseFile` oder über die Kommandozeile als `--license (-l)` definiert werden.

eXpurgate kann sowohl mit IPv4- als auch mit IPv6-Adressen umgehen. Soll eine IPv6-Adresse in Kombination mit einer Port-Nummer konfiguriert werden, muss die IP-Adresse von eckigen Klammern umschlossen sein. Beachten Sie bei der Benutzung von IPv6 außerdem, dass Optionen die sich auf IP-Adressen beziehen, wie zum Beispiel `Permissions` oder `UserSettings` in der Konfigurationsdatei, ausschließlich mit IPv6-Adressen benutzt werden. Ferner sind die öffentlichen eXpurgate Server nur über IPv4 zugänglich.

3.1. Die Kommandozeilen-Optionen

Mit Hilfe der folgenden Kommandozeilen-Optionen lässt sich eXpurgate konfigurieren. Eine Übersicht der möglichen Optionen erhalten Sie auch, wenn Sie `expurgate --help` eingeben.

Im folgenden Abschnitt ist zunächst der Name der Option angegeben, dann mögliche Argumente und schließlich eine kurze Beschreibung der Funktionsweise. Die Optionen werden jeweils mit zwei vorangestellten Bindestrichen angegeben. Wenn eine Option mehrfach verwendet werden kann, ist dies im Folgenden ausdrücklich angegeben. Kann eine Option nicht mehrfach verwendet werden, so wird allein die letzte Angabe der Option berücksichtigt.

Beispiel: Wird die Option `--exdb` (Angabe eines eXpurgate Servers) mehrfach verwendet, so werden sämtliche angegebenen eXpurgate Server eingetragen. Wird dagegen die Option `--listen` (Angabe des SMTP-Server-Interfaces und -Ports) mehrfach verwendet, so *lauscht* eXpurgate allein auf der zuletzt angegebenen Adresse.

Optionen, die kein Argument erwarten, gibt es in einer verneinten Form, wobei dem Optionsnamen ein `no-` vorangestellt wird. Dies ist sinnvoll, um abweichende Einstellungen in der Konfigurationsdatei oder in einer vorangehenden Option abzuändern.

Beispiel: Durch die Option `--no-antivir` kann eine Aktivierung des Virenschanners in der Konfigurationsdatei wieder abgeschaltet werden.

3.1.1. Optionen zur Ausgabe von Informationen

Durch Angabe der folgenden Kommandozeilen-Optionen können Sie Informationen zur Verwendungsweise und Version von eXpurgate SMTP ausgeben lassen. Das Programm beendet sich unmittelbar nach der Ausgabe, ohne eXpurgate SMTP zu starten.

Option	Beschreibung
<code>--help</code>	Gibt die möglichen Optionen aus.
<code>--version</code>	Gibt die Programmversion aus.
<code>--vcsid</code>	Gibt die interne Versionsnummer des Programms aus.
<code>--compiler</code>	Gibt den Programmnamen und die Version des verwendeten Compilers aus.
<code>--show-license DATEI</code>	Gibt die Lizenzinformationen zur angegebenen Datei aus.

3.1.2. Optionen für den Betrieb unter Unix

Folgende Einstellungen können vorgenommen werden, wenn eXpurgate SMTP in einer Unix-Umgebung läuft.

Option	Beschreibung
--------	--------------

<code>--daemonize</code>	Löst eXpurgate SMTP von der Konsole und lässt es als Hintergrund-Prozess laufen (System-Daemon). <code>--no-daemonize</code> deaktiviert diese Funktionalität.
<code>--pidfile DATEI</code>	Schreibt die Prozess-ID von eXpurgate SMTP in die angegebene Datei.
<code>--chroot VERZEICHNIS</code>	Angabe eines neuen root-Verzeichnisses, in das eXpurgate SMTP nach dem Start wechseln soll.
<code>--uid USER-ID</code>	Setzt nach der Initialisierung den effektiven Benutzer auf die angegebene (nicht privilegierte) Benutzer-ID.
<code>--gid GROUP-ID</code>	Setzt nach der Initialisierung die effektive Gruppe auf die angegebene (ebenfalls nicht privilegierte) Gruppen-ID.

3.1.3. Optionen zur Protokollierung von Log-Meldungen

eXpurgate SMTP bietet die Möglichkeit, bestimmte Log-Meldungen über unterschiedliche Log-Ziele auszugeben. Dafür folgt jeder Option eine Angabe von Wichtigkeitsstufen (Log-Levels), die bestimmt, welche Log-Meldungen in das jeweilige Log-Ziel geschrieben werden. Zu den Log-Zielen gehören Log-Dateien, die Standard-Fehlerausgabe, der System-Logger (Unix), die System-Konsole (Unix) und das Event-Log (Windows).

Beispiel: Durch die Option `--log-file ERROR-EMERGENCY:/var/log/expurgate/error.log` werden alle Fehlermeldungen in die Datei `/var/log/expurgate/error.log` geschrieben.

Option	Beschreibung
<code>--log-file MIN-MAX:DATEI</code>	Die Log-Levels und der Dateiname der Log-Datei. Diese Option kann mehrfach verwendet werden, um zum Beispiel unterschiedliche Log-Levels in separate Dateien zu loggen.
<code>--log-stderr MIN-MAX</code>	Log-Levels für die Standard-Fehlerausgabe.
<code>--log-syslog MIN-MAX:FACILITY</code>	Log-Levels für den System-Logger auf Unix-Systemen.
<code>--log-console MIN-MAX</code>	Log-Levels für die System-Konsole (<code>/dev/console</code>) auf Unix-Systemen.
<code>--log-event MIN-MAX</code>	Log-Levels für das Event-Log auf Windows-Systemen.

Im Folgenden sind die Wichtigkeitsstufen von Log-Meldungen aufgelistet.

DEBUG Interne Log-Meldung mit niedriger Priorität.

INFO Information zur normalen Funktionsweise.

NOTICE Meldung zu besonderen Ereignissen.

WARNING Warnung bei ungewöhnlichen Ereignissen.

ERROR Meldung zu nicht-kritischen Fehlermeldungen.

CRITICAL Meldung zu kritischen Fehlerzuständen.

ALERT Der Fehlerzustand erfordert einen sofortigen Eingriff.

EMERGENCY Das System ist nicht mehr funktionsfähig.

Untergrenze oder die Obergrenze können entfallen, wenn es sich um die niedrigste bzw. höchste Wichtigkeitsstufe handelt.

Beispiel: Durch die Option `--log-stderr -NOTICE` werden nur Log-Meldungen unterhalb der Wichtigkeitsstufe `WARNING` an die Standard-Fehlerausgabe gesendet.

Ist lediglich eine Wichtigkeitsstufe angegeben, so wird diese als Untergrenze interpretiert.

Beispiel: Durch die Option `--log-console CRITICAL` werden alle kritischen Fehlermeldungen auf der System-Konsole ausgegeben, einschließlich solcher der Wichtigkeitsstufe `ALERT` und `EMERGENCY`.

Bitte beachten Sie, dass nicht beide Grenzen entfallen können. Ein schlichter Aufruf von `--log-stderr` ohne Parameter führt zu einem Fehler beim Programmaufruf.

Das `FACILITY`-Feld bei der Option `--log-syslog` gibt an, um welche Art von Programm es sich handelt. Typischerweise wird der Wert `MAIL` verwendet. Erlaubte Werte sind

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

Beispiel: Durch die Option `--log-syslog NOTICE:MAIL` werden alle nicht rein informativen Log-Meldungen durch den System-Logger mit der Facility `MAIL` geloggt.

3.1.4. Optionen zum Testen von eXpurgate

Mit den folgenden Optionen lassen sich verschiedene Einstellungen von eXpurgate auf ihre Korrektheit überprüfen.

Option	Beschreibung
<code>--test-config</code>	Überprüft, die mit <code>--config</code> geladene Konfiguration auf Korrektheit.
<code>--test-exdb</code>	Überprüft, ob die konfigurierten eXpurgate Server erreichbar sind.
<code>--test-relays</code>	Überprüft, ob alle konfigurierten Relay-Server erreichbar sind.
<code>--test-tls</code>	Überprüft die TLS-Konfiguration bzw. die angegebenen Private-Keys und/oder Zertifikate.
<code>--test-ensurance</code>	Überprüft die Verfügbarkeit und die Konfiguration der enSurance 3.x.

3.1.5. Optionen zur allgemeinen Funktionsweise

Die nachfolgenden Kommandozeilen-Optionen betreffen die Funktionsweise von eXpurgate im Allgemeinen.

Option	Beschreibung
<code>--config DATEI</code>	Lädt die angegebene Konfigurationsdatei. Liegt diese Datei nicht im aktuellen Arbeitsverzeichnis, muss sie mit Pfad angegeben werden — eine automatische Suche unter <code>/etc/expurgate</code> findet nicht statt.
<code>--working-dir VERZEICHNIS</code>	Definiert das Arbeitsverzeichnis von eXpurgate, in dem zur Laufzeit benötigte Daten abgelegt werden.
<code>--license DATEI</code>	Lädt die angegebene eXpurgate Lizenz.
<code>--always-reload</code>	Weist eXpurgate an, auch bei gesetztem <code>--chroot</code> , <code>--uid</code> und/oder <code>gid</code> sicherheitsrelevante Dateien neu einzulesen, wenn das HUP-Signal empfangen wird. Ohne diese Option aktualisiert eXpurgate bei einem HUP-Signal Zertifikate oder TLS-Dateien nicht, auch wenn diese in der Konfigurationsdatei geändert wurde.

3.1.6. Optionen für den SMTP-Server

Folgende Einstellungen lassen sich von der Kommandozeile aus für den SMTP-Server vornehmen.

Option	Beschreibung
<code>--listen HOST:PORT</code>	Setzt die IP-Adresse (das Interface) und den Port, auf dem der SMTP-Server auf eingehende Verbindungen lauscht.
<code>--max-connections ZAHL</code>	Limitiert die maximale Anzahl parallel bestehender Verbindungen.
<code>--tls-certificate DATEI</code>	Verwendet die angegebene Datei als TLS-Zertifikat.
<code>--tls-private-key DATEI</code>	Verwendet die angegebene Datei als Private-Key für die TLS-Verschlüsselung.
<code>--tls-on-connect</code>	Schaltet TLS für eine eingehende Verbindung über SMTP ein. Diese Option kann auch mit <code>--no-tls-on-connect</code> deaktiviert werden.
<code>--local-domain DOMAIN</code>	Betrachtet die angegebene Domain als lokal. E-Mails dieser Domain werden immer angenommen. Dieser Parameter kann mehrfach angegeben werden.

3.1.7. Optionen für nachgelagerte SMTP-Relays

Mit folgender Einstellung können die nachgelagerten SMTP-Relays konfiguriert werden. Bitte beachten Sie, dass in der Konfigurationsdatei eine wesentlich detailliertere Konfiguration der Relays vorgenommen werden kann.

Option	Beschreibung
<code>--smtp-out HOST:PORT</code>	Definiert einen nachgelagerten SMTP-Server, über den E-Mails ausgeliefert werden können. Dieser Parameter kann mehrfach angegeben werden.

3.1.8. Optionen für die Spam-Engine

In diesem Abschnitt lassen sich Einstellungen vornehmen, die die interne Verarbeitung von E-Mails betreffen.

Option	Beschreibung
<code>--exdb HOST:PORT</code>	Hostname und Port des eXpurgate Servers, der verwendet werden soll. Achtung: Wird diese Option verwendet, werden eventuelle Einträge in der Konfigurationsdatei ignoriert. Diese Option kann mehrfach verwendet werden.
<code>--socks HOST:PORT</code>	Für die Kommunikation zum eXpurgate Server wird der angegebene SOCKS-Proxy verwendet.
<code>--socks-user USERNAME</code>	Optionaler Benutzername für den SOCKS Proxy-Server.
<code>--socks-pass PASSWORD</code>	Optionales Passwort für den SOCKS Proxy-Server.
<code>--threads ZAHL</code>	Anzahl der parallelen Threads, die E-Mails klassifizieren. Dieser Wert ist typischerweise erheblich kleiner als der Wert der Option <code>--max-connections</code> .

3.1.9. Optionen zur Konfiguration des Virencanners

Die folgenden Kommandozeilen-Optionen erlauben es, den AntiVir-Virencanner zu aktivieren und seine Funktionsweise einzustellen.

Option	Beschreibung
<code>--antivir</code>	Schaltet den Virencanner ein. Diese Option kann auch mit <code>--no-antivir</code> deaktiviert werden.
<code>--antivir-port PORT</code>	Port des Virencanners.

3.1.10. Optionen für das Simple Network Management Protocol

Mit Hilfe der folgenden Kommandozeilen-Optionen wird das Simple Network Management Protocol (SNMP) konfiguriert, mit dem eXpurgate über eine Netzwerk-Management-Software überwacht werden kann. Die Konfiguration über die Konfigurationsdatei bietet mehr Möglichkeiten als über die Kommandozeile. Lesen Sie dazu bitte den Abschnitt 3.2.8.

Option	Beschreibung
<code>--snmp</code>	Mit dieser Option schalten Sie SNMP in eXpurgate ein. Mit der Option <code>--no-snmp</code> kann SNMP explizit abgeschaltet werden.
<code>--snmp-address HOST:PORT</code>	Hostname und Port geben das Interface an, über das die Netzwerk-Management-Software eXpurgate überwachen kann.
<code>--snmp-community PASSWORD</code>	Das Passwort wird benutzt, um auf eXpurgate zuzugreifen. Wichtig ist, dass der Wert in eXpurgate und in der Netzwerk-Management-Software identisch ist, da sonst keine Daten von eXpurgate abgefragt werden können.

3.1.11. Optionen für das Freezing

Mit den folgenden Optionen kann das Freezing, also die verzögerte Zustellung von E-Mails eingestellt werden. Erweiterte Einstellungen finden Sie hierzu in der Konfigurationsdatei.

Option	Beschreibung
<code>--freezing</code>	Aktiviert das Freezing. Das Freezing kann hier auch explizit über <code>--no-freezing</code> abgeschaltet werden.
<code>--fridge-dir VERZEICHNIS</code>	Definiert das Verzeichnis, das zum Speichern der eingefrorenen E-Mails verwendet werden soll. Dieses Verzeichnis darf nicht das Arbeitsverzeichnis sein und muss sich auf dem gleichen Speichermedium befinden, auf dem auch das Arbeitsverzeichnis liegt.

3.2. Die Konfigurationsdatei

Die Konfiguration von eXpurgate erfolgt durch die Konfigurationsdatei *expurgate.conf*. Sie befindet sich im Verzeichnis */etc/expurgate* unter Unix und *C:\Programme\eleven\eXpurgate\etc* unter Windows. Der Name der Konfigurationsdatei wird über die Kommandozeilen-Option `--config (-c)` angegeben. Die meisten Einstellungen werden mit einem sinnvollen Wert vorinitialisiert, so dass sie in der Regel nicht manuell gesetzt werden müssen.

Anmerkung: Bitte beachten Sie, dass eXpurgate standardmäßig nicht filtert. Damit Spam-E-mails nicht mehr zugestellt werden, muss die Standardeinstellung im Abschnitt `<UserSettings>` geändert werden (siehe "4.4 E-Mail-Verarbeitung festlegen").

Die eXpurgate Konfigurationsdatei ist unterteilt in Sektionen. Jede Sektion beginnt mit einem Namen in spitzen Klammern und endet mit dem gleichen Namen angeführt von einem Schrägstrich, wiederum in spitzen Klammern.

Beispiel:

```
<General>
  Optionen
</General>
```

Jede Sektion kann eine Reihe von Konfigurationsanweisungen und gegebenenfalls weitere Sektionen enthalten. Bei Sektionsnamen und Namen von Konfigurationsanweisungen wird die Groß-/Kleinschreibung nicht berücksichtigt.

Die Konfigurationsdatei ist in die folgenden Sektionen unterteilt:

- General
- Logging
- SmtServer
- SmtRelay

- Tls
- SpamEngine
- Freezing
- UserSettings
- Snmp

Kommentare beginnen mit einem Doppelkreuz und erstrecken sich bis zum Ende der Zeile. Durch `Include`-Anweisungen können weitere Dateien in die Konfiguration eingebunden werden. Dies erlaubt, die Konfiguration in mehrere, einzeln editierbare Dateien aufzuteilen. Jede `Include`-Direktive erwartet entweder einen Dateinamen, zum Einbinden einer einzelnen Datei, oder ein *glob*-kompatibles Suchmuster um mehrere Dateien einzufügen. `Include`-Anweisungen können nur außerhalb von Sektionen verwendet werden. Die eingebundenen Dateien müssen wiederum der vollständigen Konfigurationssyntax entsprechen, das heißt, dass sie mindestens eine der oben genannten Sektionen definieren müssen.

Beispiel: (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>
```

Es ist durchaus möglich (und im Zusammenspiel mit der `Include`-Anweisung auch sinnvoll), dass Sektionen mehrfach definiert werden. Damit können einzelne Aspekte einer Sektion (z.B. die Empfänger-spezifischen Ausnahmen in den `UserSettings`) separat behandelt werden, ohne dass ein Konflikt bei der Definition von Sektionen entsteht.

Einzelne Optionen können ebenfalls mehrfach verwendet werden. Hierbei gilt: Kann eine Option nur einmal gesetzt werden (wie z.B. `WorkingDirectory`), so überschreibt die letzte Definition alle vorhergehenden. Kann eine Option mehrfach angegeben werden (wie z.B. `Server` in der Sektion `SpamEngine`), dann ist das Ergebnis die Summe aller Definitionen.

In den folgenden Abschnitten werden einige Optionen erwähnt, die einen Parameter vom Typ `bool` erwarten. Hier können folgende Werte verwendet werden:

- Yes, On, True oder 1 zum Aktivieren
- No, Off, False oder 0 zum Deaktivieren

Die verschiedenen Schreibweisen sind austauschbar und können nach Belieben verwendet werden. Um die Gleichwertigkeit zu demonstrieren, werden in den folgenden Beispielen ganz bewusst unterschiedliche Formen verwendet.

3.2.1. Allgemeine Einstellungen

Allgemeine Einstellungen des eXpurgate Dienstes werden in der Sektion `General` vorgenommen.

WorkingDirectory

Angabe eines Arbeitsverzeichnisses zum temporären Speichern von E-Mails und anderen Arbeitsdaten.

Syntax: `WorkingDirectory path`
Beispiel: `WorkingDirectory "/var/spool/expurgate"`
Default: `leer`

LicenseFile

Angabe der eXpurgate Lizenzdatei.

Syntax: `LicenseFile path`
Beispiel: `LicenseFile "/etc/expurgate/client.key"`
Default: `leer`

Sublicense

Angabe des eXpurgate Sublizenz-Keys

Syntax: `Sublicense string`
Beispiel: `Sublicense "abc-123"`
Default: `leer`

SublicenseFile

Angabe der eXpurgate Sublizenz-Datei.

Syntax: `SublicenseFile path`
Beispiel: `SublicenseFile "/etc/expurgate/client.subkey"`
Default: `leer`

Anmerkung: Die Optionen `Sublicense` und `SublicenseFile` sind als alternative Möglichkeiten zur Sublizenz-Angabe zu betrachten. Werden beide angegeben, dann überschreibt die zweite Option immer die erste.

Daemonize

Angabe, ob eXpurgate SMTP in den Hintergrund wechseln soll.

Syntax: `Daemonize bool`

Beispiel: `Daemonize Yes`

Default: `No`

UserId

Angabe einer User- sowie optional einer Gruppen-ID, unter der eXpurgate SMTP laufen soll. Diese Option kann verwendet werden, falls eXpurgate SMTP unter einer nicht-privilegierten User-ID laufen soll, aber unter der root-User-ID gestartet werden muss (um z.B. den eingehenden Port auf '25' setzen zu können).

Syntax: `UserId user[:group]`

Beispiel: `UserId mail:mail`

Default: `leer`

ChangeRoot

Angabe eines neuen root-Verzeichnisses in das eXpurgate SMTP nach dem Start wechseln soll.

Syntax: `ChangeRoot path`

Beispiel: `ChangeRoot "/opt/expurgate"`

Default: `leer`

PidFile

Angabe einer Datei, in die eXpurgate SMTP seine PID (Prozess-ID) schreiben soll.

Syntax: `PidFile path`

Beispiel: `PidFile "/var/run/expurgate.pid"`

Default: `leer`

Beispiel:

```
<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

Alle Einstellungen zum Logging werden in der Sektion `Logging` vorgenommen. Diese Sektion ermöglicht es, Log-Meldungen anhand ihrer Wichtigkeit auf verschiedene Log-Ziele zu verteilen.

Die Definition der Wichtigkeitsstufen (Loglevel), die auf einem Ziel ausgegeben werden, erfolgt durch die Angabe der niedrigsten und höchsten Wichtigkeitsstufe: `ERROR-EMERGENCY` beinhaltet alle Wichtigkeitsstufen von `ERROR` bis `EMERGENCY`. Untergrenze oder Obergrenze können entfallen, wenn es sich um die niedrigste bzw. höchste Wichtigkeitsstufe handelt. So meint `-NOTICE` alle Wichtigkeitsstufen von `DEBUG` bis einschließlich `NOTICE`, während `ERROR` alle Meldungen mit der Stufe `ERROR` oder höher bedeutet.

Im Folgenden sind die Wichtigkeitsstufen von Log-Meldungen aufgelistet.

DEBUG Interne Log-Meldung mit niedriger Priorität.

INFO Information zur normalen Funktionsweise.

NOTICE Meldung zu besonderen Ereignissen.

WARNING Warnung bei ungewöhnlichen Ereignissen.

ERROR Meldung zu nicht-kritischen Fehlermeldungen.

CRITICAL Meldung zu kritischen Fehlerzuständen.

ALERT Der Fehlerzustand erfordert einen sofortigen Eingriff.

EMERGENCY Das System ist nicht mehr funktionsfähig.

Als Voreinstellung sind alle Logs deaktiviert.

DefaultTimestamp

Legt das Standard-Zeitstempel-Format in `strftime()`-kompatibler Notation fest.

Syntax: `DefaultTimestamp format`

Beispiel: `DefaultTimestamp "%Y-%m-%d %H:%M:%S"`

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

FileLog

Schreibe alle Meldungen der angegebenen Loglevel in die spezifizierte Datei. Der Dateiname kann `strftime`-kompatible Formatierungen enthalten, die beim Schreiben einer Meldung durch die aktuelle Systemzeit ersetzt werden. Durch Angabe eines `strftime`-kompatibel formatierten Zeitstempels kann das Standard-Zeitstempel-Format für dieses Logziel überschrieben werden.

Wenn die Datei nicht existiert, wird sie angelegt, sobald die erste Meldung geschrieben wird. Dies gilt auch für alle übergeordneten Verzeichnisse. Existiert die Datei so werden neue Meldungen an deren Ende angehängt. Die Datei muss für den Benutzer, unter dem `eXpurgate SMTP` läuft, schreibbar sein.

Syntax: `FileLog loglevel path [timestamp timestamp]`

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

ErrorLog

Schreibe alle Meldungen der angegebenen Loglevel auf die Standard-Fehlerausgabe. Durch Angabe eines strftime-kompatibel formatierten Zeitstempels kann das Standard-Zeitstempel-Format für dieses Logziel überschrieben werden.

Syntax: ErrorLog *loglevel* [timestamp *timestamp*]

Beispiel: ErrorLog -ERROR timestamp "%c"

SysLog

Protokolliere alle Meldungen der angegebenen Loglevel über den Systemlogger. Diese Option ist nur auf Unix-Betriebssystemen verfügbar.

Das facility-Feld kann einen der folgenden Werte annehmen:

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

Syntax: SysLog *loglevel facility*

Beispiel: SysLog WARNING-EMERGENCY MAIL

ConsoleLog

Schreibe alle Meldungen der angegebenen Loglevel auf die Systemkonsole. Durch Angabe eines strftime-kompatibel formatierten Zeitstempels kann das Standard-Zeitstempel-Format für dieses Logziel überschrieben werden. Diese Option ist nur auf Unix-Systemen verfügbar.

Syntax: ConsoleLog *loglevel* [timestamp *timestamp*]

Beispiel: ConsoleLog EMERGENCY

EventLog

Protokolliere alle Nachrichten der angegebenen Loglevel über das Event-Log. Diese Option ist nur auf Windows-Systemen verfügbar.

Syntax: EventLog *loglevel*

Beispiel: EventLog ERROR-EMERGENCY

Beispiel:

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

Formatierte Log-Meldungen

In der Untersektion Messages können einzelne Meldungen verändert oder deaktiviert werden. Dazu kann jedem Log-Ereignis ein Format-String mit verschiedenen Variablen zugeordnet werden. Variablen werden vor der Ausgabe einer Log-Meldung durch konkrete Werte ersetzt. Leere Log-Meldungen werden unterdrückt.

Variablen werden innerhalb der Log-Meldungen über einen Namen, eingefasst in runden Klammern und von einem Prozent-Zeichen angeführt, referenziert.

Beispiel:

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

Jede Zeile innerhalb der Messages-Sektion besteht aus dem Namen einer Log-Meldung und dem zu verwendenden Format-String.

```
event string
```

Alle modifizierbaren Log-Meldungen werden mit der Wichtigkeit NOTICE ausgegeben. In diesem Level wird keine Meldung ausgegeben, die nicht modifizierbar ist. Eine Auflistung aller modifizierbaren Log-Meldungen finden Sie im Kapitel A.5 Log-Meldungen in dieser Dokumentation.

Beispiel:

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

3.2.3. SMTP-Server

In der Sektion `SmtPserver` können Einstellungen für das SMTP-Server-Interface von eXpurgate vorgenommen werden.

ListenAddress

Gibt Netzwerk-Adresse und Port für die SMTP-Schnittstelle an. Diese Option kann mehrfach verwendet werden, um gleichzeitig auf mehreren Netzwerk-Adressen SMTP-Daten zu empfangen.

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

HeloHostname

Gibt den Hostnamen in BANNER und HELO/EHLO-Antwort an.

Syntax: `HeloHostname domain`
Beispiel: `HeloHostname mail.example.com`
Default: `localhost`

ReceivedHeader

Definiert das Format des von eXpurgate eingefügten Received-Headers.

Syntax: `ReceivedHeader string`
Beispiel: `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

Aktiviert oder deaktiviert unterstützte SMTP-Protokoll-Erweiterungen. Unterstützte Erweiterungen sind VRFY, 8BITMIME, XCLIENT, XFORWARD, AUTH, PIPELINING und DSN. Wird eine Extension nicht explizit aktiviert, ist sie per Voreinstellung ausgeschaltet.

Syntax: `Extension identifier bool`
Beispiel: `Extension 8BITMIME On`

Anmerkung: Ist die Erweiterung PIPELINING ausgeschaltet, beendet eXpurgate die Verbindung zu Clients, die sich nicht gemäß dem Protokoll verhalten und trotzdem Pipelining benutzen.

Anmerkung: Die DSN-Extension wird von eXpurgate nicht behandelt und lediglich an den nachgelagerten Server weitergereicht. Von eXpurgate werden keine Benachrichtigungen über den Zustellstatus versandt.

Weitere Informationen zur Konfiguration von SMTP-AUTH finden Sie im Abschnitt 3.2.3.6.

TlsOnConnect

Aktiviert oder deaktiviert TLS für eingehende Verbindungen sobald ein SMTP-Client versucht eine Verbindung zum SMTP-Server aufzubauen.

Syntax: TlsOnConnect *bool*

Beispiel: TlsOnConnect Yes

Default: No

MailBufferSize

Definiert die Größe, bis zu der E-Mails im Speicher gehalten werden. E-Mails, die kleiner als die angegebene Größe sind, werden nach Möglichkeit direkt im Speicher verarbeitet, ohne sie im Spool-Verzeichnis abzulegen.

Syntax: MailBufferSize *number*

Beispiel: MailBufferSize 0

Default: 8192

ValidateAddresses

Definiert, ob Absender- und Empfänger-Adressen bereits vor der Einlieferung der E-Mail durch den Relay-Server validiert werden.

Syntax: ValidateAddresses *bool*

Beispiel: ValidateAddresses Yes

Default: No

AllowRelayAddresses

Definiert, ob typische Relay-Adressen akzeptiert werden.

Als Relay-Adressen gelten

- Adressen, die eine vollständige E-Mail-Adresse als Localpart enthalten (bspw. "john@example.com"@company.com)
- Adressen, die ein Prozent-Zeichen und eine Domain im Localpart enthalten (bspw. john%example.com@company.com)
- Adressen, die ein oder mehr Ausrufezeichen enthalten (bspw. example.com!john@company.com)

Syntax: AllowRelayAddresses *bool*

Beispiel: AllowRelayAddresses No

Default: No

MaxConnections

Gibt die maximale Anzahl an offenen Verbindungen an.

Syntax: MaxConnections *number*

Beispiel: MaxConnections 5000

Default: 0 (*unlimitiert*)

MaxInvalidCommands

Gibt die maximale Anzahl unbekannter Befehle oder syntaktischer Fehler in einer SMTP-Verbindung an. Wird hier eine 0 eingegeben, ist die Anzahl der Fehler nicht limitiert.

Syntax: MaxInvalidCommands *number*

Beispiel: MaxInvalidCommands 5

Default: 5

MaxRecipients

Gibt die maximale Anzahl an Empfängern einer E-Mail an. Wird hier eine 0 eingetragen, ist die Anzahl der Empfänger unlimitiert.

Syntax: MaxRecipients *number*

Beispiel: MaxRecipients 100

Default: 100

MaxMailSize

Gibt die maximale Größe einer E-Mail an. Auch hier kann eine 0 angegeben werden, um die Limitierung der E-Mail-Größe aufzuheben.

Syntax: MaxMailSize *number*
Beispiel: MaxMailSize 10000000
Default: 262144000 (250MB)

ConnectionTimeout

Gibt die maximale Dauer einer Verbindung an (0 deaktiviert den Timeout).

Syntax: ConnectionTimeout *seconds*
Beispiel: ConnectionTimeout 3600
Default: 3600

DataTimeout

Gibt die maximale Zeit zwischen zwei Kommandos an (0 deaktiviert auch diesen Timeout).

Syntax: DataTimeout *seconds*
Beispiel: DataTimeout 60
Default: 300

AddStandardHeaders

Ist die Option aktiviert, fügt eXpurgate Standard-Header zu E-Mails hinzu falls diese in der E-Mail fehlen. Alle E-Mails entsprechen dann den Anforderungen von *RFC 5322*.

Syntax: AddStandardHeaders *bool*
Beispiel: AddStandardHeaders yes
Default: No

Beispiel:

```
<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. Lokale Domains

In der Sektion `LocalDomains` kann eine Liste von Domains angegeben werden, die eXpurgate als lokal betrachtet. E-Mails an lokale Domains werden immer angenommen. E-Mails an nicht-lokale Domains werden nur angenommen, wenn für den versendenden Server Relaying erlaubt ist. Lesen Sie sich bitte dafür den nächsten Abschnitt durch.

Für jede `LocalDomains`-Sektion kann angegeben werden wie mit Subdomains umgegangen werden soll. Dafür gibt es die Option `UseWildCards`. Ist diese Option nicht vorhanden oder auf `off` gesetzt, gilt ein Eintrag sowohl für die Domain selber als auch für Subdomains dieser Domain. Wenn `UseWildCards` auf `on` gesetzt wird, lässt sich unterscheiden, ob ein Eintrag auch für Subdomains gilt oder nicht. Der Eintrag `example.com` gilt ausschließlich für E-Mails von dieser Domain und nicht für Subdomains. Ausschließlich für Subdomains aber nicht für E-Mails von der Domain selber gilt der Eintrag `*.example.com`. Wenn sowohl E-Mails von der eingetragenen Domain als auch von deren Subdomains als lokal betrachtet werden sollen heißt der Eintrag `*example.com`.

Ist die Sektion `LocalDomains` leer oder nicht vorhanden, so gelten alle Domains als lokal.

Achtung: Bei unbedachter Konfiguration kann leicht ein Open-Relay konfiguriert werden.

Beispiel:

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

3.2.3.2. Zugriffskontrolle

In der Sektion `Permissions` können Berechtigungen für einliefernde Server festgelegt werden. Diese Sektion besteht aus einer Reihe von Untersektionen für verschiedene Berechtigungen. Jede Untersektion besteht aus einer Liste von `Allow`- oder `Deny`-Anweisungen mit einer Netzmaske.

```
Allow netmask
Deny netmask
```

Die Sektion `Connect` regelt, welche Server E-Mails einliefern dürfen. Ist diese Sektion leer oder nicht vorhanden, so werden alle Server akzeptiert.

Die Sektion `Relay` regelt, welche Server E-Mails an nicht-lokale Domains einliefern dürfen. Ist diese Sektion leer oder nicht vorhanden, so werden alle Server abgelehnt.

Die Sektionen `XClient` und `XForward` regeln, welche Server die `XCLIENT`- bzw. `XFORWARD`-Befehle verwenden dürfen. Sind diese Sektionen leer oder nicht vorhanden, so werden alle Server abgelehnt.

Bitte beachten Sie, dass die einzelnen Abschnitte Connect, Relay, XClient und XForward separat betrachtet werden. Wenn Sie z.B. einem Netzsegment Relay-Rechte einräumen möchten, müssen Sie sicherstellen, dass es auch Connect-Rechte besitzt. Ist das nicht der Fall, kommt das Programm gar nicht erst bis zur Überprüfung der Relay-Rechte.

Beispiel:

```
<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. Abfrage von DNS-Blacklists

eXpurgate kann eine oder mehrere DNS-Blacklists nach der IP-Adresse des einliefernden Rechners abfragen und ggf. die Verbindung von diesem Rechner ablehnen. Verschiedene Blacklists und deren Ergebnisse können dabei unterschiedlich gewichtet werden. Erlangt die IP-Adresse einen konfigurierbaren Score-Wert, beendet eXpurgate die Verbindung zu dem Rechner.

Die einfachste Konfiguration einer DNS-Blacklist geschieht wie folgt:

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

In diesem Fall beendet eXpurgate die Verbindung, sobald die IP-Adresse des Clients in der Liste vorhanden ist.

Die Wirkung eines Blacklist-Eintrags kann auf bestimmte Antworten der Blacklist begrenzt werden. Dazu wird mit dem Reject-Schlüsselwort eine IP-Adresse oder ein Bereich von IP-Adressen angegeben.

Sollen die Ergebnisse mehrerer Blacklists unterschiedlich gewichtet werden, ist jedem Blacklist-Eintrag ein Score-Wert zuzuweisen. Die Verbindung wird abgelehnt, wenn der erreichte Score-Wert die Größe von RejectScore erreicht.

```
<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 diesem Beispiel wird die Verbindung abgelehnt, wenn die Client-IP-Adresse entweder auf der Liste `example1-dnsbl.net` oder auf den beiden Listen `example2-dnsbl.net` und `example3-dnsbl.net` vorhanden ist.

3.2.3.4. Bounce Address Tag Validation (BATV)

eXpurgate bietet die Möglichkeit eingehende Bounce-Mails zu überprüfen, ob sie durch E-Mails aus dem lokalen Mailsystem ausgelöst wurden. Dazu muss vorher das lokale Mailsystem die Envelope-Absender-Adresse der E-Mail mit einem BATV-Tag signieren, das später ebenfalls in der Bounce-Mail enthalten ist. Für die Überprüfung verarbeitet eXpurgate den BATV-Tag der Bounce-Mail und erkennt, ob es sich um eine Bounce-Mail handelt, die durch eine E-Mail des lokalen Mailsystems ausgelöst wurde. Wird eine Bounce-Mail erkannt, die nicht durch eine E-Mail aus dem lokalen Mailsystem ausgelöst wurde, wird die Bounce-Mail von eXpurgate abgewiesen.

Voraussetzung für die Erkennung von Bounce-Mails ist, dass das lokale Mailsystem für die Erstellung der Signatur die *Simple Private Signature (prvs)* verwendet, da nur diese durch eXpurgate unterstützt wird.

Um die Überprüfung auf gültige Bounce-Mails in eXpurgate zu aktivieren, muss innerhalb der Batv-Sektion der Parameter `Enable` eingeschaltet werden. Zusätzlich ist es notwendig, dass hinter dem Parameter `Key` der Schlüssel angegeben wird, den das lokale Mailsystem für die Generierung der BATV-Tags verwendet. Gibt es verschiedene Schlüssel, können diese durch Hinzufügen mehrerer Zeilen eingetragen werden.

Mit dem Parameter `BounceSender` werden zusätzliche Localparts von Sendern angegeben für deren E-Mails eine BATV-Überprüfung durchgeführt werden soll. Wird kein zusätzlicher `BounceSender` angegeben, führt eXpurgate die Überprüfung nur für E-Mails ohne Absender-Adresse durch. Der Parameter kann mehrfach verwendet werden.

Durch den Parameter `Domain` kann die Überprüfung von Bounce-Mails auf bestimmte Empfänger-Domains eingeschränkt werden. Wird der Parameter `Domain` nicht verwendet, wird BATV für alle Empfänger aktiviert. Zusätzlich können hinter den Domains die Werte `Optional` oder `Enforced` gesetzt werden. `Optional` bedeutet, dass Bounce-Mails für diese Empfängerdomain keinen BATV-Tag besitzen müssen, um von eXpurgate angenommen und verarbeitet zu werden. Der Wert `Enforced` bedeutet, dass jede Bounce-Mail für diese Empfängerdomain einen BATV-Tag besitzen muss. Ist hinter `Domain` kein Wert gesetzt, dann wird standardmäßig der Wert `Enforced` benutzt.

Sollen Bounce-Mails ohne BATV-Tag für bestimmte Empfänger oder Clients von der BATV-Überprüfung ausgenommen werden, können diese innerhalb der `Exceptions`-Untersektion angegeben werden. Für jeden Empfänger wird dazu hinter dem Parameter `Recipient` die E-Mail-Adresse angegeben. Alternativ können mehrere Empfänger innerhalb der `Recipients`-Sektion definiert werden. Für jeden Client wird hinter dem Parameter `ClientIp` das Netzwerk festgelegt. Sind mehrere Clients vorhanden können sie innerhalb der `ClientIps`-Sektion angegeben werden.

Besitzt eine E-Mail einen ungültigen BATV-Tag und soll sie erst beim Empfangen von DATA durch eXpurgate zurückgewiesen werden, muss der Parameter DelayReject eingeschaltet werden.

Beispiel:

```
<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>
```

Die Domain-Einträge im obigen Beispiel haben folgende Bedeutung: Der Eintrag `example.com` aktiviert die Überprüfung von Bounce-Mails für diese Domain, nicht aber für ihre Subdomains. Die Überprüfung ausschließlich für die Subdomains nicht aber für die Domain selber erfolgt durch den Eintrag `*.example.de`. Der Eintrag `*example.net` schaltet die Überprüfung von Bounce-Mails für die eingetragene Domain und deren Subdomains ein. Für die Domain `example.de` ist zusätzlich der Wert `Optional` gesetzt, damit Bounce-Mails an dieser Empfängerdomains ohne BATV-Tag angenommen werden. Bounce-Mails für die Empfänger `foobar@example.com`, `john@example.com`, `jane@example.com` und Bounce-Mails von den Clients `172.16.0.0/12`, `10.0.0.0/8`, `192.168.0.1/32` benötigen keinen BATV-Tag. Sie werden durch die BATV-Überprüfung von eXpurgate akzeptiert.

3.2.3.5. Sender Policy Framework (SPF)

eXpurgate bietet die Möglichkeit eingehende E-Mails mit Hilfe der SPF-Technik zu überprüfen. Dafür kontrolliert eXpurgate die HELO- und MAIL FROM-Identität des SMTP-Clients, indem eine SPF-Regel vom entsprechenden DNS abgefragt wird. Mit Hilfe dieser Regel stellt eXpurgate anschließend fest, ob der SMTP-Client autorisiert ist, diese Domain als Absender zu verwenden. Falls nicht, wird die E-Mail abgewiesen.

In der aktuellen Version fordert eXpurgate nur TXT-Records vom DNS an, um die SPF-Regeln zu erhalten. Falls kein TXT-Record gefunden werden konnte, wird die SPF-Überprüfung für diese E-Mail nicht durchgeführt.

Zur Aktivierung der SPF-Überprüfung muss innerhalb der Spf-Sektion der Parameter `Enable` eingeschaltet werden. Es besteht die Möglichkeit die HELO-Prüfung ein- bzw. auszuschalten. Dazu müssen Sie den Parameter `HeloCheck` setzen. Für die Domain des MAIL FROM wird die SPF-Prüfung immer durchgeführt.

Mit `HostDomain` kann die vollständige Domain Ihres Hosts angegeben werden. Er wird ggf. für die Generierung von SMTP-Antworten benötigt. Standardmäßig wird hier der `HeloHostname` aus der `SmtPServer`-Sektion verwendet.

Ist es erforderlich, dass einzelne E-Mail-Clients von der SPF-Überprüfung ausgenommen werden, können Sie diese innerhalb der `NoCheck`-Untersektion angeben.

Beispiel:

```
<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. Authentifizierung via SMTP AUTH

Einliefernde Clients können über die *SMTP AUTH* Protokollerweiterung (RFC 4954) authentifiziert werden. Die Authentifizierung erfolgt durch den nachgelagerten E-Mail-Server mittels des PLAIN-Mechanismus (RFC 4616). Hierzu muss die Protokollerweiterung durch die `Extension`-Direktive eingeschaltet werden. In der Sektion `Authentication` können dann nähere Einstellungen für die Authentifizierung vorgenommen werden.

Beispiel:

```
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>
```

Die `Disabled`-, `Optional`- und `Enforced`-Anweisungen werden jeweils von einer Netzmaske gefolgt. Die `Optional`-Anweisung ist die Standardeinstellung: Hierdurch wird die Authentifizierung für das angegebene Netzsegment angeboten, aber nicht erzwungen. Durch `Disabled` wird die Authentifizierung für das angegebene Netzsegment abgeschaltet. Durch `Enforced` werden alle SMTP-Befehle außer HELO, EHLO, NOOP, RSET, STARTTLS und AUTH abgelehnt, bis der Client erfolgreich authentifiziert ist. Die `Disabled`-, `Optional`- und `Enforced`-Anweisungen können mehrfach verwendet werden.

Die `RequireTls` Anweisung regelt, dass keine Authentifizierung angeboten wird, bis die Verbindung über TLS gesichert ist.

3.2.3.7. SMTP-Protokoll-Meldungen

Alle Antworten des SMTP-Servers können frei konfiguriert werden. Dazu muss, ähnlich der Log-Meldungen, eine Sektion `Messages` angelegt werden, in der jeder SMTP-Antwort ein Format-String zugewiesen wird. Eine Auflistung aller SMTP-Protokoll-Meldungen finden Sie in Kapitel A.6 in dieser Dokumentation.

Beispiel:

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

3.2.4. SMTP-Relay

eXpurgate versucht für die Auslieferung verarbeiteter E-Mails an seine Relay-Server, Verbindungen dauerhaft zu nutzen. Dabei ist es auch möglich, mehrere Relay-Server anzugeben und diese zu priorisieren.

Zur Konfiguration werden zusammengehörige Server zu einem sogenannten Pool zusammengefasst. Jeder Pool wird durch eine `Pool` Untersektion definiert. Alle in einem Pool zusammengefassten Relay-Server gelten, von ihrer Priorität abgesehen, als gleichbedeutend und verwenden die gleichen Einstellungen.

Welcher der definierten Pools zum Versenden einer E-Mail verwendet wird, kann über die Sektion `UserSettings` festgelegt werden. Siehe dazu auch Abschnitt 4.

Es existiert immer mindestens ein Pool, der sogenannte Default-Pool. Dieser Pool wird immer dann verwendet, wenn nicht explizit ein anderer Pool für den Versand spezifiziert wurde.

AutoXforward

Legt fest, ob eXpurgate die IP-Adresse des einliefernden Clients per `XFORWARD`-Kommando an den Relay-Server weiterleitet.

Diese Option kann nur global definiert werden und ist nicht pro Pool einstellbar.

Syntax: `AutoXforward bool`
Beispiel: `AutoXforward On`
Default: `Off`

AutoXclient

Legt fest, ob eXpurgate die Attribute des einliefernden Clients per `XCLIENT`-Kommando an den Relay-Server weiterleitet.

Diese Option kann nur global definiert werden und ist nicht pro Pool einstellbar.

Syntax: `AutoXclient bool`
Beispiel: `AutoXclient On`
Default: `Off`

Name

Legt den Namen fest, über den ein Pool ausgewählt werden kann. Diese Direktive kann nur innerhalb der Pool-Untersektion verwendet werden. Bitte beachten Sie hierbei, dass der Name "Quarantine" eine besondere Bedeutung hat und für E-Mails verwendet wird, die in die Quarantäne geschickt werden sollen.

Syntax: Name *identifizier*

Beispiel: Name "VIP-Customers"

Default: *leer*

MaxPoolSize

Gibt die maximale Anzahl an gleichzeitig offenen Verbindungen in diesem Pool an.

Syntax: MaxPoolSize *number*

Beispiel: MaxPoolSize 50

Default: 0 (*unlimitiert*)

DataTimeout

Gibt die maximale Zeit zwischen zwei Kommandos bzw. zwischen zwei Datenblöcken an. Null (0) deaktiviert den Timeout.

Syntax: DataTimeout *number*

Beispiel: DataTimeout 60

Default: 600

MaxMailsPerConnection

Gibt an, wie viele E-Mails maximal über eine Verbindung verschickt werden dürfen, bevor diese Verbindung geschlossen wird (0 = unlimitiert).

Syntax: MaxMailPerConnection *number*

Beispiel: MaxMailsPerConnection 50

Default: 50

Helo

Gibt den im HELO/EHLO verwendeten Domain-Namen an. Der Wert Passthrough sorgt dafür, dass der bei der Einlieferung der E-Mail verwendete Domain-Name verwendet wird.

Syntax: Helo *domain*

Beispiel: Helo example.com

Default: *HeloHostname aus SmtServer*

Achtung: Die Benutzung von Passthrough führt dazu, dass eXpurgate auf einer ausgehenden Verbindung mehrfach HELO/EHLO sendet. Dies kann in Verbindung mit einigen Mail-Servern, zum Beispiel Sendmail, zu Problemen führen.

Server

Gibt einen SMTP-Relay-Server für diesen Pool an.

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

Beispiel: `Server 127.0.0.1:25`

Default: `leer`

AsciiConversion

Ist der Wert auf `yes` gesetzt, konvertiert eXpurgate den Mail-Body nach *US-ASCII*, falls der Empfänger die *8BITMIME*-Erweiterung nicht unterstützt. Ist die Option ausgeschaltet, sendet eXpurgate alle E-Mails ohne Konvertierung an den Relay-Server. Wenn der Relay-Server *8BITMIME* nicht unterstützt werden in diesem Fall nicht-*US-ASCII* Zeichen bei der Übertragung zerstört.

Syntax: `AsciiConversion bool`

Beispiel: `AsciiConversion yes`

Default: `No`

Encryption

Legt fest, ob eine TLS-Verschlüsselung für ausgehende Verbindungen optional oder notwendig ist oder ob der *common-name* (CN) verifiziert wird. Auf das Schlüsselwort `Verified` kann eine Zeichenkette folgen. In diesem Fall vergleicht eXpurgate die Zeichenkette mit dem *common-name* des Relay-Zertifikats.

Ist keine Zeichenkette vorhanden, führt eXpurgate ein *reverse-DNS-lookup* auf der IP-Adresse des Relay-Servers aus. Der resultierende Hostname wird dann mit dem *common-name* des Relay-Zertifikats verglichen.

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

Beispiel: `Encryption Verified`

Default: `Optional`

TrustedCertificate

Definiert die enthaltenen Zertifikate für ausgehende Verbindungen als vertrauenswürdig.

Syntax: `TrustedCertificate path`

Beispiel: `TrustedCertificate "/etc/ssl/ca.cert"`

Default: `leer`

TrustedCertificateDirectory

Definiert alle Zertifikate in einem Verzeichnis für ausgehende Verbindungen als vertrauenswürdig. Die Zertifikatsdateien müssen nach dem Hash des enthaltenen Zertifikats benannt sein.

Syntax: TrustedCertificateDirectory *path*

Beispiel: TrustedCertificateDirectory "/etc/ssl/certs"

Default: *leer*

Beispiel:

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

Anmerkung: Sie können die Standardeinstellungen für das SMTP-Relay konfigurieren, indem Sie die oben beschriebenen Werte direkt innerhalb der Sektion `SmtpRelay` definieren (siehe Beispielkonfiguration am Ende dieser Anleitung). Alternativ können Sie einen Pool definieren, der das spezielle Schlüsselwort `Default` gesetzt hat (wie im Beispiel gezeigt). Die Wirkung ist in beiden Fällen gleich.

3.2.5. TLS

Die eXpurgate Software erlaubt den Empfang und Versand von E-Mails über TLS-verschlüsselte Verbindungen. Neben der Verschlüsselung der Kommunikation ist es auch möglich, die Authentizität des jeweiligen Kommunikationspartners zu verifizieren.

Für den verschlüsselten Empfang wird ein privater Schlüssel und ein Zertifikat nach X.509 benötigt. eXpurgate kann mit self-signed Zertifikaten und Zertifikaten von einer Certificate Authority umgehen.

Für den verschlüsselten Versand werden weder Zertifikat noch Schlüssel benötigt. Ist ein Zertifikat vorhanden, wird dieses auch beim Versand zur Identifikation verwendet. Zertifikate und Schlüssel können im DER- oder PEM-Format vorliegen. Das PEM-Format erlaubt Schlüssel und Zertifikat in der gleichen Datei zu speichern sowie eine Zertifikatskette zu definieren.

Alle Optionen, die den verschlüsselten Empfang betreffen, werden in der Sektion `Tls` konfiguriert. Optionen zum verschlüsselten Senden von E-Mails finden Sie in der Sektion `SmtpRelay` (Abschnitt 3.2.4).

Certificate

Gibt die Zertifikatsdatei an.

Syntax: Certificate *path*

Beispiel: Certificate "/etc/expurgate/server.crt"

Default: *leer*

PrivateKey

Gibt den privaten Schlüssel an.

Syntax: PrivateKey *path*

Beispiel: PrivateKey "/etc/expurgate/server.key"

Default: *leer*

TrustedCertificate

Definiert die enthaltenen Zertifikate als vertrauenswürdig.

Syntax: TrustedCertificate *path*

Beispiel: TrustedCertificate "/etc/ssl/ca.cert"

Default: *leer*

TrustedCertificateDirectory

Definiert alle Zertifikate in einem Verzeichnis als vertrauenswürdig. Die Zertifikatsdateien müssen nach dem Hash des enthaltenen Zertifikats benannt sein.

Syntax: TrustedCertificateDirectory *path*

Beispiel: TrustedCertificateDirectory "/etc/ssl/certs"

Default: *leer*

Anmerkung: Sind Zertifikat und Private Key in derselben Datei gespeichert, so müssen trotzdem beide Optionen, Certificate und PrivateKey, angegeben werden.

Anmerkung: Die Direktiven TrustedCertificate und TrustedCertificateDirectory sind ebenfalls in der Untersektion Policy anwendbar.

Alle weiteren TLS-Einstellungen können in Abhängigkeit von Empfänger- und Absender-Domain einer E-Mail, sowie der IP-Adresse des einliefernden Rechners konfiguriert werden. Dies erfolgt in der Policy-Untersektion.

Untersektion Policy

Eine Policy-Sektion kann sich entweder auf eine oder mehrere Ziel-Domains beziehen oder als Standard für alle nicht explizit genannten Domains gelten.

Default

Legt die Sektion als Standard-Policy fest. Das heißt, diese gilt für alle nicht explizit genannten Empfänger-Domains.

Domain

Legt die Sektion als Policy für eine spezielle Empfänger-Domain fest.

Syntax: Domain *domain*

Beispiel: Domain example.com

Verfeinerung der Regeln und Validierung

Innerhalb einer Policy-Sektion können individuelle Verschlüsselungs- und Authentifizierungs-Regeln in Abhängigkeit der Absender-Domain oder der IP-Adresse des einliefernden Rechners festgelegt werden. Dies geschieht über Validation-Sektionen.

Default

Legt diese Validierungsregel als Standard fest. Das heißt, sie gilt für alle eingehenden Verbindungen, die von keiner anderen Validation-Sektion erfasst wird.

Sender

Ordnet die Validierungsregel einer Absender-Domain zu.

Syntax: Sender *domain*

Beispiel: Sender random.com

ClientIp

Ordnet die Validierungsregel einer IP-Adresse oder Netzwerkadresse von einliefernden Clients zu.

Syntax: ClientIp *netmask*

Beispiel: ClientIp 192.168.0.0/24

Encryption

Legt fest, ob eine TLS-Verschlüsselung optional oder notwendig ist oder ob der *common-name* (CN) verifiziert wird. Auf das Schlüsselwort *Verified* kann eine Zeichenkette folgen. In diesem Fall vergleicht eXpurgate die Zeichenkette mit dem *common-name* des Client-Zertifikats.

Ist keine Zeichenkette vorhanden, führt eXpurgate ein *reverse-DNS-lookup* auf der IP-Adresse des einliefernden Clients aus. Der resultierende Hostname wird dann mit dem *common-name* des Client-Zertifikats verglichen.

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

Beispiel: Encryption Verified

Default: Optional

Einstellungen der Standard-Policy- und Standard-Validation-Sektion können auch außerhalb der entsprechenden Sektionen stehen.

Beispiel:

```
<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-Erkennung

In der Sektion SpamEngine werden allgemeine Einstellungen zur Spam-Erkennung und E-Mail-Kategorisierung festgelegt.

Server

Gibt einen eXpurgate Server für die Kategorisierung der E-Mails an.

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

Beispiel: Server exa.expurgate.net:55555 prio 0

Default: Alle öffentlichen eleven eXpurgate Server

SocksProxy

Gibt einen SOCKS5-Proxy für die Verbindung zu den eXpurgate Servern an. Optional können ein Benutzername und ein Passwort für den Proxy-Server angegeben werden.

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

Beispiel: SocksProxy proxy.intern:1080 user "proxyuser" password "secret"

Default: *leer*

DangerousExtensions

Legt die Liste fest, die als gefährlich eingestufte Dateieindungen enthält.

Syntax: DangerousExtensions *string*

Beispiel: DangerousExtensions "exe,com,scr,vbs"

Default: "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, vbmactros, vbs, vsw, wmd, wmz, ws, wsc, wsf, wsh, xxe"

EnableGtube

Legt fest, ob die GTUBE-Test-Signatur zu einer *spam*-Kategorisierung führt. Das Aktivieren dieser Option kann zu einer Verschlechterung der Performance führen.

Syntax: EnableGtube *bool*

Beispiel: EnableGtube Off

Default: No

Threads

Definiert, wie viele E-Mails parallel verarbeitet werden können. Ein hoher Wert kann die Performance steigern, führt aber auch zu einem gesteigerten Ressourcenverbrauch.

Syntax: Threads *number*

Beispiel: Threads 64

Default: 32

TempRejectOnError

Legt fest, ob bei einem Kommunikationsfehler mit den eXpurgate Servern die E-Mail temporär abgelehnt wird oder eine Klassifizierung als *clean* erfolgt.

Syntax: TempRejectOnError *bool*

Beispiel: TempRejectOnError On

Default: Yes

Beispiel:

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

3.2.6.1. Untersektion Antivir

In der Untersektion Antivir werden Einstellungen zum Virens Scanner *Avira AntiVir* vorgenommen.

Enable

Legt fest, ob der Virens Scanner AntiVir verwendet werden soll.

Syntax: Enable *bool*

Beispiel: Enable Yes

Default: No

Port

Gibt den Port an, über den der Virens Scanner angesprochen werden soll.

Syntax: Port *number*

Beispiel: Port 55556

Default: 55556

MaxPoolSize

Gibt die maximale Anzahl an parallelen Verbindungen zum Virens Scanner an.

Syntax: MaxPoolSize *number*

Beispiel: MaxPoolSize 20

Default: 3

Extensions

Definiert die Liste aller Dateitypen, die vom Virens Scanner untersucht werden sollen.

Syntax: Extensions *string*

Beispiel: Extensions "exe,com,cmd"

Default: "ade, adp, bas, bat, bnx, 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

Gibt die maximale Rekursionstiefe beim Scannen von Archiven bzw. verschachtelten Dateien an. Wird hier bei MaxScanDepth eine 0 angegeben, wird die Überprüfung von Archiven deaktiviert.

Syntax: MaxScanDepth *number*

Beispiel: MaxScanDepth 10

Default: 5

MaxScanSize

Gibt die maximale Größe der zu scannenden Dateien an.

Syntax: MaxScanSize *number*

Beispiel: MaxScanSize 100000000

Default: 0 (*unlimitiert*)

Beispiel:

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

3.2.6.2. Untersektion NoFilter

Mit der Untersektion NoFilter können lokale E-Mails von der Kategorisierung durch eXpurgate ausgenommen werden. Als lokal gelten E-Mails, die nur eine begrenzte Anzahl von Received-Zeilen eines definierten Formats enthalten.

Enable

Aktiviert die Ausnahme von lokalen E-Mails.

Syntax: Enable *bool*

Beispiel: Enable Yes

Default: No

Network

Definiert ein Netzwerk, dessen E-Mails von der Kategorisierung ausgenommen werden.

Syntax: Network *netmask*

Beispiel: Network 10.0.0.0/8

Default: leer

MaxReceivedHeaders

Definiert die maximale Anzahl von Received-Headern in lokalen E-Mails.

Syntax: MaxReceivedHeaders *number*

Beispiel: MaxReceivedHeaders 2

Default: 0 (*keine*)

ReceivedHeaderRegex

Definiert das Format erlaubter Received-Zeilen in Form eines Perl-kompatiblen regulären Ausdrucks.

Syntax: ReceivedHeaderRegex *pattern*

Beispiel: ReceivedHeaderRegex /from 192\.168\./

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

Beispiel:

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

3.2.7. Freezing

Mit Hilfe der Freezing-Funktionalität können E-Mails, die bereits das Massen-E-Mail-Kriterium erfüllen, aber noch nicht als Spam erkannt werden, kurzfristig aufgehalten und zu einem späteren Zeitpunkt erneut untersucht werden. Dies führt zu einer noch besseren Spam-Erkennung.

In der Freezing-Sektion werden alle Einstellung bezüglich dieser Funktionalität vorgenommen.

Enable

Legt fest, ob die Freezing-Funktionalität aktiviert werden soll.

Syntax: `Enable bool`

Beispiel: `Enable Yes`

Default: `No`

FridgeDirectory

Legt das Verzeichnis fest, in dem aufgehaltene E-Mails gespeichert werden. Dieses Verzeichnis darf nicht das Arbeitsverzeichnis sein und muss sich auf dem gleichen Speichermedium befinden, auf dem auch das Arbeitsverzeichnis liegt.

Syntax: `FridgeDirectory path`

Beispiel: `FridgeDirectory "/var/spool/expurgate-fridge"`

Default: `leer`

CheckInterval

Legt fest, in welchen Zeitabständen aufgehaltene E-Mails untersucht werden sollen.

Syntax: `CheckInterval seconds`

Beispiel: `CheckInterval 60`

Default: `30`

DayTime

Legt fest, welcher Zeitraum als Tag und welcher als Nacht gilt. Während der Tag- und Nacht-Zeiträume können unterschiedliche maximale Freezing-Zeiten gelten.

Syntax: `DayTime from to`

Beispiel: `DayTime 7:00 20:00`

Default: `7:00 2:30`

MaxFreezingTime

Legt die maximale Verzögerung einer E-Mail in Sekunden während des Tages und der Nacht fest. Der zweite Parameter ist dabei optional — wird er weggelassen, gilt über den ganzen Tag der erste Wert.

Syntax: MaxFreezingTime *day night*

Beispiel: MaxFreezingTime 300 3600

Default: 1200 7200

InvalidRecipientLimit

Legt fest, ab welcher Anzahl von ungültigen Empfängern eine E-Mail eingefroren werden soll. Der Wert 0 schaltet diese Funktionalität aus.

Syntax: InvalidRecipientLimit *number*

Beispiel: InvalidRecipientLimit 1

Default: 0

MaxThawTasks

Legt die Anzahl an Tasks fest, die für das Überprüfen eingefrorener E-Mails zuständig sind.

Syntax: MaxThawTasks *number*

Beispiel: MaxThawTasks 2

Default: 20

MaxFrozenMails

Legt die maximale Anzahl eingefrorener E-Mails fest.

Syntax: MaxFrozenMails *number*

Beispiel: MaxFrozenMails 500

Default: 10000

Beispiel:

```
<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 unterstützt das Simple Network Management Protocol (SNMP), mit dem es durch eine Netzwerk-Management-Software überwacht werden kann. Für die Überwachung müssen der Netzwerk-Management-Software die Daten bekannt sein, die von eXpurgate abgefragt werden können. Diese Informationen sind in sogenannten MIB-Dateien gespeichert, die durch die eleven GmbH bereitgestellt werden. Zu ihnen gehören die Dateien ELEVEN-MIB.mib und ELEVEN-EXPURGATE-MIB.mib, die im Ordner `/usr/share/doc/-expurgate` unter Unix bzw. `C:\Programme\eleven\eXpurgate\doc` unter Windows installiert wurden. Die MIB-Dateien benötigen die Standard-MIBs SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, SNMP-FRAMEWORK-MIB, INET-ADDRESS-MIB sowie HCNUM-TC und müssen sich daher auf Ihrem System befinden.

Aktuell wird von eXpurgate die SNMP Version 2c unterstützt.

Für die Konfiguration von SNMP steht innerhalb der Konfigurationsdatei die `Snmp`-Sektion zur Verfügung.

Enable

Legt fest, ob SNMP für eXpurgate aktiviert werden soll.

Syntax: `Enable bool`

Beispiel: `Enable Yes`

Default: `No`

ListenAddress

Gibt Netzwerk-Interface und Port für die SNMP-Schnittstelle an, über die der SNMP-Dienst erreichbar sein soll.

Syntax: `ListenAddress ip[:port]`

Beispiel: `ListenAddress 0.0.0.1:161`

Default: `0.0.0.0:161`

UseTcp

Standardmäßig benutzt eXpurgate für die Kommunikation über SNMP das User Datagram Protocol (UDP). Als Alternative können Sie sich für das Transmission Control Protocol (TCP) entscheiden. Dazu müssen sie diesen Parameter einschalten.

Syntax: `UseTcp bool`

Beispiel: `UseTcp Yes`

Default: `No`

Community

Über diesen Parameter besteht die Möglichkeit den Zugriff auf eXpurgate durch ein Passwort einzuschränken. Wichtig ist, dass der Wert für `Community` in eXpurgate und in der Netzwerk-Management-Software identisch ist, da sonst keine Daten von eXpurgate abgefragt werden können.

Syntax: `Community string`
Beispiel: `Community "public"`
Default: `leer`

Beispiel:

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

Die Daten sind in einzelnen Tabellen organisiert und können über einen MIB-Browser angesehen werden. Es werden dabei die folgenden Tabellen angezeigt:

Tabelle	Beschreibung
expurgateGlobal	Es werden allgemeine Informationen über eXpurgate bereitgestellt.
exServiceInTable	Zeigt die aktuellen Daten über den Zustand des eingehenden Netzwerkdienstes von eXpurgate an.
exServiceOutTable	Speichert die aktuellen Daten über den Zustand des ausgehenden Netzwerkdienstes von eXpurgate.
exSmtpServiceInTable	Enthält Daten über die Kommunikation via SMTP zwischen einliefernden Mail-Servern und eXpurgate.
exSmtpServiceOutTable	Enthält Daten über die Kommunikation via SMTP zwischen eXpurgate und den lokalen Mail-Servern.
exSmtpConnectionInTable	Es werden Informationen über die aktuellen SMTP-Verbindungen der einliefernden Mail-Server angezeigt.
exSmtpConnectionOutTable	Es werden Informationen über die aktuellen SMTP-Verbindungen zu den lokalen Mail-Servern bereitgestellt.
exMessageTypeInTable	Daten über die Klassifizierung von eingehenden E-Mails werden in dieser Tabelle gespeichert.
exSmtpErrorInTable	In dieser Tabelle werden Informationen gesammelt, die eine Ablehnung auf SMTP-Ebene zur Folge hatten.
expurgateFridge	Es werden Informationen über den Fridge von eXpurgate bereitgestellt.

3.2.9. Lightweight Directory Access Protocol (LDAP)

eXpurgate bietet die Möglichkeit Teile der Konfiguration per LDAPv3 von einem externen Server zu beziehen. Für die Konfiguration von LDAP steht innerhalb der Konfigurationsdatei die `Ldap`-Sektion zur Verfügung.

Zurzeit kann lediglich die Validierung von Empfängeradressen an einen LDAP-Server delegiert werden.

Enable

Legt fest, ob LDAP für eXpurgate aktiviert werden soll.

Syntax: Enable *bool*

Beispiel: Enable Yes

Default: No

Library

Gibt die Bibliothek an, die für die Kommunikation über LDAP notwendig ist. Als Wert können Sie einen Pfad zur Bibliothek oder den Namen der Bibliothek angeben. Wurde nur der Bibliotheksname benutzt, wird versucht die Datei im Dateisystem in bestimmten Verzeichnissen zu finden.

Syntax: Library *path*

Beispiel: Library "/usr/local/lib/libldap_r.so"

Default: "libldap_r.so" (*Unix*)

Default: "wldap32.dll" (*Windows*)

Server

Legt fest, mit welchem LDAP-Server eXpurgate kommunizieren soll. Diese Option kann mehrfach verwendet werden.

Syntax: Server "*uri*" [*prio number*]

Beispiel: Server "ldap://ldap-server1.here.it.is:3456" prio 0

Default: *leer*

MaxConnections

Es wird die maximale Anzahl der Verbindungen zu einem LDAP-Server festgelegt.

Syntax: MaxConnections *number*

Beispiel: MaxConnections 10

Default: 2

Bind

Die Bind-Option gibt an, wie sich eXpurgate gegenüber dem LDAP-Server authentifiziert. Es können Authentifizierungs-Methode und optional Benutzername und Passwort angegeben werden.

eXpurgate unterstützt die Authentifizierung-Methoden `basic` und `simple`, sowie die Authentifizierung über SASL. Bei der Authentifizierung mit den Methoden `basic` und `simple` ist die Angabe einer Bind DN und eines Passwortes notwendig. Abhängig vom verwendeten SASL Mechanismus ist die Angabe von Nutzernamen und Passwort bei der Authentifizierung über SASL nicht erforderlich.

Durch die Angabe einer Liste erlaubter SASL Mechanismen kann die Verwendung unerwünschter Algorithmen verhindert werden.

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

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

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

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

Default: Bind SASL

Beispiel:

```
<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. LDAP-Server-Abfragen

eXpurgate benutzt die LDAP-Anbindung, um über den Server Abfragen durchzuführen. Diese Abfragen können in der Konfigurationsdatei eingestellt werden. Für die Empfängervalidierung ist der Abfragentyp `Recipients` verfügbar.

Allgemein ist festgelegt, dass eine benutzte Abfrage eine Sektion überschreibt, die die gleiche Funktionalität erfüllt. Für die Empfängervalidierung bedeutet das z.B., dass die `Recipients`-Abfrage die `Recipients`-Untersektion in der `SmtServer`-Sektion überschreibt.

Für die Aktivierung von Abfragen steht die `Query`-Untersektion zur Verfügung.

QueryType

Gibt an, welche Abfrage an den LDAP-Server gesendet werden soll.

Syntax: QueryType *string*

Beispiel: QueryType Recipients

Default: *leer*

Search

Die Search-Option gibt an, ab welcher Position im Verzeichnisbaum nach Objekten durchsucht werden soll. Der Filter definiert dabei das Kriterium, das ein gefundenes Objekt erfüllen muss, um in die Ergebnismenge aufgenommen zu werden. Für die Empfängervalidierung steht zusätzlich der Platzhalter %(recipient) zur Verfügung, der die E-Mail-Adresse ersetzt.

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

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

Default: *leer*

Beispiel:

```
<Query>
  QueryType Recipients

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

3.2.10. eXelerate

eXpurgate kann Teile seiner Konfiguration an einen eleven eXelerate Middleware Server auslagern.

Server

Gibt die Adresse des eXelerate Servers an.

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

Beispiel: Server exelerate.example.com:11223 prio 0

Default: *leer*

DataTimeout

Gibt die maximale Zeit in Sekunden an, die auf eine Antwort des eXelerate Servers gewartet wird.

Syntax: DataTimeout *number*

Beispiel: DataTimeout 5

Default: 30

MaxConnections

Gibt die maximale Anzahl an Verbindungen zu eXelerate Servern an.

Syntax: MaxConnections *number*

Beispiel: MaxConnections 5

Default: 2

Query

Gibt an, welche Teile der Konfiguration durch eXelerate Abfragen ersetzt werden sollen.

Syntax: Query *query-type* *boolean*

Beispiel: 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>
```

Alle verfügbaren eXelerate Abfragen sind in der Datei *exelerate-expurgate.conf* definiert. Rahmen für die Implementation der eXelerate Query-Funktionen sind in der Datei *exelerate-expurgate.lua* vorgegeben. Beide Dateien befinden sich nach der Installation im Dokumentations-Verzeichnis des Paketes.

3.2.10.1. Local Domains Query

Mit der Local Domains Abfrage wird bestimmt, welche Domänen als lokal gelten. Die Abfrage ersetzt die <LocalDomains> Sektion der Konfigurations-Datei.

Query Identifier

```
Query LocalDomains On
```

Request Structure

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

domain Der Domänen-Teil einer Empfänger-E-Mail-Adresse.

Response Structure

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

islocal True falls die Domäne lokal ist.

3.2.10.2. Recipient Validation Query

Mit der Recipient Validation Abfrage wird bestimmt, ob eine Empfänger-Adresse gültig ist. Die Abfrage ersetzt die <Recipients> Sektion innerhalb der <SmtpServer> Sektion der Konfigurations-Datei.

Query Identifier

```
Query Recipients On
```

Request Structure

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

recipient Die Empfänger-Adresse.

Response Structure

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

exists True falls die Adresse gültig ist.

3.2.10.3. Blacklist Query

Mit der Blacklist Abfrage wird bestimmt, ob eine IP- oder Absender-Adresse zugelassen wird. Die Abfrage ersetzt die <Blacklists> Sektion innerhalb der <SmtServer> Sektion der Konfigurations-Datei.

Query Identifier

```
Query Blacklists On
```

Request Structure

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

client Die IP-Adresse des einliefernden Servers.

sender Die Absender-Adresse.

recipient Die Empfänger-Adresse.

Response Structure

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

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

reason Der Ablehnungsgrund. Ip falls die IP-Adresse des einliefernden Servers nicht akzeptiert wird, Email falls die Absender-Adresse nicht akzeptiert wird oder Ok falls IP- und Absender-Adresse angenommen werden.

3.2.10.4. BATV Policy Query

Mit der BATV Policy Abfrage wird bestimmt, ob eine gegebene E-Mail-Adresse mit BATV geschützt ist. Die Abfrage ersetzt Teile der <Batv> Sektion innerhalb der <SmtServer> Sektion der Konfigurations-Datei.

Query Identifier

```
Query Batv On
```

Request Structure

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

client Die IP-Adresse des einliefernden Servers.

sender Die Absender-Adresse.

recipient Die Empfänger-Adresse.

Response Structure

```
<Enum ExBatvPolicy>  
  Optional 0  
  Enforced 1  
</Enum>  
  
<Struct ExBatvPolicyResponse>  
  ExBatvPolicy policy  
</Struct>
```

policy True falls die E-Mail-Adresse mit BATV geschützt ist.

3.2.10.5. TLS Policy Query

Mit der TLS Policy Abfrage wird bestimmt, ob die SMTP-Transaktion verschlüsselt bzw. validiert erfolgen muss. Die Abfrage ersetzt die <Validation> Sektion innerhalb der <Tls> Sektion der Konfigurations-Datei.

Query Identifier

```
Query TlsPolicy On
```

Request Structure

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

client Die IP-Adresse des einliefernden Servers.

sender Die Absender-Adresse.

recipient Die Empfänger-Adresse.

Response Structure

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

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

policy Enforced falls die SMTP-Transaktion verschlüsselt erfolgen muss, Validated falls der Client ein bekanntes Zertifikat vorzeigen muss oder Optional falls die Transaktion auch unverschlüsselt erfolgen darf.

subject Der erwartete Wert des Subject-Feldes des Client-Zertifikats. Wird nur in Verbindung mit Validated als Wert für policy verwendet.

store Der Name des Zertifikatsspeichers zur Überprüfung des Client-Zertifikats. Wird nur in Verbindung mit Validated als Wert für policy verwendet.

3.2.10.6. TLS Store Query

Die TLS Store Abfrage dient dem Transfer von bekannten Zertifikaten. Die Abfrage ersetzt die TrustedCertificate und TrustedCertificateDirectory Einstellungen in der <Tls> Sektion in der Konfigurationsdatei.

Query Identifier

```
Query TlsPolicy On
```

Request Structure

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

identifier Der Name des Zertifikatsspeichers wie er im Parameter store der TLS Policy Antwort angegeben wurde.

Response Structure

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

certificates Die Liste aller bekannten Zertifikate dieses Speichers. Die Zertifikate können in jedem von OpenSSL unterstützten Format angegeben werden.

3.2.10.7. User Feature Query

Die User Feature Abfrage wird verwendet, um die E-Mail-Klassifizierung zu parametrisieren. Die Abfrage ersetzt die Feature Einstellung in der <UserSettings> Sektion in der Konfigurationsdatei.

Query Identifier

```
Query Features On
```

Request Structure

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

recipient Die Empfänger-Adresse.

Response Structure

```

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

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

```

features Die Liste der aktiven Features des Nutzers.

3.2.10.8. Mail Action Query

Die Mail Action Abfrage bestimmt, wie mit einer klassifizierten E-Mail zu verfahren ist. Die Abfrage ersetzt die <MailAction> Sektion in der <UserSettings> Sektion in der Konfigurationsdatei.

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 Die IP-Adresse des einliefernden Servers.

sender Die Absender-Adresse.

recipient Die Empfänger-Adresse.

type Die Klassifikation der E-Mail.

stage Zeigt an, ob die E-Mail eingefroren wurde.

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 Eine Liste von Aktionen.

4. Finetuning der E-Mail-Behandlung

4.1. Verarbeitungsregeln

In der Sektion `UserSettings` wird spezifiziert, wie mit eingehenden E-Mails vor und nach der Kategorisierung verfahren werden soll. Dabei wird zwischen globalen Aktionen, die für alle Empfänger einer E-Mail gelten, sowie Domain- und empfängerspezifischen Einstellungen unterschieden.

In dieser Sektion lassen sich Funktionen wie ein Filterausschluss für einzelne Domains und Empfänger konfigurieren. Ebenso ist es möglich, Black- und Whitelists für IP-Adressen von sendenden Hosts und Absendern beim Empfang einer E-Mail zu definieren.

Globale versus empfängerspezifische Einstellungen

In den `UserSettings` lassen sich Einstellungen vornehmen, die für jeden Empfänger einer E-Mail zutreffen. Daneben ist es möglich, Einstellungen nur auf Domains und Empfänger anzuwenden.

Erscheinen Anweisungen direkt unterhalb der `UserSettings`-Sektion, so gelten diese zunächst global für jeden Empfänger. Einschränkungen sind dabei durch Einbetten der Anweisungen in eine `Recipient`-Sektion möglich. Im Betrieb sucht eXpurgate zunächst nach einer möglichst genauen Übereinstimmung des Empfängers und wendet dessen Einstellungen an. Wird keine empfängerspezifische Einstellung gefunden, so werden die globalen Einstellungen herangezogen.

Beispiel:

```
<UserSettings>
  # Anweisungen gelten global
  <Recipient>
    # Anweisungen gelten nur fuer den Empfaenger
  </Recipient>
</UserSettings>
```

4.2. Empfänger definieren

Empfänger werden in `Recipient`-Sektionen definiert, in denen durch die Anweisungen `Domain`, `Domains`, `Address` sowie `Addresses` Einschränkungen vorgenommen werden können.

4.2.1. Nach Domains selektieren

Durch die Anweisung `Domain` lässt sich eine Domain festlegen, für die die nachfolgenden Einstellungen innerhalb der `Recipient`-Sektion gelten sollen.

Beispiel:

```
<Recipient>
  Domain example1.com
  Domain *example2.com
  Domain *.example3.com
  # Weitere Anweisungen fuer diese Domaenen
</Recipient>
```

Im obigen Beispiel werden mit den drei `Domain`-Anweisungen Empfänger-Domains definiert, für die bestimmte Einschränkungen gelten.

Hierbei kann auch das Zeichen `'*'` als Wildcard verwendet werden:

- `*example2.com` trifft alle Unter-Domains von `example2.com` inklusive `example2.com` selbst. So würde diese `Recipient`-Sektion auf Empfänger mit den Domains `abteilung1.example2.com` sowie `example2.com` zutreffen.
- `*.example3.com` trifft ebenfalls alle Unter-Domains, nicht jedoch die Domain `example3.com` selbst. So würden hier E-Mails an die Domain `abteilung1.example3.com` betroffen sein. E-Mails an `example3.com` hingegen nicht. Sollen viele Domains angegeben werden, bietet sich als verkürzte Schreibweise die Verwendung einer eigenen `Domains`-Sektion an.

Beispiel:

```
<Recipient>
  <Domains>
    example1.com
    *example2.com
    *.example3.com
  </Domains>
  # Weitere Anweisungen fuer diese Domaenen
</Recipient>
```

4.2.2. Nach Empfängern selektieren

eXpurgate bietet die Möglichkeit Einstellungen auf einzelne Empfänger zu beschränken, indem die Anweisung `Address` oder die `Addresses`-Sektion angewendet wird.

Beispiel:


```
<Recipient>
  Address user1@example.com
  <Addresses>
    user2@abteilung1.example.com
    user2@abteilung2.example.com
  </Addresses>
  # Weitere Anweisungen, die nur fuer die oben
  # genannten Adressen gelten.
</Recipient>
```

Auch hier ist — wie bei Domain — die verkürzte Schreibweise durch Verwendung einer Addresses-Sektion möglich.

4.3. Features

Mit Feature-Anweisungen in den UserSettings können sie bestimmte einzelne Funktionen von eXpurgate aktivieren und deaktivieren. Die Features lassen sich global und empfängerspezifisch setzen.

Aktuell sind die nachfolgenden Features definiert.

4.3.1. Feature Spam

Aktiviert die E-Mail-Kategorisierung und damit die Spam-Erkennung.

Beispiel:

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

Hiermit wird die Spam-Erkennung von eXpurgate global eingeschaltet. Für einzelne Empfänger wird die Erkennung jedoch ausgeschaltet.

4.3.2. Feature Virus

Aktiviert den integrierten Virenschanner AntiVir.

Beispiel:

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

Der Virens Scanner wird hiermit global eingeschaltet. Eine Domain sowie ein einzelner Empfänger werden jedoch von der Erkennung ausgenommen und erhalten E-Mails mit Viren ungefiltert.

4.3.3. Feature Outbreak

Aktiviert die Virenfrüherkennung Virus-Outbreak-Detection in eXpurgate.

Beispiel:

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

Die Virus-Outbreak-Detection wird global eingeschaltet.

4.3.4. Feature Freezing

Dieses Feature aktiviert das Freezing in eXpurgate. Lesen Sie sich bitte für weitere Informationen den Abschnitt 3.2.7 durch.

Beispiel:

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

Mit dieser Sektion wird Freezing global aktiviert. Allerdings werden zwei Adressen ausgenommen, um eine verzögerungsfreie Zustellung von E-Mails für diese Empfänger zu garantieren.

4.4. E-Mail-Verarbeitung festlegen

Für kategorisierte E-Mails lässt sich festlegen, wie diese behandelt werden sollen. Dafür steht die `MailActions`-Sektion bereit. In dieser Sektion können Regeln zur Verarbeitung von E-Mails in Abhängigkeit von der Kategorisierung und des Absenders definiert werden.

Auch diese Verarbeitungsregeln können empfängerspezifisch konfiguriert werden, indem die `MailActions`-Sektion in eine entsprechende `Recipient`-Sektion eingebettet wird.

Durch Aktionen wird die eigentliche Verarbeitung von E-Mails gesteuert. Es gibt finale und nicht-finale Aktionen. Jede Verarbeitungsregel kann eine finale Aktion und beliebig viele nicht-finale Aktionen enthalten.

Es stehen die folgenden finalen Aktionen zur Verfügung:

Deliver

Die E-Mail wird an den ursprünglichen Empfänger zugestellt. Für den Transport wird der Standard-SMTP-Server verwendet.

Syntax: `Deliver`

DeliverTo

Die E-Mail wird an einen neuen Empfänger zugestellt. Dabei stehen die in Abschnitt 4.6 genannten Substitutionsvariablen zur Verfügung.

Achtung: Die Aktion `DeliverTo` hat lediglich ein Umschreiben des `Envelope-Recipients` zur Folge. Dies hat keine Auswirkung auf die Auswahl des Relay-Servers.

Syntax: `DeliverTo address`

Beispiel: `DeliverTo john@example.com`

Delete

Die E-Mail wird unwiderruflich gelöscht. Es erfolgt keine Zustellung und Warnung bzw. Bounce-Mail an den Absender der E-Mail.

Anmerkung: Die Verwendung von `Reject` ist oft eine bessere Lösung, da der Absender dann im Falle einer Fehlklassifizierung (False Positive) eine Bounce-Nachricht erhält, die darauf hinweist, dass die E-Mail nicht zugestellt werden konnte

Syntax: `Delete`

Reject

Die E-Mail wird mit einem permanenten Fehler-Code im SMTP-Protokoll abgelehnt. Dies führt im Allgemeinen dazu, dass der einliefernde E-Mail-Server eine Bounce-Meldung an den Absender schickt, in der darauf hingewiesen wird, dass die E-Mail nicht zugestellt werden konnte.

Syntax: Reject

HandleAs

Hiermit wird die E-Mail wie ein anderer E-Mail-Typ behandelt und alle für den anderen E-Mail-Typ definierten Aktionen ausgeführt.

Syntax: HandleAs *type*

Beispiel: HandleAs Spam

Außerdem stehen die folgenden nicht-finalen Aktionen zur Verfügung

UseRelay

Für die Auslieferung der E-Mail wird ein spezieller SMTP-Server oder Relay-Pool verwendet. Eine Relay-Angabe in der Form `host:port` erzwingt die Auslieferung an den genannten Server. Alternativ kann der Name eines in der Konfiguration definierten Relay-Pools angegeben werden. In diesem Fall erfolgt die Auslieferung an einen der zugehörigen Server. Siehe dazu Abschnitt 3.2.4.

Syntax: UseRelay *pool|host:port*

Beispiel: UseRelay prio-relay.example.com:25

AddHeader

Diese Anweisung fügt der E-Mail einen frei definierbaren Header hinzu. Die Anweisung erwartet zwei Parameter: Den Namen des Headers sowie seinen Wert (in Anführungszeichen). Für den Wert können die in Abschnitt 4.6 eingeführten Substitutionsvariablen verwendet werden.

Syntax: AddHeader *header string*

Beispiel: AddHeader X-Spam-Level "0"

RemoveHeader

Diese Anweisung entfernt einen Header aus der E-Mail.

Syntax: RemoveHeader *header*

Beispiel: RemoveHeader X-Mailer

RewriteSubject

Überschreibt den aktuellen Betreff einer E-Mail durch einen eigenen, frei definierbaren Wert. Auch hier können die dokumentierten Variablensubstitutionen verwendet werden.

Der wesentliche Vorteil beim Überschreiben des Betreffs ist, dass Anwender den Betreff üblicherweise direkt in ihrem E-Mail-Programm sehen, so dass sich dort leicht Hinweise und Warnungen unterbringen lassen.

Syntax: RewriteSubject *string*

Beispiel: RewriteSubject "[Dangerous] %s"

4.4.1. Kategoriebasierte Regeln

Die häufigste Verwendung von Aktionen erfolgt in Abhängigkeit der Kategorisierung durch eXpurgate. Mit der Sektion MailType kann eine besondere Behandlung für einzelne E-Mail-Typen erzwungen werden. Die Auswahl der Kategorie erfolgt mit der Anweisung Category.

Beispiel:

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

Hier wird für die E-Mail-Typen *spam* und *dangerous.virus* festgelegt, dass solche E-Mails zurückgewiesen werden sollen. Über eine *HandleAs*-Aktion wird die gleiche Behandlung auch für *bulk.advertisement* erzwungen. Im obigen Beispiel werden globale Einstellungen für die E-Mail-Typen festgelegt. Wird eine MailActions-Sektion in eine Recipient-Sektion eingebettet, so gilt die Behandlung dieser E-Mail-Typen nur für die entsprechenden Empfänger.

Beispiel:

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

```
</MailType>
</MailActions>
<Recipient>
  Domain marketing.example.com
  <MailActions>
    <MailType>
      Category Bulk.Advertisement
      Deliver
    </MailType>
  </MailActions>
</Recipient>
</UserSettings>
```

Hier wird das Beispiel von oben erweitert: Spam-, Viren- und Werbe-E-Mails werden global abgelehnt. Für die Domain `marketing.example.com` wird eine Sonderbehandlung eingestellt, da diese Werbe-E-Mails erhalten soll.

4.4.2. Absenderbasierte Regeln

Die Definition von Absendern, die dann z.B. für Black- und Whitelisting verwendet werden können, erfolgt in `MailFrom`- und `SenderId`-Sektionen innerhalb der `MailActions`-Sektion.

Mit der Sektion `MailFrom` können Envelope-Mail-From-basierte Verarbeitungsregeln definiert werden. Wie in der `Recipient`-Sektion stehen hier die Anweisungen `Domain`, `Domains` sowie `Address` und `Addresses` zur Verfügung, um den Absender einzugrenzen.

Beispiel:

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

Hiermit wird ein Absender definiert, der die Domains `partner.com` und `partner.de` einschließt sowie alle ihre Unter-Domains. E-Mails von diesen Absendern werden als *clean* behandelt (Whitelisting).

Mit der `SenderId`-Sektion können IP-basierte Verarbeitungsregeln definiert werden. Eine oder mehrere Source-Anweisungen spezifizieren den Host genau.

Beispiel:

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

Hier werden ein Host mit der IP-Adresse 10.10.1.100 definiert sowie ein komplettes Netzwerk 10.10.0.0 mit einer 24-Bit-Netzmaske. Für diese Sender-IP-Adressen wird die Verbindung generell abgelehnt (Blacklisting).

Auch IP-Adressen lassen sich in eine Recipient-Sektion einschließen. Dadurch lässt sich eine Sonderbehandlung dieser Adressen für den jeweiligen Empfänger festlegen.

4.4.3. Aktionen für IP-Adressen, Absender und E-Mail-Typen

Die Leistungsfähigkeit der Verarbeitungsregeln ergibt sich aus der Möglichkeit, die Aktionen mit E-Mail-Typen, sendenden IP-Adressen und Absendern zu kombinieren. Diese können wiederum je Empfänger angewendet werden, so dass sich sehr fein granulierte Einstellungen für die E-Mail-Verarbeitung vornehmen lassen.

Bei der Suche nach passenden Aktionen für eine E-Mail wird zunächst nach einer möglichst genauen Übereinstimmung des Empfängers in einer Recipient-Sektion gesucht. Findet sich keine Übereinstimmung, werden die globalen Einstellungen herangezogen.

Bei den auszuführenden Aktionen wird in der Reihenfolge (1). SenderIp, (2). MailFrom, (3). MailType nachgesehen, ob eine Übereinstimmung für die aktuelle E-Mail gefunden wird. Die erste Übereinstimmung führt dazu, dass die zugehörigen Aktionen ausgeführt werden. Nach weiteren Übereinstimmungen wird dann nicht mehr gesucht. Eine Ausnahme bildet hier die Aktion HandleAs: Diese setzt die Suche nach einer MailType-Sektion fort, die mit dem als Parameter angegebenen E-Mail-Typen übereinstimmt. SenderIp- und MailFrom-Sektionen werden dann ignoriert.

4.5. Anwendungsbeispiele

4.5.1. Whitelisting

Die folgende Konfiguration erstellt eine Whitelist für eine bestimmte Empfänger-Domain.

Beispiel:

```
<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>
```

```
<SenderId>
  # Dieser Host gehoert einer Partner-Firma
  Source 10.10.10.1
  HandleAs Clean
</SenderId>
<MailFrom>
  # Diese Absender duerfen immer durch
  Domain *partner.com
  Address friend@reseller.com
  AddHeader X-Whitelisted "Whitelisting for partners"
  HandleAs Clean
</MailFrom>
</MailActions>
<Recipient>
</UserSettings>
```

Spam- sowie Virencheck sind hier global eingeschaltet. Für E-Mails, die als *spam* oder *virus* erkannt wurden, wird als Standard ein Reject durchgeführt, d.h. die E-Mail wird mit einem permanenten Fehler abgelehnt. E-Mails, die als *clean* oder *bulk* erkannt wurden, erhalten einen zusätzlichen E-Mail-Header, der den Typ der E-Mail enthält. Schließlich erfolgt eine Zustellung an den Empfänger der E-Mail. In der Recipient-Sektion wird jedoch eine Ausnahmeregel für die Domain marketing.example.com eingeführt. Diese versieht eine IP-Adresse, eine Absender-Domain sowie einen Absender mit einem HandleAs Clean. Dadurch werden alle E-Mails, die von diesen Absendern gesendet wurden, wie eine *clean*-E-Mail behandelt und die entsprechenden Aktionen ausgeführt. Zu diesen Aktionen gehören das Hinzufügen des E-Mail-Headers X-Whitelisted und die Zustellung der E-Mail. Die so per Whitelisting behandelten E-Mails werden also speziell markiert.

4.5.2. Blacklisting

Auch eine Blacklist läßt sich über die HandleAs-Anweisung und den Einsatz von SenderIp- und MailFrom-Sektionen realisieren.

Beispiel:

```
<UserSettings>
  Feature Spam On
  Feature Virus On
  <MailActions>
    <MailFrom>
      # Diese Absender duerfen nie durchgelassen werden
      Domain *annoying.com
      Reject
    </MailFrom>
  </MailActions>
</UserSettings>
```

Dieses Beispiel realisiert eine einfache Blacklist. E-Mails von der Domain annoying.com werden generell abgelehnt.

4.6. Substitutionen

Für die Aktionen `AddHeader`, `RewriteSubject` sowie `DeliverTo` stehen einige Variablen zur Verfügung, die Text durch aktuelle Daten aus dem Verarbeitungsprozess der E-Mail ersetzen können.

Dies sind im Einzelnen:

%d Der Teil der Empfänger-Adresse nach dem @-Zeichen, also die Domain.

%s Der originale Betreff der E-Mail.

%t Der eXpurgate E-Mail-Typ nach einer Behandlung durch `HandleAs`.

%T Der originale E-Mail-Typ vor der Behandlung durch `HandleAs`.

%u Der Teil der Empfänger-Adresse vor dem @-Zeichen (der Localpart).

%v Der Name eines eventuell erkannten Virus in der E-Mail.

%x Die eXpurgate ID der E-Mail. Dabei handelt es sich um eine von eXpurgate vergebene ID, welche die E-Mail eindeutig identifiziert und bei Support-Anfragen von Bedeutung ist.

%z Die Größe der E-Mail nach dem Parsen der MIME-Struktur.

%% Das Prozent-Zeichen selbst.

Beispiel:

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

Hier wird für E-Mails, die als *dangerous.virus* erkannt werden, der Betreff umgeschrieben. Dem ursprünglichen Betreff wird der Name des erkannten Virus vorangestellt. Zudem wird die E-Mail über den Pool *Quarantine* zugestellt.

Beispiel:

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

An Spam-E-Mails wird hier ein spezieller Header angehängt, der sowohl die ursprüngliche Kategorisierung der E-Mail als auch die Kategorie nach Behandlung durch eine `HandleAs`-Aktion enthält. E-Mails, die als *bulk.advertisement* klassifiziert wurden, werden wie *spam* behandelt. Durch diese Regeln ergibt sich eine Markierung von *spam*-E-Mails mit dem Headerwert *spam / spam*. Für *bulk.advertisement*-E-Mails wird *spam / bulk.advertisement* hinzugefügt.

4.7. Limits

Es gibt keine Einschränkungen hinsichtlich der Anzahl von `Recipient`-, `MailType`-, `SenderId`- oder `MailFrom`-Sektionen, die in den `UserSettings` vorkommen können. Sie können beliebig viele Empfängergruppen definieren, Black- oder Whitelists anlegen und Spezialfälle bei der E-Mail-Verarbeitung abdecken.

4.8. Standardeinstellungen

eXpurgate führt einige Aktionen standardmäßig aus. Diese müssen in den `UserSettings` nicht explizit aufgeführt sein.

4.8.1. Header hinzufügen

Die folgenden Header werden jeder E-Mail, die nicht gelöscht oder zurückgewiesen wird, hinzugefügt:

X-purgate-ID mit einer eindeutigen ID.

X-purgate-type mit dem Typ der E-Mail, die gerade verarbeitet wird.

X-purgate-size mit der Größe der E-Mail.

X-purgate-Ad mit einer kurzen Zeichenkette, die auf die Verwendung von eXpurgate hinweist.

Diese Header ermöglichen einen Support durch eleven, der auch auf Nachfragen nach einzelnen E-Mails reagieren kann. Daher lassen sich diese Änderungen in den `UserSettings` nicht überschreiben.

4.8.2. Features

Das Feature Anti-Spam ist standardmäßig aktiviert. Anti-Virus, Virus-Outbreak-Detection und Freezing werden in Abhängigkeit von der Lizenzdatei aktiviert. Erlaubt diese Lizenz die Benutzung eines Features, so wird es von eXpurgate automatisch für alle Empfänger und eingehenden E-Mails eingeschaltet.

4.8.3. Zustellung

Jede E-Mail wird standardmäßig nach dem Hinzufügen der oben genannten Header zugestellt. Dabei wird das Standard-SMTP-Relay verwendet, das in der `SmtpRelay`-Sektion definiert wird (siehe Abschnitt 3.2.4).

5. Testen von eXpurgate

eXpurgate bietet verschiedene Möglichkeiten, Installation und Einstellungen zu überprüfen. Dabei wird das eXpurgate Binary mit entsprechenden Optionen zum Testen direkt aufgerufen. Nachdem die Konfigurationsdatei angepasst wurde, können diese Einstellungen durch die Option `--test-config` überprüft werden.

Beispiel:

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

Für die Funktion von eXpurgate ist die Erreichbarkeit der in der Konfigurationsdatei angegebenen eXpurgate Server notwendig. Dies kann durch die Option `--test-exdbs` überprüft werden. Dadurch werden die definierten Server der Reihe nach angesprochen; bei jedem Test werden der Name des Servers und das Testergebnis ausgegeben.

Beispiel:

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

Mit der Option `--test-relays` können Sie die Erreichbarkeit der konfigurierten SMTP-Relay-Server überprüfen.

Beispiel:

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

6. eXpurgate Reporting

Die Reporting-Funktion von eXpurgate bietet Ihnen die Möglichkeit, sich einen statistischen Überblick über die Verteilung der einzelnen E-Mail-Kategorien zu verschaffen. Zur Reporting-Funktion gelangen Sie über das eleven Web-Interface [my.eleven](https://my.eleven.de) unter <https://my.eleven.de>. Geben Sie Benutzername und Passwort (die Sie von eleven bekommen haben) ein und klicken sie links in der Navigationsleiste auf STATISTIKEN.

Im ersten Feld (links oben) können Sie den Zeitraum für die Statistik auswählen und die Domains. Wobei die Auswahl LETZTE WOCHE und LETZTER MONAT vom aktuellen Tag an rückwärts zählen. Wählen Sie beispielsweise am 21. des aktuellen Monats LETZTER MONAT, so wird Ihnen der Zeitraum bis zum 21. des Vormonats angezeigt. Alternativ können Sie per *markieren* einen Bereich im oberen Diagramm markieren, der Ihnen darunter vergrößert angezeigt wird.

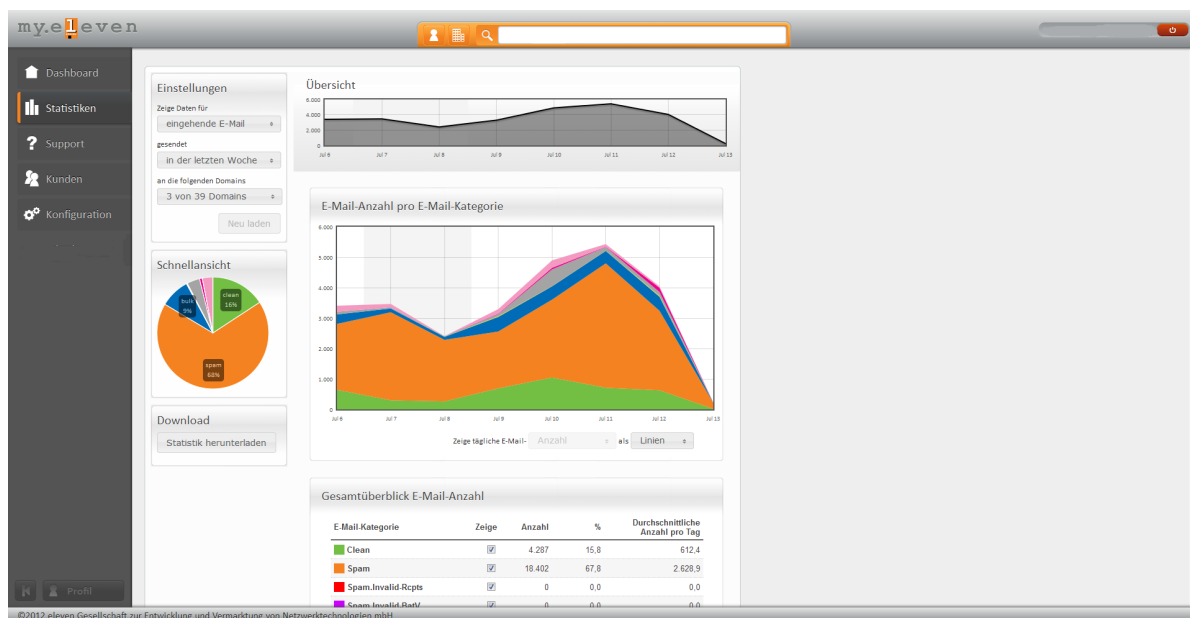


Abbildung 6.1.: Anzeige der statistischen Daten über das E-Mail-Aufkommen.

Bei der Option BELIEBIGER ZEITRAUM müssen Sie einen Zeitraum (von bis) angeben. Bitte achten Sie dabei auf die korrekte Schreibweise. Jahres-, Monats- und Tagesangaben müssen durch einen Minusstrich getrennt werden. Der 2. Dezember 2008 hätte folgende Schreibweise: 2008-12-02.

Sie erhalten die Daten über die verarbeiteten E-Mails in drei Formen: tabellarisch, als Torten- und als Verlaufsdiagramm. Außerdem können Sie sich die Daten der tabellarischen Darstellung als Excel-Datei herunterladen, um diese für eigene Berechnungen bzw. Präsentationen zu nutzen.

Den unterschiedlichen Darstellungsformen ist gemein, dass Sie jeweils die absolute Anzahl der einzelnen E-Mail-Kategorien und deren prozentualen Anteil bezogen auf alle E-Mails umfassen und farbig darstellen. So erhalten Sie schnell einen Überblick darüber, wie hoch der Anteil *sauberer* (*cleaner*) E-Mails im Verhältnis zu den weniger bzw. gar nicht erwünschten E-Mails ist.

A. Anhang

A.1. Best-Practice-Empfehlungen

Um die Sicherheit der Enduser zu gewährleisten, empfiehlt eleven, die Best-Practice-Einstellungen zu wählen. Um diese zu erreichen, müssen lediglich die Regeln für drei Kategorien eingestellt werden. Die Kategorien *spam*, *dangerous.virus-outbreak* und *dangerous.virus* werden dazu auf *reject*, also abweisen gesetzt, *df* steht dabei für default. Wenn Ihre Lizenz keinen Virenschutz enthält, müssen Sie die E-Mail-Behandlung für die Kategorien *dangerous.virus* und *dangerous.virus-outbreak* nicht konfigurieren. Stattdessen stellen Sie in diesem Fall bitte den Reject-Modus für die Kategorie *dangerous.attachment* ein. Bitte beachten Sie, dass die Kategorie *bulk.porn*, die Newsletter pornografischen Inhalts umfasst, in der Grundkonfiguration als *behandeln wie Spam* eingestellt ist.

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

Tabelle A.1.: Default-Einstellungen und Empfehlungen von eleven zur E-Mail-Behandlung

A.2. Beispieldatei

```

<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 Kategorien

eXpurgate weist allen geprüften E-Mails eine der folgenden Kategorien zu:

clean E-Mails, die keine verdächtigen Merkmale aufweisen

bulk In Massen versendete E-Mails, wie zum Beispiel Newsletter

spam Eindeutig identifizierte Spam- und Phishing-E-Mails

dangerous E-Mails, die unter Umständen gefährlichen ausführbaren Code oder entsprechende Attachments (Dateianhänge) enthalten

dangerous.attachment E-Mails, die ein ausführbares Attachment (Dateianhang) enthalten. Das sind: ade, adp, app, asp, bas, bat, bxx, cab, ceo, chm, cmd, com, cpl, crt, csr, der, exe, fxx, 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 mit potentiell gefährlichem Inhalt, wie zum Beispiel Links auf lokale Dateien

dangerous.iframe E-Mails, die das iframe-Feature benutzen (Ein in einer E-Mail eingebettetes iframe könnte beispielsweise benutzt werden, um ein Script auszuführen, das Zugang zum lokalen Dateisystem hat und Dateien lesen oder löschen kann.)

dangerous.virus E-Mails, die einen Virus enthalten (Diese Kategorie steht nur dann zur Verfügung, wenn der die Anti-Virus-Option aktiviert ist.)

dangerous.virus-outbreak E-Mails, die mit höchster Wahrscheinlichkeit einen neuen, unbekannten Virus enthalten, der aber aufgrund seiner Neuartigkeit von Virensclannern noch nicht als solcher erkannt werden kann (Diese Kategorie steht nur dann zur Verfügung, wenn der die Anti-Virus-Option aktiviert ist.)

bulk.advertising Werbe-E-Mails, die kein typischer Spam, aber in der Regel unerwünscht sind

bulk.porn E-Mails mit pornografischen Inhalten, die nicht *spam* sind (zum Beispiel pornografische Newsletter)

clean.empty E-Mails, die weder über ein Subject noch über einen Body verfügen und somit völlig inhaltsleer sind

clean.empty-body E-Mails, deren Body leer und deren Subject nicht leer sind

clean.almost-empty E-Mails, deren Body beinahe leer ist

clean.bounce E-Mails, die wegen eines Zustellungsfehlers an den Absender zurückgeschickt werden

A.4. Variablen

action Finale Aktion für einen einzelnen Empfänger.

all-rcpttos Liste aller Envelope-Empfänger-Adressen der E-Mail durch Semikolon getrennt.

authcid Username des AUTH-Befehls.

cipher Verwendeter Verschlüsselungsalgorithmus.

cipher-bits Schlüssellänge des SSL/TLS-Session-Keys.

commands Liste aller verfügbaren SMTP-Kommandos.

connection-id Eindeutiger Identifikationsstring einer SMTP-Verbindung.

domain SMTP-Domain für Banner und HELO/EHLO Antworten. Konfigurierbar durch die Einstellung `HeloHostname` in der `SmtpServer`-Sektion.

error Fehlermeldung.

expurgate-id Identifikationsstring der E-Mail im eXpurgate-System.

extensions Liste aller unterstützten SMTP-Erweiterungen.

helo Parameter des HELO bzw. EHLO Befehls.

issuer Common Name des Ausstellers des Zertifikats des einliefernden E-Mail-Servers.

mailfrom Envelope-Absender-Adresse der E-Mail aus dem MAIL FROM-Befehl.

message SMTP-Antwort des Relay-Servers.

message-id Eindeutiger Identifikationsstring einer E-Mail. Setzt sich aus `connection-id` und `message-number` zusammen.

message-number Laufende Nummer der E-Mail-Transaktionen innerhalb einer Verbindung. Wird durch die SMTP-Befehle HELO, EHLO und RSET, sowie die vollständige Übertragung einer E-Mail erhöht.

original-rcptto Ursprünglicher Empfänger vor Umschreibung durch DeliverTo.

peer IP-Adresse und Port des einliefernden E-Mail-Servers.

peer-ip IP-Adresse des einliefernden E-Mail-Servers.

peer-port Port des einliefernden E-Mail-Servers.

pool Name des verwendeten Relay-Pools oder Servers.

protocol Name des verwendeten Protokolls.

rcptto Envelope-Empfänger-Adresse der E-Mail oder `multiple-recipients` falls mehrere Empfänger vorhanden sind.

received Zeitstempel des Empfangs der E-Mail.

relay IP-Adresse und Port des Relay-Servers.

relay-ip IP-Adresse des Relay-Servers.

relay-port Port des Relay-Servers.

score Summe aller Score-Werte aus DNS-Blacklist-Abfragen.

subject Common Name des Zertifikats des einliefernden E-Mail-Servers.

tls-version Verwendete Version des SSL/TLS-Protokolls.

type Klassifikation der E-Mail.

version Version der eXpurgate Software im Format X.Y.Z.

zones Liste aller DNS-Blacklisten in denen der einliefernde E-Mail-Server gelistet ist.

A.5. Log-Meldungen

Keyword	Bedeutung
general-start	Meldung zum Start des Dienstes Variablen: version
general-shutdown	Meldung beim Beenden des Dienstes Variablen: version
general-reconfigure	Meldung bei Erhalten eines Reconfigure-Signals Variablen: version
smtp-connect	Meldung bei neuer SMTP-Verbindung Variablen: version, connection-id, peer, peer-ip, peer-port
smtp-disconnect	Meldung bei Ende einer SMTP Verbindung Variablen: version, connection-id, peer, peer-ip, peer-port
smtp-helo	Meldung bei HELO/EHLO Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo
smtp-mailfrom	Meldung bei MAIL FROM Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom
smtp-rcptto	Meldung bei RCPT TO Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom, rcptto
smtp-data	Meldung bei DATA Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom
smtp-endofdata	Meldung bei Abschluss der Einlieferung Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, helo, mailfrom
smtp-reset	Meldung bei RSET Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id
smtp-quit	Meldung bei QUIT Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id
smtp-xclient	Meldung bei XCLIENT Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id
smtp-xforward	Meldung bei XFORWARD Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id
smtp-auth	Meldung bei AUTH Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, authcid
smtp-starttls	Meldung bei STARTTLS Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id
smtp-tlsupgraded	Meldung bei erfolgreichem TLS-Upgrade Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, tls-version, cipher, cipher-bits, subject, issuer
smtp-tlsupgradedfailed	Meldung bei nicht erfolgreichem TLS Upgrade Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, error
smtp-syntax-error	Meldung bei syntaktisch inkorrekten Befehlen innerhalb einer E-Mail-Transaktion Variablen: version, connection-id, peer, peer-ip, peer-port, message, error
smtp-syntax-error-connection	Meldung bei syntaktisch inkorrekten Befehlen außerhalb einer E-Mail-Transaktion Variablen: version, connection-id, peer, peer-ip, peer-port, message, error

acl-connect-denied	Meldung bei nicht erlaubten eingehenden Verbindungsaufbau Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
acl-relay-denied	Meldung bei Verbot eines Servers E-Mails an nicht-lokale Domains einzuliefern Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
acl-xclient-denied	Meldung bei Verbot eines Servers den XCLIENT-Befehl anzuwenden Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
acl-xforward-denied	Meldung bei Verbot eines Servers den XFORWARD-Befehl anzuwenden Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
relay-address-denied	Meldung bei Ablehnung eines Empfängers mit einer Relay-Adresse Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
check-mailfrom-permanent-reject	Meldung bei permanenter Ablehnung eines Absenders durch den Relay-Server Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
check-mailfrom-temporary-reject	Meldung bei temporärer Ablehnung eines Absenders durch den Relay-Server Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
check-rcptto-permanent-reject	Meldung bei permanenter Ablehnung eines Empfängers durch den Relay-Server Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
check-rcptto-temporary-reject	Meldung bei temporärer Ablehnung eines Empfängers durch den Relay-Server Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
tls-not-encrypted	Meldung bei fehlender Verschlüsselung Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
tls-verification-failed	Meldung bei fehlschlagen einer Zertifikats-Verifikation Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
auth-failed	Meldung bei fehlgeschlagener Authentifizierung Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, message
dnsbl-reject	Meldung bei Ablehnung eines E-Mail-Servers aufgrund eines DNS-Blacklisten-Eintrages Variablen: version, connection-id, message-number, message-id, peer, peer-ip, peer-port, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, score, zones
arbiter-scan	Meldung bei erstmaligem Scannen einer E-Mail Variablen: connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type
arbiter-rescan	Meldung bei wiederholtem Scannen einer E-Mail Variablen: connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type
arbiter-action	Meldung bei Festlegung der MailAction pro Empfänger Variablen: connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos, expurgate-id, type, action

relay-delivery	Meldung bei erfolgreichem Versand einer E-Mail Variablen: 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
relay-delivery-failed	Meldung bei Abweisung einer E-Mail durch den Relay-Server Variablen: 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
batv-denied	Meldung bei Ablehnung einer E-Mail aufgrund einer ungültigen BATV-Signatur Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos
batv-delayed-denied	Meldung bei verzögerter Ablehnung einer E-Mail aufgrund einer ungültigen BATV-Signatur Variablen: version, connection-id, peer, peer-ip, peer-port, message-number, message-id, protocol, authcid, helo, mailfrom, rcptto, received, all-rcpttos

A.6. SMTP-Antworten

Keyword	Bedeutung
banner	SMTP-Banner bei Verbindungsaufbau Variablen: domain, product-name, version, peer, peer-ip, peer-port
helo	Antwort auf HELO Variablen: domain, product-name, version, peer, peer-ip, peer-port, helo
ehlo	Antwort auf EHLO Variablen: domain, product-name, version, peer, peer-ip, peer-port, helo, extensions
quit	Antwort auf QUIT Variablen: domain, product-name, version, peer, peer-ip, peer-port
rset	Antwort auf RSET Variablen: domain, product-name, version, peer, peer-ip, peer-port
mailfrom	Antwort auf MAIL FROM Variablen: domain, product-name, version, peer, peer-ip, peer-port, mailfrom
rcptto	Antwort auf RCPT TO Variablen: domain, product-name, version, peer, peer-ip, peer-port, rcptto
xclient	Antwort auf XCLIENT Variablen: domain, product-name, version, peer, peer-ip, peer-port
xforward	Antwort auf XFORWARD Variablen: domain, product-name, version, peer, peer-ip, peer-port
starttls	Antwort auf STARTTLS Variablen: domain, product-name, version, peer, peer-ip, peer-port
vrfy	Antwort auf VRFY Variablen: domain, product-name, version, peer, peer-ip, peer-port
help	Antwort auf HELP Variablen: domain, product-name, version, peer, peer-ip, peer-port, commands
auth	Antwort auf AUTH Variablen: domain, product-name, version, peer, peer-ip, peer-port, authcid
data	Antwort auf DATA Variablen: domain, product-name, version, peer, peer-ip, peer-port
not-available	Fehlermeldung bei Shutdown Variablen: domain, product-name, version, peer, peer-ip, peer-port
session-timeout	Fehlermeldung bei Session Timeout Variablen: domain, product-name, version, peer, peer-ip, peer-port
command-timeout	Fehlermeldung bei Command Timeout Variablen: domain, product-name, version, peer, peer-ip, peer-port
local-error	Meldung zu lokalen Fehlern Variablen: domain, product-name, version, peer, peer-ip, peer-port
rcptto-too-many	Fehlermeldung bei zu vielen RCPT TO Variablen: domain, product-name, version, peer, peer-ip, peer-port
invalid-command	Fehlermeldung bei unbekannten Kommandos Variablen: domain, product-name, version, peer, peer-ip, peer-port
syntax-error	Fehlermeldung bei syntaktischen Fehlern Variablen: domain, product-name, version, peer, peer-ip, peer-port
not-implemented	Fehlermeldung bei nicht verfügbaren Kommandos Variablen: domain, product-name, version, peer, peer-ip, peer-port
tls-failed	Fehlermeldung bei fehlgeschlagenem SSL-Handshake Variablen: domain, product-name, version, peer, peer-ip, peer-port
helo-first	Fehlermeldung bei nicht verwendetem HELO/EHLO Variablen: domain, product-name, version, peer, peer-ip, peer-port
mailfrom-nested-mail	Fehlermeldung bei mehrfachen MAIL FROMs Variablen: domain, product-name, version, peer, peer-ip, peer-port

rcptto-mailfrom-needed	Fehlermeldung bei RCPT TO ohne MAIL FROM Variablen: domain, product-name, version, peer, peer-ip, peer-port
data-rcptto-needed	Fehlermeldung bei DATA ohne RCPT TO Variablen: domain, product-name, version, peer, peer-ip, peer-port
data-size-exceeded	Fehlermeldung für zu große E-Mails Variablen: domain, product-name, version, peer, peer-ip, peer-port
xclient-in-progress	Fehlermeldung bei XCLIENT nach MAIL FROM Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-in-progress	Fehlermeldung bei AUTH nach MAIL FROM Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-already	Fehlermeldung bei mehrfachen AUTHs Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-unsupported	Fehlermeldung bei ungültigem Authentifizierungsmechanismus Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-cancelled	Fehlermeldung bei Abbruch der Authentifizierung durch den Client Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-failed	Fehlermeldung bei ungültigen Authentifizierungsdaten Variablen: domain, product-name, version, peer, peer-ip, peer-port
auth-required	Fehlermeldung bei obligatorischer Authentifizierung Variablen: domain, product-name, version, peer, peer-ip, peer-port
acl-connect-denied	Fehlermeldung bei Ablehnung durch Connect-ACL Variablen: domain, product-name, version, peer, peer-ip, peer-port
acl-relay-denied	Fehlermeldung bei Ablehnung durch Relay-ACL Variablen: domain, product-name, version, peer, peer-ip, peer-port
acl-xclient-denied	Fehlermeldung bei Ablehnung durch XClient-ACL Variablen: domain, product-name, version, peer, peer-ip, peer-port
acl-xforward-denied	Fehlermeldung bei Ablehnung durch XForward-ACL Variablen: domain, product-name, version, peer, peer-ip, peer-port
tls-not-encrypted	Fehlermeldung bei Ablehnung durch TLS-Policy Variablen: domain, product-name, version, peer, peer-ip, peer-port
tls-verification-failed	Fehlermeldung bei Ablehnung durch TLS-Policy Variablen: domain, product-name, version, peer, peer-ip, peer-port
check-mailfrom-temporary-error	Fehlermeldung bei temporärer MAIL FROM-Ablehnung durch Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, message
check-mailfrom-permanent-error	Fehlermeldung bei permanenter MAIL FROM-Ablehnung durch Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, message
check-rcptto-temporary-error	Fehlermeldung bei temporärer RCPT TO-Ablehnung durch Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, message
check-rcptto-permanent-error	Fehlermeldung bei permanenter RCPT TO-Ablehnung durch Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, message
endofdata-accept	Antwort bei Annahme einer E-Mail Variablen: domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type
endofdata-reject	Antwort bei Ablehnung einer E-Mail Variablen: domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type
endofdata-temporary-error	Fehlermeldung bei temporären Auslieferungsproblemen an den Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type
endofdata-permanent-error	Fehlermeldung bei permanenten Auslieferungsproblemen an den Relay-Server Variablen: domain, product-name, version, peer, peer-ip, peer-port, expurgate-id, message, type
batv-denied	Fehlermeldung bei Ablehnung durch ungültige BATV-Signatur Variablen: domain, product-name, version, peer, peer-ip, peer-port, rcptto

batv-delayed-deny

Fehlermeldung bei verzögerter Ablehnung durch ungültige BATV-Signatur
Variablen: domain, product-name, version, peer, peer-ip, peer-port, rcptto

A.7. IP-Bereiche der eXpurgate Server

Gegenwärtig werden von der eleven GmbH die folgenden Netze für die Erbringung des eXpurgate Dienstes verwendet und sind wie folgt in der RIPE-Datenbank dokumentiert:

```
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. Lizenzen

eXpurgate verwendet die folgenden Lizenzen:

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

Abbildungsverzeichnis

1.1. eXpurgate als Inhouse-Installation. Die Verarbeitung der E-Mails erfolgt im Unternehmensnetzwerk. Es werden nur Kontrollsummen mit der eXpurgate Datenbank ausgetauscht. . . .	6
1.2. Allen E-Mails werden Fingerprints zugeordnet, die in der eXpurgate Datenbank gesammelt werden. Die Identifizierung als <i>spam</i> erfolgt, wenn eine gleiche oder ähnliche Kontrollsumme massenhaft auftritt und über zusätzliche Prüfmethode ausgeschlossen werden kann, dass es sich um eine legitime Massen-E-Mail (z. B. Newsletter) handelt.	8
2.1. Startseite des Installationsassistenten	14
2.2. Lizenzvereinbarung	15
2.3. Auswahl des Zielverzeichnisses	16
2.4. Einfügen von eXpurgate in das Startmenü	17
2.5. Verbindungsoptionen	18
2.6. Weitere Behandlung der Spam-E-Mails	19
2.7. Umschreiben der Betreffzeile	20
2.8. Auswahl der SSL/TLS-Optionen	21
2.9. Prüfen der eingegeben Daten	22
2.10. Abschlussbildschirm der Installation	23
2.11. Eintrag von eXpurgate als Dienst in der Microsoft-Dienste-Konsole	24
2.12. Exchange-System-Manager	26
2.13. Virtueller Standardserver	27
2.14. Advanced	28
2.15. Identifikation	29
6.1. Anzeige der statistischen Daten über das E-Mail-Aufkommen.	93