

NoSpamProxy 12.2

Betriebshandbuch

- Protection
- Large Files



Impressum

Alle Rechte vorbehalten. Dieses Handbuch und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Handbuch enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2017 Net at Work GmbH

Net at Work GmbH

Am Hoppenhof 32a

D-33104 Paderborn

Handelsmarken

Microsoft®, Windows®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2® und Windows Server 2016® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® ist eine eingetragene Handelsmarke der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern / Inhabern.

17. April 2018

Inhalt

1. NoSpamProxy	9
NoSpamProxy Protection	9
Spam und Spam-Schutz	9
Abwehren statt Sortieren	9
Wie kann ich als Anwender einen False Positive korrigieren?	10
Proxy statt Relay	10
Proxy-Vorteile	10
Schutzfunktion	10
NoSpamProxy Large Files	11
NoSpamProxy Disclaimer	11
Mehrnutzen durch NoSpamProxy Encryption	11
2. Hilfe und Unterstützung	12
3. Die Rollen von NoSpamProxy	13
Gateway Rolle	13
Intranet Rolle	13
Web Portal	13
4. Funktionsweise und Einbindung in die Infrastruktur	14
Firewall	15
SMTP E-Mail-Server	15
SQL-Datenbank	16
Domain Name System (DNS)	16
Verzeichnisdienst, Active Directory	16
Beispiele für die Implementierung	16
Prinzipielles zum Einsatz von NoSpamProxy	16
NoSpamProxy vorgeschaltet	16
NoSpamProxy auf dem E-Mail-Server	17
NoSpamProxy mit NAT-Router	17
NoSpamProxy mit Firewall und DMZ	18
NoSpamProxy und SMTP-Virenschanner	18
Installation der Rollen auf unterschiedlichen Servern	19
Negativbeispiel: Falsche Konfiguration	21
E-Mails an externe Adressen	22
5. NoSpamProxy Verwaltungskonsolle	23
Sprache der Oberfläche ändern	23
Verbindung zur Intranet Rolle herstellen	23
6. Übersichtsseite	25
Liste der Rollen	25
Bereich für Aktionen	26
Serverleistung ansehen	26
Datenverkehr	26
System	26
Konfigurationsassistent starten	27

Handbuch herunterladen	28
Lizenz verwalten	28
Editionen vergleichen	29
Update herunterladen	29
Auswahl des Update-Kanals	29
Vorfälle	29
Neueste Meldungen	30
7. Monitoring	31
Nachrichtenverfolgung	31
Die Details nachprüfen	33
E-Mail-Warteschlangen	34
Angehaltene E-Mails	36
Large files	38
Reports	39
Datenverkehr und Spam Report	40
Most wanted	41
De-Mail	42
Lizenz-Report	42
Ereignisanzeige	43
8. Menschen und Identitäten	45
Domänen und Benutzer	45
Eigene Domänen	46
Eigene Domänen hinzufügen	46
DomainKeys Identified Mail	47
Unternehmensbenutzer	49
Benutzer hinzufügen	50
Neue Adressumschreibung	56
Standardeinstellungen für Benutzer	58
Automatischer Benutzerimport	58
Neuer Benutzerimport	59
Active Directory	60
Generisches LDAP	63
Zusätzliche Benutzerfelder	67
Textdatei	67
Partner	68
Partnerabschnitt	68
Standardeinstellungen für Partner	68
Partnerdomänen	69
Neue Partnerdomäne	71
Partnerdomäne bearbeiten	74
Benutzereintrag einer Partnerdomäne	74
Open Keys Web Service nutzen	75
Zusätzliche Benutzerfelder	76
9. Konfiguration	78

E-Mail-Routing	78
Lokale E-Mail-Server	79
Mehrfach verwendete Einstellungen der Konnektoren	83
Name	83
Bindung an Gateway Rollen	83
Kosten	83
Verbindungssicherheit	84
SMTP Sicherheitseinstellungen	84
Server- oder Client-Identität	85
DNS Routing Einschränkungen durch Konnektor-Namensräume	87
Smarthost: E-Mail-Zustellung über dedizierten Server	88
Lokale Zustellung	91
Zustellung über Warteschlangen	91
Allgemeine Einstellungen	92
SMTP Verbindungen	92
Konfiguration eines Smarthosts	92
DNS Routing Einschränkungen	92
Direkte Zustellung	92
Externe Zustellung	93
SMTP	93
Allgemeine Einstellungen	93
Zustellung - Direkte Zustellung (DNS)	94
Zustellung - Dedizierte Server (Smarthosts)	95
DNS Routing Einschränkungen	95
De-Mail über Telekom	95
De-Mail über Mentana-Claimsoft GmbH	96
Zuordnung der eigenen Domänen	97
E-Postbrief Konnektor	98
Deutschland-Online - Infrastruktur Konnektor	100
Empfangskonnektoren	102
SMTP-Konnektoren	103
SMTP-Einstellungen	103
Ungültige Anfragen	104
Verbindungssicherheit	106
Regeln	107
Filter	108
Aktionen	109
Aktionen für die Spam-Prüfung	109
Wie NoSpamProxy Protection eine E-Mail als Spam klassifiziert	109
Konfiguration der Regeln	110
Neue Regel erstellen	111
Reihenfolge der Regeln ändern	119
Filter in NoSpamProxy	120
Cyren IP Reputation	120

Cyren AntiSpam	120
Erlaubte Unicode Sprachbereiche	121
Realtime Blocklists	122
Spam URI Realtime Blocklists	124
SpamAssassin Konnektor	124
Reputationsfilter	126
Wortübereinstimmungen	127
Aktionen in NoSpamProxy	128
Aktionen können E-Mails verändern	128
Adressmanipulation	129
Cyren Premium AntiVirus	130
CSA-Whitelist	130
Dateibasierter Virenschanner	131
Greylisting	132
Verberge interne Topologie	134
Automatische Antwort	134
Leite E-Mail um	134
DKIM-Signatur anwenden	135
Disclaimer anwenden	135
Berechnung des Spam Confidence Level	136
Voreinstellungen	139
Farbschema	140
Wortübereinstimmungen	140
Neue Wortgruppe hinzufügen	141
Realtime Blocklists	142
Neue Blocklist hinzufügen	142
Inhaltsfilter	146
Inhaltsfilter	147
Hinweise zum Hochladen	152
Aktionen des Inhaltsfilters	153
NoSpamProxy Komponenten	156
Gateway Rollen	157
Server-Identität	158
Verbindung zu einer Gateway Rolle herstellen	159
Web Portal	159
Web Portal Verbindungen	159
Web Portal - Einstellungen	161
Datenbanken	163
Verbundene Systeme	166
DNS-Server	167
Archivschnittstelle	168
De-Mail-Anbieter	177
Telekom De-Mail-Verbindungen	178
Verbindung zu Mentana-Claimsoft	179

CSA-Whitelist	180
Benutzer-Benachrichtigungen	181
Administrative E-Mail-Adressen	182
Benutzer-Benachrichtigungen	182
Erweiterte Einstellungen	182
Schutz sensibler Daten	183
Monitoring	184
Betreffkennzeichnungen	186
Level-of-Trust-Konfiguration	188
Allgemeine Einstellungen	189
Stoppwörter	190
Intelligente DSN-Filterung	191
Nachrichtenkennzeichnungen	192
SMTP-Protokolleinstellungen	192
Verhalten	192
Einstellungen	194
Statusmeldungen	194
SSL/TLS-Konfiguration	195
10. Troubleshooting	197
Protokolleinstellungen	197
Geblockte IP-Adressen	199
Berechtigungen korrigieren	200
Web Portal Sicherheit	201
11. Das Web Portal	202
Large Files	202
Sichere E-Mails über das Web Portal ohne Einladung	203
12. Disclaimer	205
Bereitstellen von Platzhaltern	205
Zusätzliche Benutzerfelder im manuell eingetragene Benutzer	207
Zusätzliche Benutzerfelder im Benutzerimport	207
Benutzung der Felder im Disclaimer	208
13. Anhang	210
Mehrfach verwendete Einstellungen in der Konfiguration	210
Passwörter	210
Auswahl von Zertifikaten	210
Sicherung und Wiederherstellung	212
Betriebssystem, Treiber und Software	212
Lizenzen von NoSpamProxy	212
Konfigurationsdateien der Rollen	212
Datenbanken von NoSpamProxy	213
Fehlersuche	214
Support durch E-Mail	214
NoSpamProxy kontrollieren	215
NoSpamProxy testen	217

TELNET	217
NSLOOKUP	218
Häufige Fehler und Ihre Ursachen	219
NoSpamProxy Protection filtert nicht	219
NoSpamProxy lehnt alle E-Mails an lokale Adressen ab	220
SQL-Datenbank steht nicht zur Verfügung	220
NoSpamProxy Protection findet keine Viren	220
Smartcard nicht per RDP verwaltbar	221
Exchange-Management-Konsole startet nicht mehr	221
Kontrolle der Verbindungen	223
Leistungsindikatoren	224
Einstellungen über die Konfigurationsdatei	226
Aktivieren der Option 'Zustellen von ungültigen E-Mails'	226
Verarbeitung von RTF-Dateien bei der Inhaltsfilterung	227
SMTP RFCs	227
SMTP Errorcodes	227
SMTP Timeouts	229
Glossar	230

1. NoSpamProxy

NoSpamProxy Protection

Spam und Spam-Schutz

Mit immer ausgefeilteren Methoden versuchen Spammer, bestehende Schutzsysteme auszuhebeln und ihre Botschaften an den Adressaten zu bringen. Mit dem täglichen Aufräumen des Posteingangs ist es oft leider nicht getan; Spam bedeutet längst eine gravierende ökonomische Belastung für viele Unternehmen.

Spam wirkt störend auf die Geschäftsprozesse und bindet Mitarbeiter ebenso wie Systemressourcen. Die ungewünschten E-Mails können zudem Ihre E-Mail-Server erheblich beeinträchtigen und im Extremfall sogar lahmlegen. Sie können Inhalte und Anhänge aufweisen, die Ihr System angreifen oder ausspähen und so eine Bedrohung für Ihr Unternehmen darstellen.

Des Weiteren versuchen viele Spammer, Ihr System als Relay zu missbrauchen. Ist dies möglich, werden E-Mails unter Ihrem Namen und auf Kosten Ihrer Kapazität versendet. Seriöse E-Mail-Partner bewerten Ihre Domäne in der Folge möglicherweise als Spam-Sender, so dass wichtige Verbindungen unversehens gesperrt werden.

Doch Spam ist nicht gleich Spam, und die Angriffs-Szenarien sind vielfältig. Und so verschieden die Interessen von Unternehmen sein können, so unterschiedlich kann auch die Bewertung einer E-Mail ausfallen. Ob Sie eine E-Mail-Werbung, einen Newsletter oder eine E-Mail mit chinesischen Schriftzeichen als Spam einstufen, sollten Sie selbst definieren können. Und genau dies ermöglicht Ihnen NoSpamProxy Protection.

Abwehren statt Sortieren

Viele Spammer reagieren immer schneller und versierter auf neue Schutzmethoden. Dies bedeutet, dass statische Spam-Filter kurzfristig mitunter sehr erfolgreich arbeiten - und dennoch morgen schon nutzlos sein können.

Um wirklich greifen zu können, muss ein effektiver Spam-Schutz daher intelligent, flexibel und lernfähig sein.

Er sollte nicht nur vor unerwünschten E-Mails schützen. Mindestens genauso wichtig ist es, dass er "gute" E-Mails korrekt bewertet. Eine Quote von 99 % geblockter Spam-E-Mails klingt gut - nur schadet sie mehr als sie nützt, wenn dabei wichtige gute E-Mails versehentlich mit blockiert werden oder im falschen Ordner landen. Außerdem sollte der Schutz genauso individuell und vielseitig sein, wie es die Anforderungen Ihrer Geschäftsprozesse sind. Gleichgültig, ob Ihr Unternehmen 25 oder 5.000 Mitarbeiter hat. Letztendlich sollte ein Schutz Ihr System und die Unternehmensabläufe nicht nur vor Spam bewahren, sondern auch vor unnützer Belastung des Systems - denn die Schonung Ihrer Ressourcen steht schließlich im Mittelpunkt.

Diese Anforderungen an einen intelligenten Spam-Schutz waren unser Antrieb zur Entwicklung von NoSpamProxy Protection. Der Grundgedanke ist einfach: Im Gegensatz zu anderen Filtern wehrt NoSpamProxy Protection Spam-E-Mails ab, bevor sie in Ihr System gelangen. Strikt nach dem Motto: Abwehren statt Sortieren.

Wie kann ich als Anwender einen False Positive korrigieren?

Als False Positives bezeichnet man gute E-Mails, die versehentlich als verdächtig bewertet und abgelehnt werden. Wie bereits erwähnt, liegt hierin eine der größten Gefahren einer Filterlösung: Je mehr Spam Sie aussortieren müssen, desto wahrscheinlicher ist es, dass Sie versehentlich eine gute E-Mail beseitigen. Die Folgen können unter Umständen fatal sein.

Angenommen, Sie erhalten von einem Kunden per Telefon die Nachricht, dass seine E-Mail an Sie nicht durchgekommen ist, sondern als Spam klassifiziert und abgewiesen wurde. Diese unschöne Situation können Sie mit NoSpamProxy Protection schnell und einfach auflösen. Sie müssen hierzu weder Administrator sein noch Systemeinstellungen oder Änderungen an NoSpamProxy Protection vornehmen. Statt dessen schicken Sie einfach eine E-Mail an den Kunden.

Die nächste E-Mail des Kunden wird dann von NoSpamProxy automatisch als Reaktion auf Ihre E-Mail gewertet - auch wenn der Absender nicht die "Antwort"-Funktion verwendet - und als gut bzw. erwünscht beurteilt.

Dies bedeutet, dass ein zweiter Anlauf in der Regel problemlos durchkommt und keine weiteren False Positives entstehen. Die E-Mail-Adresse des Absenders ist von NoSpamProxy Protection als vertrauenswürdig eingestuft worden.

Proxy statt Relay

NoSpamProxy ist - wie der Name schon sagt - als Proxy konzipiert. Vereinfacht gesagt ist ein Proxy eine Zwischenstation zwischen dem Internet und Ihrem System. Ähnlich wie bei einer Firewall ist Ihr internes Netzwerk vor einem ungefilterten Kontakt mit dem Internet geschützt.

Beim Senden einer E-Mail an eigene Domänen wird zunächst eine Verbindung von außen zu NoSpamProxy aufgebaut. Anschließend stellt NoSpamProxy eine zweite Verbindung zu Ihrem E-Mail-Server her.

NoSpamProxy protokolliert die Daten, extrahiert die relevanten SMTP-Informationen und legt diese den konfigurierten Filtern zur Prüfung vor. Wird eine E-Mail als Spam erkannt, verweigert NoSpamProxy Protection deren Annahme. Dies veranlasst den einliefernden E-Mail-Server, eine Unzustellbarkeitsnachricht an den Absender zu schicken. Ein Proxy ist ideal geeignet, um eine frühzeitige Spam-Abwehr zu realisieren.

Proxy-Vorteile

Viele Funktionen des internen E-Mail-Servers bleiben nutzbar. Zum Beispiel kann der interne E-Mail-Server weiterhin E-Mails auf Grund eines vollen oder nicht mehr existierenden Postfachs ablehnen. NoSpamProxy Protection lehnt dann seinerseits die Verbindung von extern ab.

Ihr System wird nicht mit unnützem Datenvolumen beladen. Viele Verbindungen können sehr früh als Spam erkannt werden und belasten den internen E-Mail-Server nicht.

Schutzfunktion

Ihr Server ist nicht von außen erreichbar. 'Denial of Service'-Attacken behindern daher nicht die interne Kommunikation.

NoSpamProxy Large Files

Mit Large Files können Benutzer über ihre gewohnte Outlook-Oberfläche beliebig große Dateien an Empfänger übertragen, ohne das E-Mail-System zu belasten. An Stelle der Datei selbst wird ein Link an die E-Mail angehängt, mit dessen Hilfe der oder die Empfänger der E-Mail die Dateien über TLS abgesichert herunterladen können. Zusätzlich können Sie externen Empfängern einen Einladungslink für das Web Portal von Large Files zusenden, damit diese Ihnen große Dateien zusenden können.



Sprechen Sie uns unter info@netatwork.de an, wenn Sie die Möglichkeiten der Large Files interessieren. Wir beraten Sie gerne und unterstützen Sie bei der Erweiterung Ihrer bestehenden Lizenz.

NoSpamProxy Disclaimer

Mit der Disclaimer-Funktion können Vorlagen für E-Mail-Disclaimer in Ihre versandten E-Mails automatisch nach vorher definierten Regeln eingebunden werden. Die Konfiguration ist hier aufgeteilt zwischen dem NoSpamProxy-Administrator der Werte und Einstellungen für die Disclaimer vorbereitet und den Administratoren für die Disclaimer-Erstellung die diese Werte und Einstellungen auf der Disclaimer-Webseite in ihren erstellten Vorlagen und Regeln benutzen können.

Die Konfiguration der Werte wird im Kapitel [Disclaimer](#) im Detail beschrieben.

Mehrnutzen durch NoSpamProxy Encryption

Da NoSpamProxy Encryption auf den Technologien des bewährten AntiSpam-Gateways NoSpamProxy basiert, lassen sich dessen Funktionen einfach durch eine Lizenzenerweiterung freischalten. So kann auf nur einem Gateway und mit einer einheitlichen Administration die vertrauliche Kommunikation mit Partnern durchgeführt werden.

Wenn Sie NoSpamProxy mit nicht SMTP Systemen wie De-Mail, dem E-Postbrief, der Deutschland-Online - Infrastruktur und POP3-Postfächern verbinden möchten, können Sie dieses durch das einspielen einer erweiterten Lizenz mit NoSpamProxy Encryption tun.

2. Hilfe und Unterstützung

Hilfe und Unterstützung für die Installation und den Betrieb von NoSpamProxy bekommen Sie von Net at Work in vielen Formen.

- **Trainingsvideos**

Die [Trainingsvideos](#) bieten einen Überblick über verschiedene Bereiche und zeigen Möglichkeiten der Konfiguration für konkrete Anwendungsfälle.

- **Blog**

Das [Blog](#) bietet tagesaktuelle Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und viele weitere Hinweise, die Sie unterstützen. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy Konfigurationskonsole eingeblendet, so dass Sie keine wichtigen Hinweise verpassen.

- **Knowledge Base**

Die [Knowledge Base](#) enthält weiterführende technische Informationen zu speziellen Problemstellungen.

- **Support**

Wenn Sie weitergehende Unterstützung brauchen, besuchen Sie unsere [Support-Webseite](#).

3. Die Rollen von NoSpamProxy

NoSpamProxy besteht aus mehreren Rollen, die im Weiteren beschrieben werden.

Gateway Rolle

Hinter der Gateway Rolle verbirgt sich der eigentliche Kern von NoSpamProxy. In Abhängigkeit von Ihrer Umgebung kann diese Rolle entweder in eine Demilitarisierte Zone (DMZ) oder im Intranet installiert werden. Um ein hochverfügbares System aufzubauen, kann diese Rolle auf mehreren Servern installiert werden.

NoSpamProxy nimmt die E-Mails auf Port 25 an, prüft diese auf Spam und weist sie gegebenenfalls ab.

Intranet Rolle

Wie der Name schon andeutet, wird die Intranet Rolle typischerweise im Intranet Ihres Unternehmens installiert.

Web Portal

Wenn Sie Large Files aktiviert haben, können Anwender große Dateien über das Web Portal übertragen.

Um ein hochverfügbares System aufzubauen, kann diese Rolle auf mehreren Servern installiert werden.

4. Funktionsweise und Einbindung in die Infrastruktur

NoSpamProxy arbeitet in Ihrer Umgebung mit den anderen Komponenten Ihrer Infrastruktur zusammen ([Bild 1](#)).

Alle Komponenten des Systems können auf demselben Server betrieben werden. NoSpamProxy kann in kleinen Umgebungen zusammen mit einer Firewall und Ihrem E-Mail-Server auf einem einzigen Server installiert werden. Zusätzlich zu den einzelnen Komponenten sind auch die TCP Ports dokumentiert, die zwischen den Komponenten verwendet werden ([Bild 2](#)).

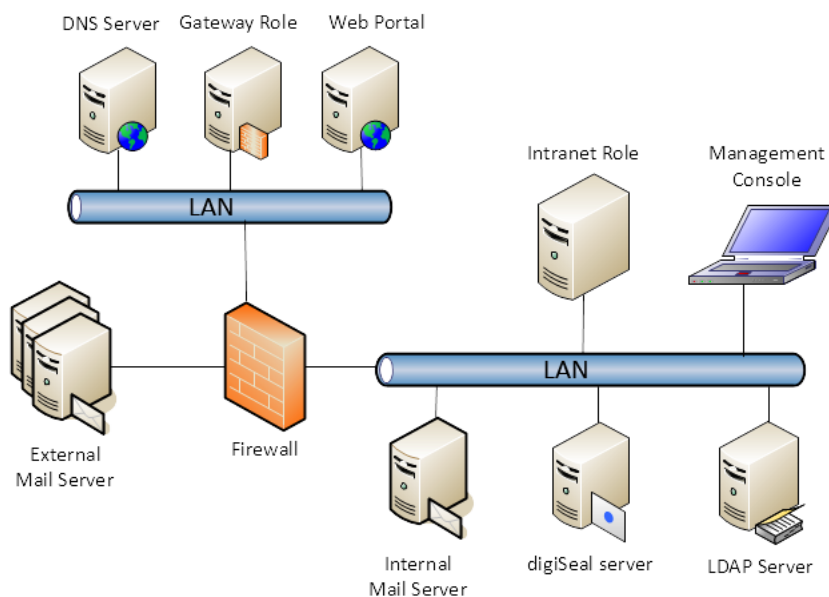


Bild 1: Komponenten von NoSpamProxy

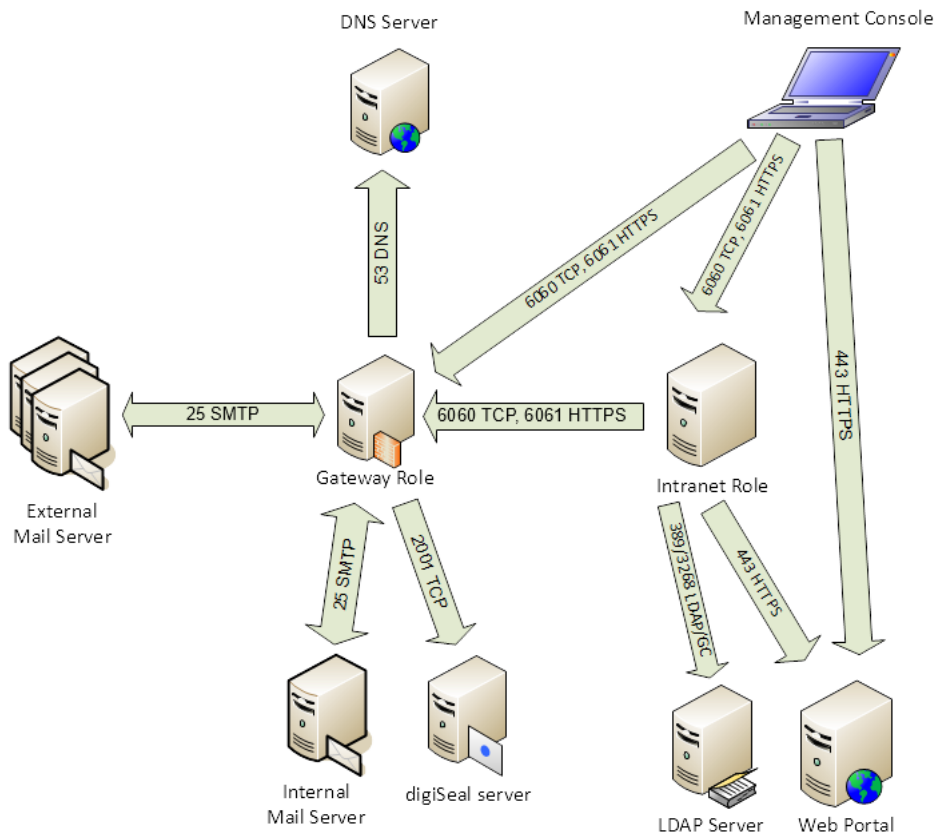


Bild 2: Kommunikation von NoSpamProxy untereinander und mit anderen Komponenten

Firewall

Für die Funktion von NoSpamProxy ist es erforderlich, dass das Netzwerk die nötigen Kommunikationsbeziehungen nicht verhindert. Dies ist im Wesentlichen das Protokoll SMTP auf Port 25/TCP und DNS auf Port 53 TCP/UDP. Sofern die Rollen von NoSpamProxy in unterschiedlichen Netzwerksegmenten installiert werden, muss auf der Firewall die Kommunikation für TCP auf Port 6060 und für HTTPS auf 6061 erlaubt werden. Sowohl die Management Konsole als auch die Intranet Rolle verwenden Port 443/HTTPS um auf das Web Portal zuzugreifen.

SMTP E-Mail-Server

Alle E-Mails an externe Adressen sollten auch über NoSpamProxy versandt werden, damit das Level-of-Trust-System die Kommunikationsbeziehungen Ihrer Organisation erlernen kann.

SQL-Datenbank

NoSpamProxy speichert die für den Betrieb benötigten Dateien in einer Microsoft SQL Datenbank. Er unterstützt dabei den Microsoft SQL Server 2008 oder neuer. Die kostenlose Express Edition kann ebenfalls verwendet werden.

Domain Name System (DNS)

Ihr System sollte über eine Domain Name System (DNS) Auflösung verfügen. Der DNS-Name, mit dem sich ein E-Mail-Server meldet, sollte zudem per DNS auflösbar ist. Meldet sich ein Server als "mail.netatwork.de", sollte er auch als "mail.netatwork.de" im DNS auflösbar sein. Ist er nicht auflösbar, dann ist der Domain-Name entweder falsch, was auf eine Fehlkonfiguration des DNS Servers hindeutet, oder der DNS Name ist nicht im DNS gepflegt.

Verzeichnisdienst, Active Directory

NoSpamProxy kann E-Mails an nicht existierende oder nicht berechtigte Empfänger schon beim Empfang ablehnen. Dazu muss im Gateway eine Liste der gültigen SMTP-Adressen gepflegt werden. Dies kann z.B. über einen automatischen Abgleich mit den Daten aus dem Active Directory oder Lotus Domino erfolgen. Wenn Sie dies nicht wünschen, können Sie die Benutzer auch manuell einpflegen.

Beispiele für die Implementierung

Prinzipielles zum Einsatz von NoSpamProxy

Ob die E-Mail von einem Provider oder direkt vom Absender kommt: NoSpamProxy ist noch vor dem ersten E-Mail-Server oder Relay des Empfängers positioniert.

Ist dies nicht der Fall, so kann in diesem Fall weder die IP-Adresse des einliefernden Gateways geprüft noch die Verbindung mit einer Fehlermeldung abgebrochen werden. Das einliefernde Gateway würde eine Unzustellbarkeitsnachricht versenden. Der wesentliche Vorteil von NoSpamProxy, E-Mails abzulehnen und Datenvolumen zu sparen, würde nicht greifen.

NoSpamProxy vorgeschaltet

Die einfachste Funktion ist die Vorschaltung von NoSpamProxy als eigenes System vor den eigenen E-Mail-Server ([Bild 3](#)).

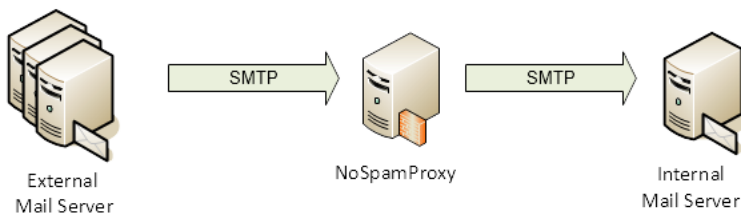


Bild 3: NoSpamProxy vor dem eigenen E-Mail-Server

NoSpamProxy auf dem E-Mail-Server

Für kleine Umgebungen ist es unter Umständen zu aufwändig, einen eigenen Server für NoSpamProxy zur Verfügung zu stellen. In diesem Fall kann das Gateway auf dem bestehenden E-Mail-Server installiert werden.

In diesem Fall ändern Sie die Konfiguration des bestehenden E-Mail-Servers wie folgt: Anstatt E-Mails auf Port 25 anzunehmen, konfigurieren Sie hierfür einen anderen Port (z.B. 2525). Anschließend konfigurieren Sie im NoSpamProxy einen Smarthost für E-Mails an lokale Adressen für Host 'localhost', Port '2525'.

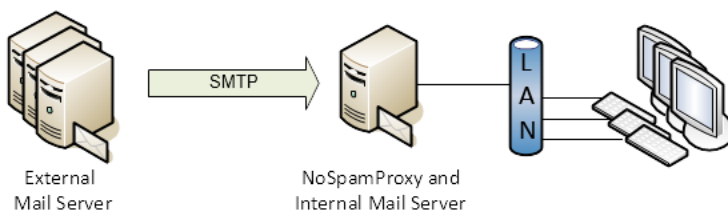


Bild 4: NoSpamProxy auf dem E-Mail-Server

NoSpamProxy nimmt nun die Verbindungen auf Port 25 an und leitet diese dann an den E-Mail-Server über 'localhost:2525' weiter.

NoSpamProxy mit NAT-Router

Wenn der Server selbst nicht über eine eigene offizielle IP-Adresse verfügt, dann ist ein System vor dem Server für die Umsetzung zuständig. Bei kleineren Installationen ist dies meist ein Router mit Network Address Translation (NAT).

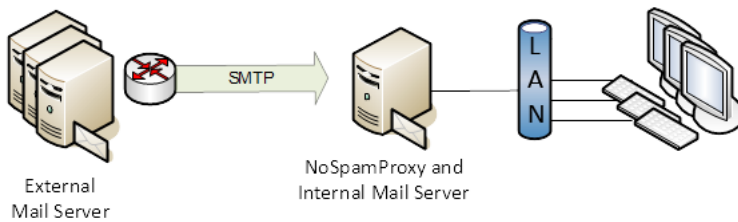


Bild 5: NoSpamProxy mit NAT Router

Diesen müssen Sie für den Einsatz mit NoSpamProxy so einstellen, dass er alle Verbindungen, die auf der offiziellen IP-Adresse an Port 25 empfangen werden, an NoSpamProxy weitergibt. Die Konfiguration von NoSpamProxy entspricht dabei einem der beiden vorherigen Beispiele.

NoSpamProxy mit Firewall und DMZ

Größere Installationen nutzen häufig eine mehrstufige Firewall oder eine so genannte "Demilitarisierte Zone" (DMZ), um den Datenverkehr zwischen den Systemen besser kontrollieren zu können.

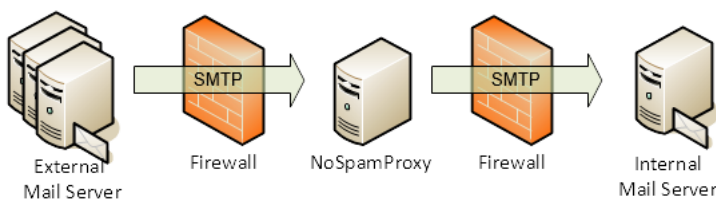


Bild 6: NoSpamProxy mit Firewall

In diesem Fall ist NoSpamProxy auf einem eigenen Server in der DMZ installiert. Die Firewall lässt Verbindungen von außen auf den Server (an Port 25 von NoSpamProxy) zu. Bei dieser Konstellation sollten Sie nur die Gateway Rolle in der DMZ installieren. Die Intranet Rolle sollten Sie im Intranet installieren.

NoSpamProxy und SMTP-Virenschanner

NoSpamProxy kann Viren auf mehrere Arten erkennen. Diese werden in der folgenden Liste beschrieben.

- **Cyren AntiSpam**
E-Mails können durch den Cyren AntiSpam Dienst auf Viren und Malware überprüft werden. Dieser Dienst wird zusammen mit NoSpamProxy installiert.
- **On-Access-Virenschanner auf dem NoSpamProxy Server**

Ein zusätzlich auf NoSpamProxy installierter Virens Scanner kann E-Mails mit Hilfe der Aktion [Dateibasierter Virens Scanner](#) überprüfen.

- **SMTP-Virens Scanner als SMTP-Relay**

Ein SMTP-Virens Scanner arbeitet in der Regel als SMTP-Relay und muss deshalb zwischen NoSpamProxy und Ihrem Intranet installiert werden

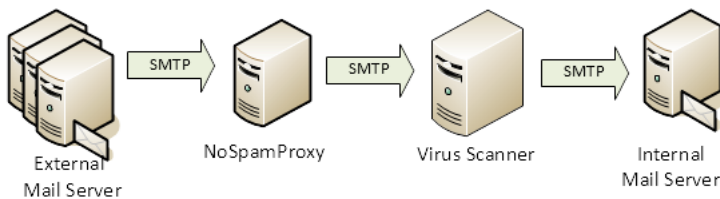


Bild 7: NoSpamProxy mit Virens Scanner



Ein SMTP-Virens Scanner arbeitet in der Regel als SMTP-Relay und darf daher nicht zwischen Internet und NoSpamProxy eingebunden werden.

Installation der Rollen auf unterschiedlichen Servern

In sehr kleinen Umgebungen empfiehlt es sich, alle Rollen auf einem Server zu installieren. Auch auf einem Small Business Server läuft NoSpamProxy ohne Einschränkungen.

In größeren Umgebungen mit einer DMZ könnte eine mögliche Verteilung der Rollen wie im folgenden Diagramm aussehen ([Bild 8](#)).

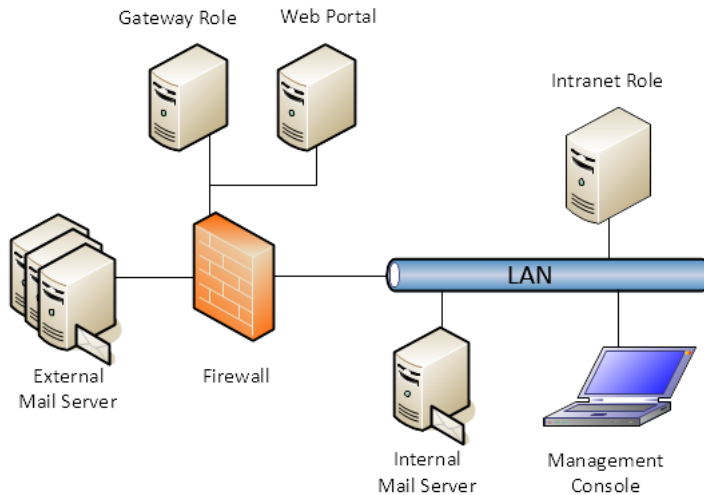


Bild 8: Installation von NoSpamProxy in der DMZ

In der Demilitarisierten Zone (DMZ) steht ein Server mit der installierten Gateway Rolle. Hier werden die E-Mails verarbeitet, gefiltert und anschließend an den internen E-Mail-Server weitergeleitet. Im LAN könnte dann ein Server laufen, auf dem die Intranet Rolle installiert sind - was die Sicherheit erhöht. Auf der Firewall müssen für den Datentransfer zwischen der Gateway Rolle und den anderen beiden Rollen lediglich der Port 6060 für TCP und Port 6061 für HTTPS aus dem LAN in die DMZ geöffnet werden. Die einzige zwingende Verbindung aus der DMZ in das LAN ist der Port 25 für die E-Mail-Kommunikation.

In größeren Umgebungen mit hohem E-Mail-Aufkommen haben Sie die Möglichkeit, in der DMZ mehrere Server mit der Gateway Rolle zu installieren. Hiermit ist es möglich, ein hochverfügbares System aufzubauen. Auf dem PC des Administrators kann man die NoSpamProxy-Verwaltungskonsole installieren und damit alle anderen Rollen im LAN und in der DMZ zentral verwalten ([Bild 9](#)).

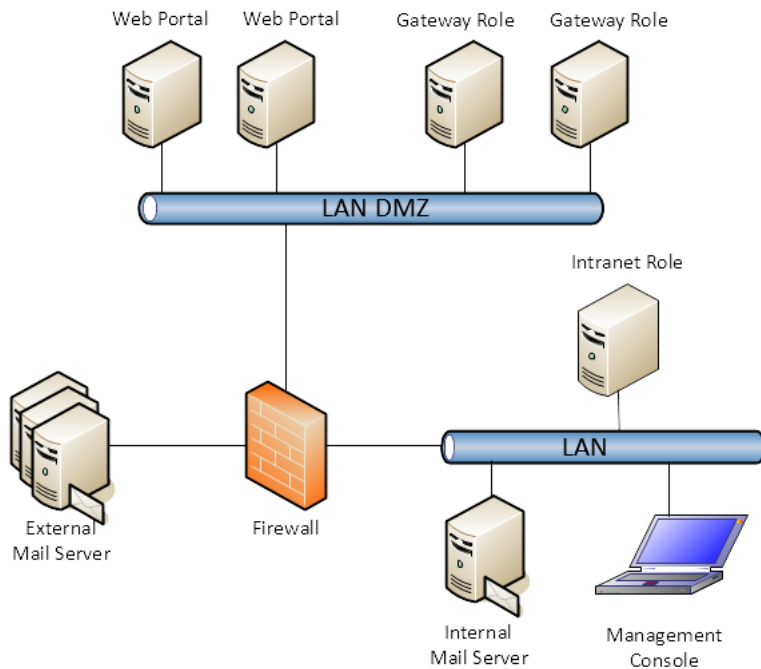


Bild 9: Rollen von NoSpamProxy auf verteilten Servern

Negativbeispiel: Falsche Konfiguration

Zur Verdeutlichung zeigt dieses Bild eine nicht zulässige Installation.

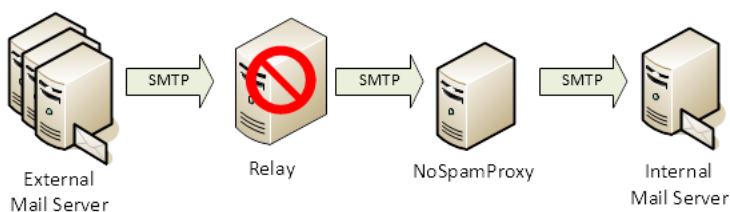


Bild 10: Falsche Konfiguration - NoSpamProxy kann nicht funktionieren

Wie bereits angesprochen: Eine E-Mail wird durch das Relay schon komplett empfangen, bevor sie an NoSpamProxy gesendet wird. Resultat: NoSpamProxy kann nicht sinnvoll arbeiten. Weder wird Datenvolumen eingespart, noch kann NoSpamProxy eine bestehende Verbindung abbrechen. Es wäre auch unmöglich, die IP-Adresse des einliefernden Gateways zu prüfen.

E-Mails an externe Adressen

Der Erfolg des Level-of-Trust-Systems hängt im großen Maß davon ab, dass E-Mails an externe Adressen über NoSpamProxy versandt werden.

NoSpamProxy kann sich bei E-Mails an externe Adressen eines Smarthosts bedienen oder die E-Mails direkt zustellen. Wenn Sie über einen Smarthost versenden, können Sie zum Beispiel den Smarthost Ihres Providers oder auch ein speziell für diesen Zweck installiertes Mail-Relay nutzen.



Wenn Sie nicht über eine statische IP-Adresse verfügen, dann sollten Sie E-Mails an externe Adressen über Ihren Provider schicken. Dynamische IP-Adressen werden von vielen Firmen und E-Mail-Providern kategorisch abgelehnt.

5. NoSpamProxy Verwaltungskontrolle

NoSpamProxy wird über eine Microsoft Management Console (MMC) verwaltet. Die Installation der Oberfläche wird in der [NoSpamProxy Installationsanleitung](#) beschrieben. Bitte beachten Sie die Hinweise in diesem Handbuch vor dem Inbetriebnehmen von NoSpamProxy.

Die Verwaltungskontrolle von NoSpamProxy gliedert sich in folgenden Bereiche:

- **Die Übersichtsseite**
Unter dem obersten Knoten der Verwaltungskontrolle mit dem Namen **NoSpamProxy** liegt die [Übersichtsseite](#). Sie bietet einen schnellen Überblick über das gesamte Gateway mit allen verbundenen Rollen. Sie können außerdem auf dieser Seite auch verschiedene Aktionen starten, die im Kapitel der Übersichtsseite beschrieben werden.
- **Monitoring**
Das **Monitoring** bietet eine Übersicht über den Empfang und die Zustellung von E-Mails. Zusätzlich können Sie die Ereignisanzeige von allen verbundenen Rollen einsehen.
- **Menschen und Identitäten**
Der Bereich **Menschen und Identitäten** verwaltet Ihre eigenen Domänen und Unternehmensbenutzer aber auch externe Kommunikationspartner. Sie können für diese Identitäten Einstellungen zu Vertrauen und Sicherheit festlegen.
- **Konfiguration**
Die Knoten unter **Konfiguration** dienen der Einstellung von NoSpamProxy. Hier definieren Sie Sende- und Empfangskonnektoren für E-Mails, Ihre Regeln und Benachrichtigungen aber auch die Verbindungen zu Komponenten von NoSpamProxy oder Drittanbieterkomponenten.
- **Troubleshooting**
Zur Diagnose von NoSpamProxy steht Ihnen der Bereich **Troubleshooting** zur Verfügung. Erstellen Sie Log-Dateien der einzelnen NoSpamProxy Komponenten oder lassen Sie Einstellungen automatisch korrigieren.

Sprache der Oberfläche ändern

Die Oberfläche von NoSpamProxy ist standardmäßig auf die Systemsprache eingestellt. Wenn Sie die Sprache ändern möchten, klicken Sie auf den Knoten **NoSpamProxy** und wählen Sie im Menü **Aktion / Sprache ändern** bzw. **Action / Change language**. Alternativ können Sie diese Funktion durch einen Rechtsklick auf dem Knoten **NoSpamProxy** anwählen. Damit die Änderung wirksam wird, müssen Sie die Oberfläche schließen und neu starten.

Verbindung zur Intranet Rolle herstellen

Die Verbindung der Management Konsole zur Intranet Rolle steht nach der Installation auf `localhost`. Bei einer Installation der Konsole auf einem anderen Rechner als der Rechner der Intranet Rolle müssen Sie die Verbindung anpassen. Bitte wählen Sie dazu im Menü **Aktion / Server ändern** bzw. **Action / Change server**. Geben Sie hier den Namen des Servers (zum Beispiel: "mail.example.com") und den Port (normalerweise "6060") ein. Alternativ können Sie auch diese Funktion durch einen Rechtsklick auf dem Knoten **NoSpamProxy** anwählen. Damit die Änderung wirksam wird, müssen Sie die Oberfläche schließen und neu starten.



Falls das Gateway in einer DMZ betrieben wird und Sie aus dem LAN mit der NoSpamProxy MMC den Dienst fernsteuern möchten, müssen Sie auf der Firewall lediglich den TCP-Port 6060 und für HTTPS den Port 6061 freischalten. Diese Verbindung ist zertifikatsbasierend verschlüsselt.

6. Übersichtsseite

Die Seite unter dem Knoten **NoSpamProxy** ([Bild 11](#)) dient Ihrem schnellen Überblick. Sie erhalten hier eine Übersicht über den Status der installierten Rollen.

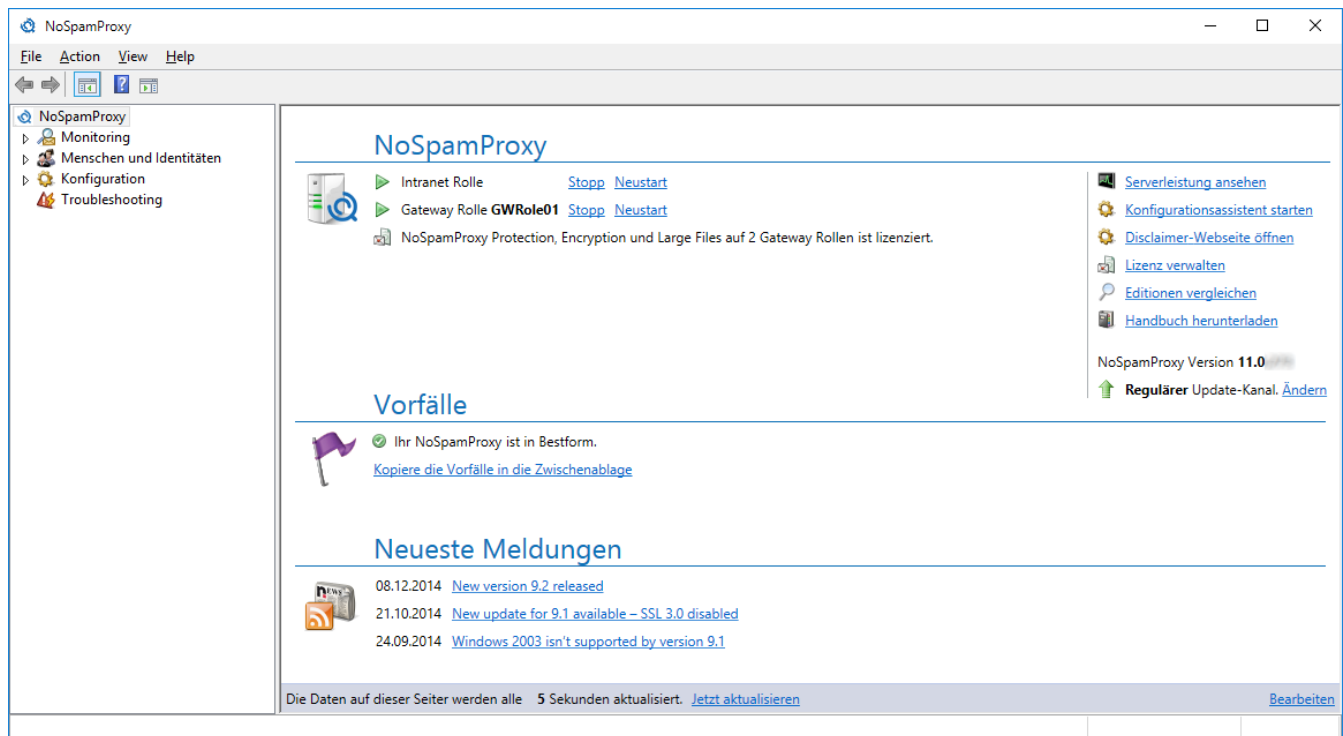


Bild 11: Die Übersicht über die Konfiguration der Gateway Rolle

Bei der ersten Inbetriebnahme ist NoSpamProxy weitgehend unkonfiguriert. Die fehlenden Konfigurationsoptionen erscheinen in der Liste **Vorfälle**. Statt jeden Vorfall einzeln abzuarbeiten, empfehlen wir die Verwendung des [Konfigurationsassistenten](#). Der Assistent unterstützt Sie bei der schnellen und vollständigen Inbetriebnahme von NoSpamProxy in den meisten Umgebungen. Er ermittelt und erstellt anhand der lizenzierten Funktionen in Ihrer Lizenz die empfohlene Konfiguration.

Liste der Rollen

Direkt unter der Überschrift **NoSpamProxy** werden alle verbunden Rollen aufgeführt. Die Liste zeigt für jede Rolle an, ob Sie gestartet oder gestoppt ist. Zusätzlich können Sie die Rollen auch manuell starten, stoppen und neu starten. Unter der Liste wird nach dem Einspielen der Lizenz eine Zusammenfassung derselben angezeigt.

Bereich für Aktionen

In der rechten oberen Ecke werden die derzeit möglichen Aktionen angezeigt. Die Aktion **Disclaimer-Webseite öffnen** führt Sie zu den Vorlagen und Regeln für die [Disclaimer](#). Unter der Liste mit den Aktionen finden Sie die momentan installierte Version von NoSpamProxy.

Serverleistung ansehen

Die Aktion **Serverleistung ansehen** gibt Ihnen einen schnellen Überblick über die aktuelle Verarbeitung von E-Mails und die derzeit zu Verfügung stehenden Ressourcen.

Datenverkehr

Die Seite **Datenverkehr** zeigt einen gleitenden Durchschnitt der verarbeiteten E-Mails der letzten Minute bzw. Stunde. Die Seite wird automatisch aktualisiert und zeigt Ihnen zudem, ob NoSpamProxy aktuell E-Mails empfängt ([Bild 12](#)).

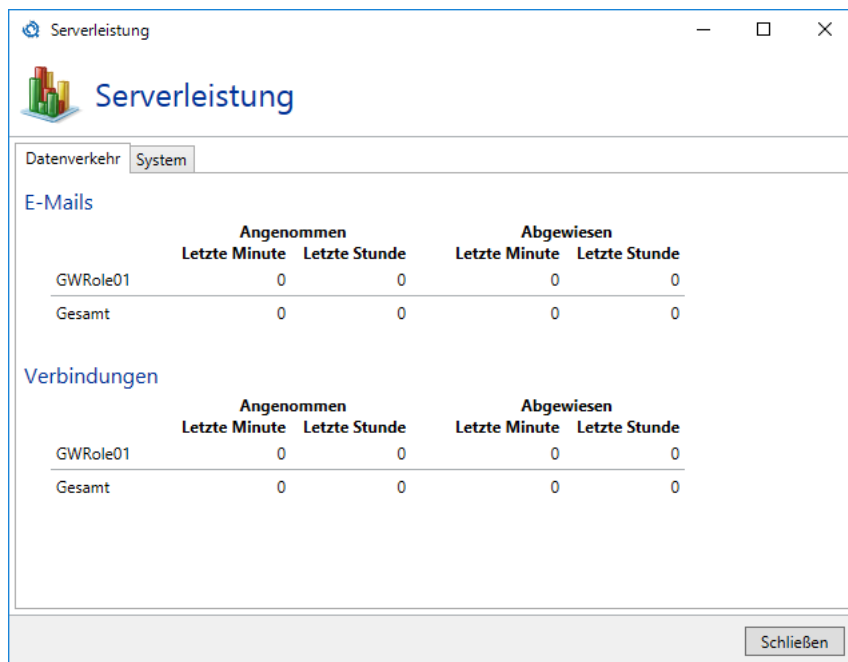


Bild 12: Die aktuell verarbeiteten Nachrichten

System

Die Seite **System** zeigt für jedes System mit Intranet oder Gateway Rollen die installierten Dienste, deren Status und die verwendeten Ressourcen ([Bild 12](#)).

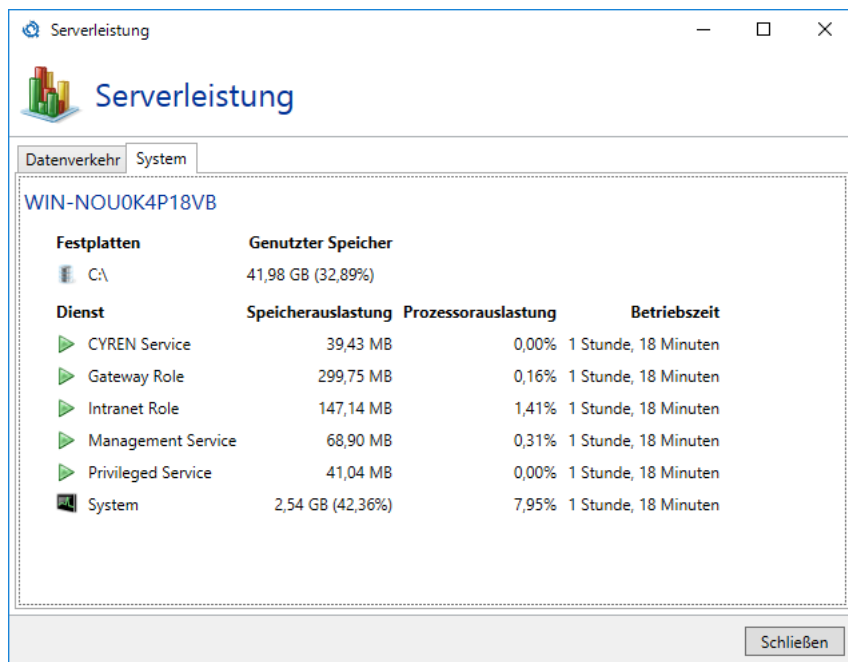


Bild 13: Die aktuell verwendeten und die zur Verfügung stehenden Ressourcen

Zusätzlich zu dieser Ansicht stehen Ihnen auf dem Server außerdem die [Leistungsindikatoren](#) zur Verfügung.

Konfigurationsassistent starten

Der **Konfigurationsassistent** führt Sie durch alle wesentlichen Schritte der NoSpamProxy Konfiguration:

- **Lizenz**
Spielen Sie eine Lizenz ein oder ändern Sie die bestehende [Lizenz](#). Falls Sie noch keine Regeln erstellt haben, können Sie in Abhängigkeit von Ihren lizenzierten Funktionen die passenden [Standardregeln](#) erstellen lassen.
- **Verbindung zur Gateway Rolle**
Wenn noch keine Gateway Rolle verbunden wurde, können Sie hier Ihre [Gateway Rolle verbinden](#). Legen Sie nach dem Hinzufügen der Rolle den DNS Namen für die [Server-Identität](#) dieser Gateway Rolle fest.
- **Eigene Domänen**
Konfiguration der [eigenen Domänen](#). Falls das Gateway beim Ausführen des Assistenten noch keine eigenen Domänen eingetragen hat, wird in diesem Schritt die primäre Domäne der Lizenz in die Liste der eigenen Domänen eingefügt.
- **Lokale E-Mail-Server**
Konfiguration der [lokalen E-Mail-Server](#).
- **Lokale Zustellung**
Konfiguration der [Zustellung](#) von E-Mails an lokalen E-Mail-Server.

- **Externe Zustellung**
Konfiguration der [Zustellung](#) von E-Mails an externe E-Mail-Server.
- **Administrative Benachrichtigungsadressen**
Konfigurieren Sie die [administrativen E-Mail-Adressen](#).
- **Schutz sensibler Daten**
Legen Sie ein Passwort zum [Schutz sensibler Daten](#) fest.

Führen Sie nach Abschluss des Assistenten eine Kontrolle durch:

- Kontrollieren Sie die Konfiguration der [Empfangskonnektoren](#).

Die Durchführung dieser Schritte stellt die Funktion von NoSpamProxy sicher.

Handbuch herunterladen

Über diese Aktion laden Sie das aktuelle Benutzerhandbuch herunter. Wenn Sie bereits Ihre Lizenz in NoSpamProxy eingespielt haben, wird die für Ihre Lizenz passende Version des Handbuchs heruntergeladen.

Lizenz verwalten

Die Aktion öffnet den Dialog für die derzeit verwendete Lizenz. Er zeigt Ihnen alle relevanten Daten Ihrer Lizenz und warnt Sie, falls Probleme mit der Lizenz auftreten ([Bild 14](#)).

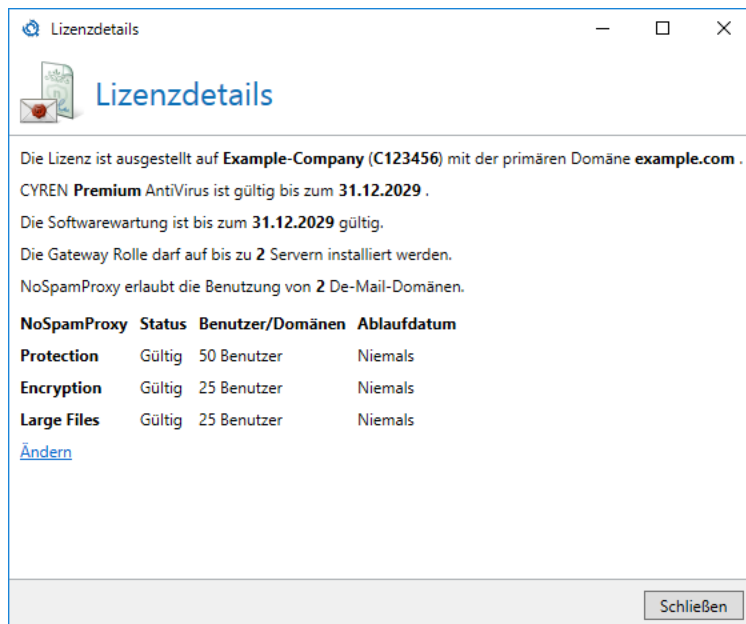


Bild 14: Die derzeit eingespielte Lizenz

Sie sehen hier Ihre C-Nummer, Domäne sowie alle lizenzierten Funktionen und deren Gültigkeitszeitraum. Durch den Link **Ändern** können Sie eine andere Lizenz-Datei laden und in

NoSpamProxy verwenden, soweit das Ablaufdatum der Softwarewartung noch mindestens genau so weit oder weiter in der Zukunft liegt, wie bei der derzeit verwendeten Lizenz.

Editionen vergleichen

Der Link öffnet die Seite mit dem [Vergleich der Lizenz-Features](#). Jedes Feature wird hier kurz erklärt.

Update herunterladen

Falls auf dem Server von Net at Work eine neuere Version von NoSpamProxy veröffentlicht wurde, wird diese Aktion eingeblendet. Sie laden damit die Installationsdatei von NoSpamProxy herunter. Die Installation können Sie im Nachhinein manuell anstoßen.

Auswahl des Update-Kanals

Updates für NoSpamProxy werden über zwei Update-Kanäle angeboten. Den **regulären Kanal** und den **schnellen Kanal** ([Bild 15](#)). Der reguläre Kanal ist die Standardeinstellung und bietet Aktualisierungen an, die bereits lange getestet wurden und die höchste Stabilität für NoSpamProxy erreichen. Der schnelle Kanal bietet Aktualisierungen früher an, diese haben ebenfalls alle automatischen Tests bestanden und wurden auch bereits erfolgreich installiert, haben aber kürzere Testzyklen in realen Umgebungen absolviert.

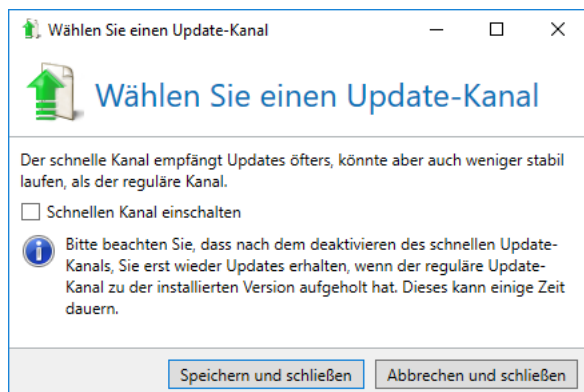


Bild 15: Einstellungen für den Update-Kanal



Falls Sie vom schnellen auf den regulären Update-Kanal wechseln, erhalten Sie erst wieder Updates, wenn die zur Aktualisierung angebotene Version eine höhere Versionsnummer als die bereits installierte hat. Dieses kann einige Zeit dauern.

Vorfälle

Die Liste der **Vorfälle** zeigt Ihnen fehlende oder fehlerhafte Einstellungen an (soweit vorhanden).

Neueste Meldungen

Diese Meldungen weisen Sie auf Produktaktualisierungen oder allgemeine Verbesserungsvorschläge für die Konfiguration von NoSpamProxy hin. Durch einen Klick auf die Überschriften können Sie den dazu passenden Artikel im NoSpamProxy-Blog lesen.

7. Monitoring

Die Knoten unterhalb von Monitoring ([Bild 16](#)) informieren Sie über den Empfang und Versand Ihrer E-Mails. Außerdem werden Status-Informationen über das System und den E-Mail-Verkehr angezeigt.

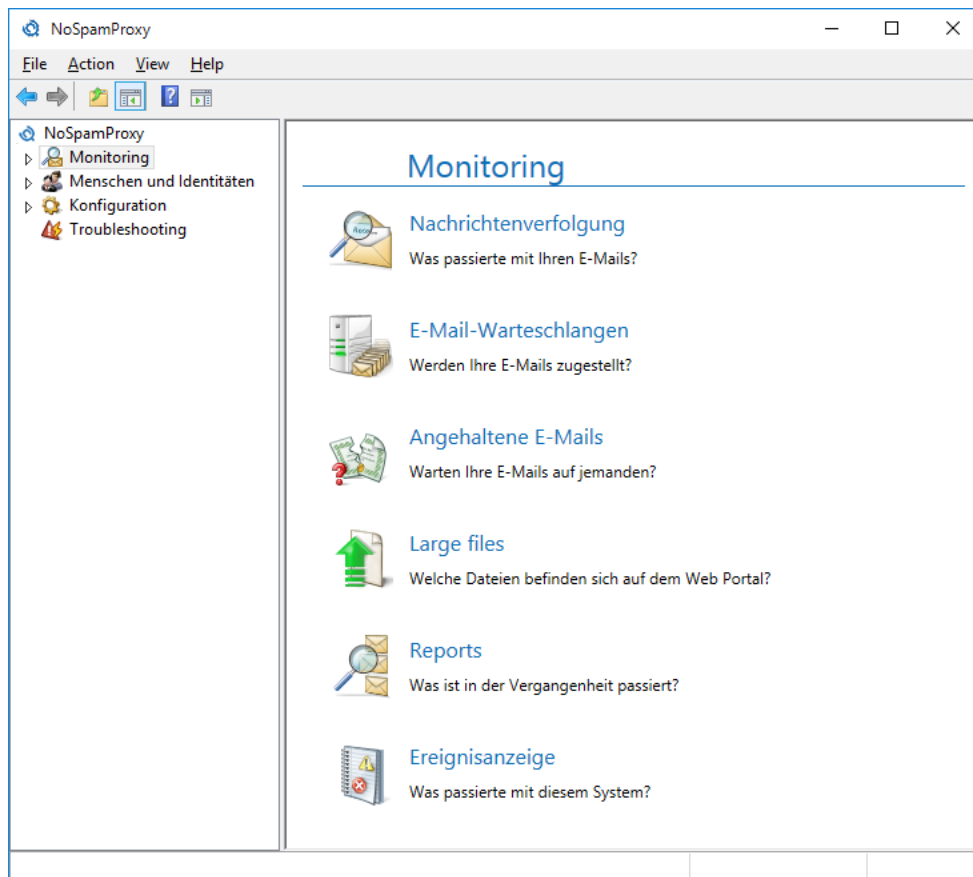


Bild 16: Übersicht über die Bereiche des Monitoring

Nachrichtenverfolgung

Die Nachrichtenverfolgung erlaubt Ihnen nachzuvollziehen, wann welche E-Mails geblockt oder durchgelassen wurden ([Bild 17](#)). Die Suche können Sie nach bestimmten Absender- und Empfängerkriterien, dem Betreff sowie nach konkreten Zeitintervallen und dem "E-Mail-Status" festlegen.

Ferner können Sie detaillierte Informationen darüber einsehen, wie die E-Mail verarbeitet wurde. So können Sie das Vorgehen von NoSpamProxy und das Funktionieren der Regeln leicht nachvollziehen.

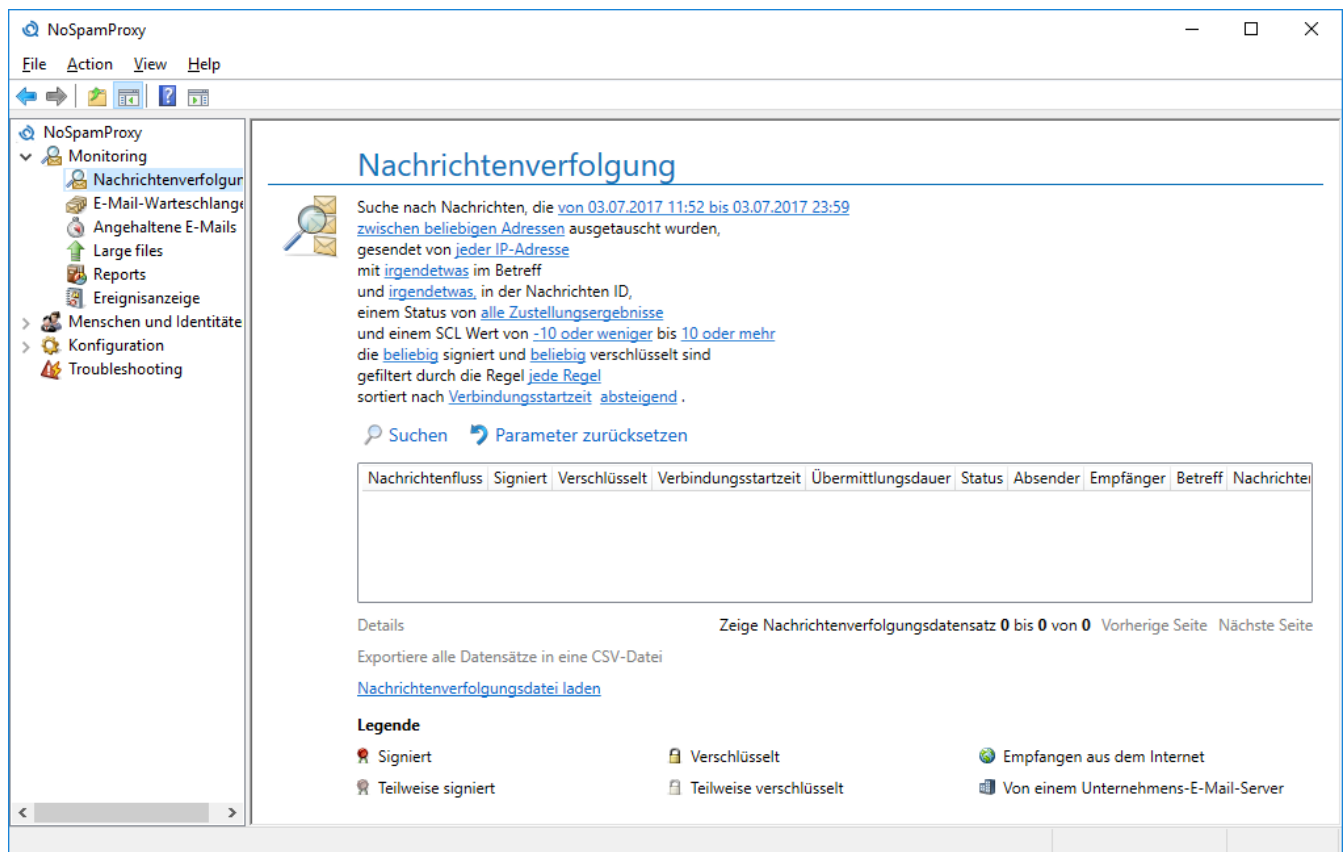


Bild 17: Die Suche der Nachrichtenverfolgungsdatensätze

Suchkriterien helfen Ihnen dabei, E-Mails nachzuverfolgen. Diese Suchkriterien können Sie einzeln oder kombiniert anwenden. Ein Zeitraum, in dem die E-Mail oder die E-Mails eintrafen, muss jedoch in jedem Fall angegeben werden. Standardmäßig wird die Startzeit auf die aktuelle Systemzeit - 1 Stunde und die Endzeit auf heute um 23:59 Uhr gesetzt.

Bei der Suche können Sie auf die folgenden Eigenschaften filtern. Bei der Eingabe von Text können Sie immer den gesamten zu suchenden Text oder Teile davon eingeben.

- Versandzeitraum: Durch die Auswahl unter **Zeiträume** können oft benötigte Suchen schnell gewählt werden.
- Absender- und Empfängeradresse: die E-Mail-Adressen der Kommunikationspartner. Es kann auf lokale und externe Adressen gefiltert werden. Die Suche kann für exakte Treffer ausgeführt werden oder für Bestandteile von Adressen. Die Suche nach exakten Treffern wird wesentlich schneller durchgeführt.
- Betreff: Der Inhalt der Betreffzeile.
- Nachrichten ID: Interne Kennung der E-Mail.
- Zustellergenergebnisse: Der Status der Zustellung.
- SCL Wert: Einschränkung auf den errechneten SCL Wert.

- Regel: Der Name der Regel, von der die Nachricht verarbeitet wurde.

In der Liste der Nachrichtenverfolgungsdatensätze erscheinen alle E-Mails, die den Suchkriterien entsprechen. Sie werden mit den Angaben **Richtung, Sicherheit, Verbindungsstartzeit, Übermittlungsdauer, Status, Absender, Empfänger, Betreff, Nachrichten-ID** und **Gateway Rolle** angezeigt.

Die neuesten E-Mails stehen oben in der Liste.

Die Details nachprüfen

In den Details werden Ihnen detaillierte Informationen über den Zustellstatus einer E-Mail dargestellt. Ob und wie eine E-Mail signiert bzw. verschlüsselt wurde, wird hier ebenfalls angezeigt.

Klicken Sie die den Datensatz an, dessen Details Sie einsehen möchten.

Wählen Sie jetzt die Aktion **Nachrichtendetails** oder führen Sie einen Doppelklick aus.

Es erscheint der Dialog **Nachrichtenverfolgung** ([Bild 18](#)). Vom Start bis zum Schließen der Verbindung finden Sie hier alle Bearbeitungsschritte und Details, auf Registerkarten verteilt, detailliert aufgeführt. Sie sehen auf einen Blick, ob die Verbindung verschlüsselt wurde und welches Zertifikat der SMTP-Server bzw. der SMTP-Client verwendet hat. Auf den weiteren Registerkarten werden Ihnen die Filterergebnisse und generelle Verarbeitungsfehler von NoSpamProxy angezeigt, so dass Sie jederzeit genau nachverfolgen können, ob etwas mit der E-Mail-Zustellung nicht ordnungsgemäß funktioniert.

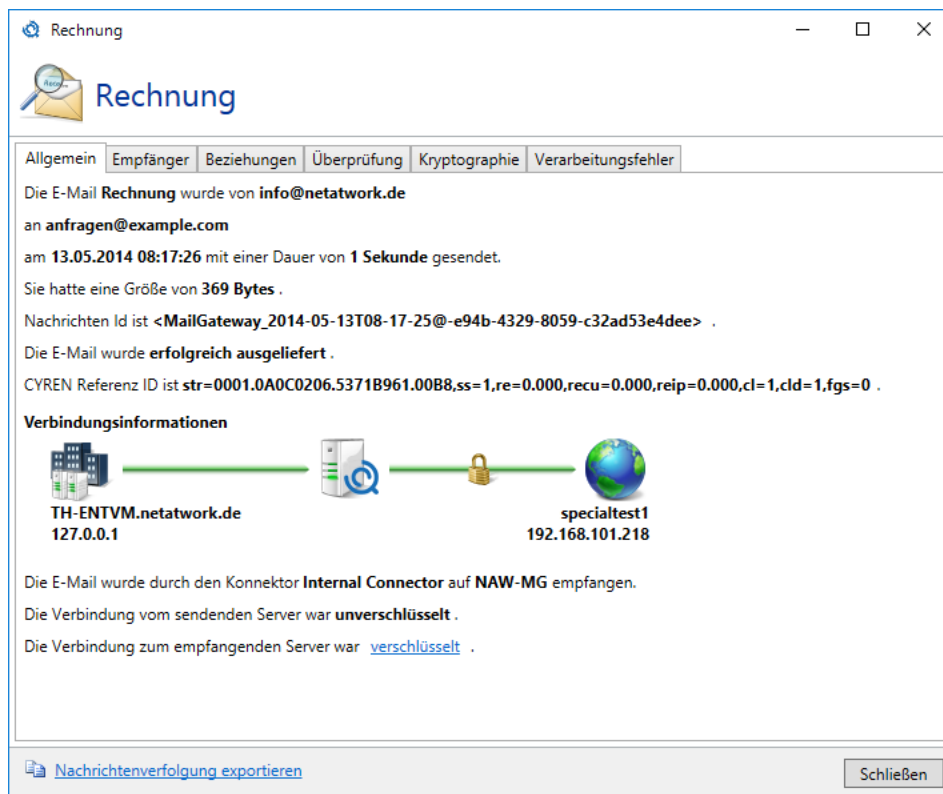


Bild 18: Das Ergebnis der E-Mail-Zustellung im Detail



Sie können die Datensätze der Nachrichtenverfolgung auch einfach auf Ihrer lokalen Festplatte abspeichern oder abgespeicherte Datensätze wieder mit allen Details anzeigen. Diese Funktion ist sehr hilfreich, falls man Unterstützung bei der Analyse eines Datensatzes benötigt. Für den Export wählen Sie den Link **Nachrichtenverfolgung exportieren** in der linken unteren Ecke des Detaildialogs. Um die Details wieder anzuzeigen wählen Sie den Link **Nachrichtenverfolgungsdatei laden** in der Liste aller gefundenen Datensätze.

E-Mail-Warteschlangen

E-Mails an externe Adressen werden Ihrer Domäne entsprechend in Warteschlangen gestellt. Pro Domäne gibt es eine Warteschlange. Unter dem Menüpunkt **Warteschlangenmanagement** werden Ihnen sämtliche aktiven E-Mail-Warteschlangen angezeigt ([Bild 19](#)). Hier können Sie auf einen Blick sehen, an welche Domänen noch E-Mails versendet werden müssen. Sie haben hier auch die Möglichkeit, gezielt die Übertragung an eine oder mehrere bestimmte Domänen anzuhalten.

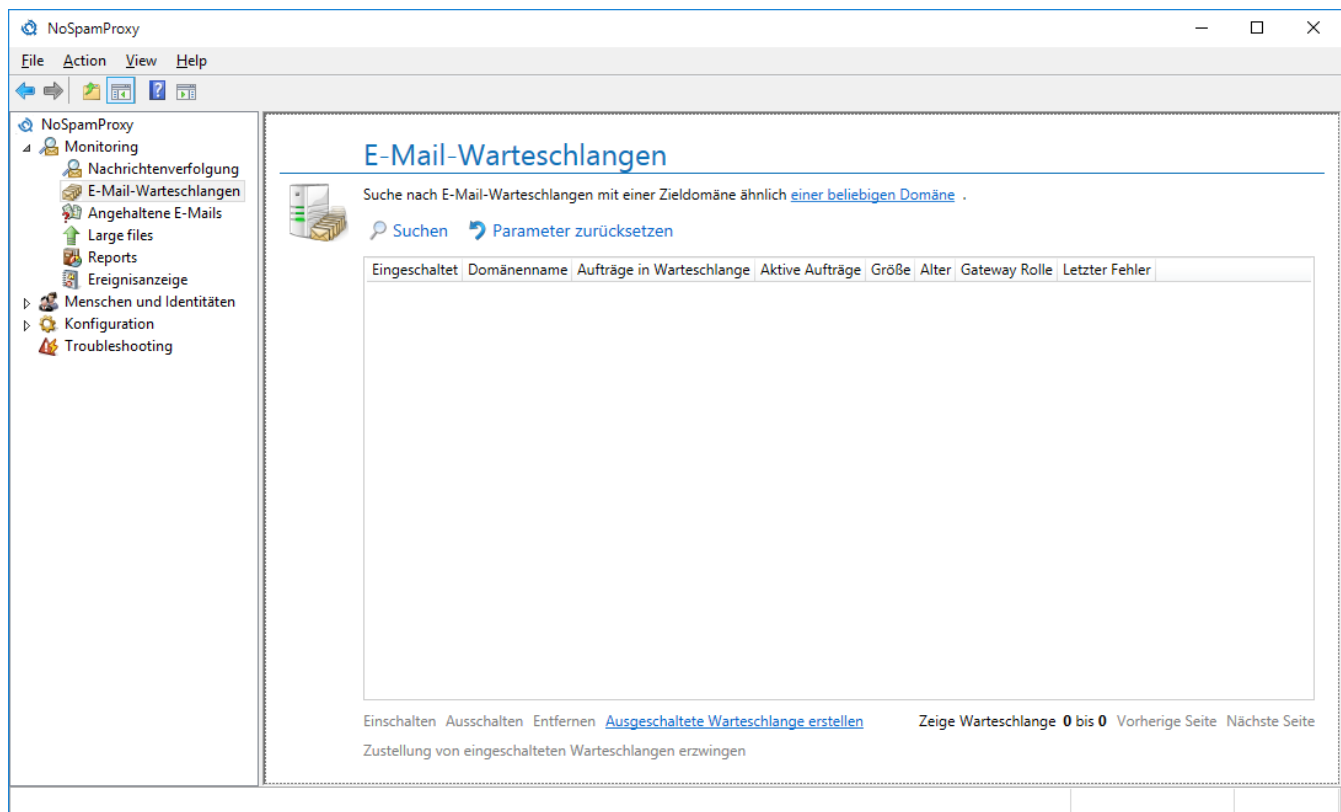


Bild 19: Alle unversendeten E-Mails befinden sich, gruppiert nach Domänenname, in Warteschlangen

Mit der Suche können Sie gezielt nach Warteschlangen suchen. Geben Sie dazu den Suchbegriff in das Suchfeld ein und klicken Sie auf **Suchen**, um die Suche zu starten. Es werden Ihnen dann alle Warteschlangen angezeigt, die dem Suchbegriff entsprechen.

Die Spalte **Eingeschaltet** zeigt an, ob derzeit für diese Domäne E-Mails zugestellt werden.

Der **Domänenname** entspricht dem Namen der Zieldomäne.

Die **Warteschlangenlänge** entspricht der Anzahl der wartenden E-Mails.

Die Spalte **Aktive Aufträge** zeigt die derzeit offenen SMTP-Verbindungen zur Zieldomäne. Dies ist besonders bei einem Massen-E-Mail-Versand interessant, in dem mehrere E-Mails an dieselbe Domäne gesendet werden.

Über die Aktion **Einschalten** und **Ausschalten** können Sie die Zustellung der E-Mails an die ausgewählten Domänen starten bzw. pausieren.

Sie können auch direkt eine ausgeschaltete Warteschlange erstellen, um die Verbindung zu einer bestimmten Domäne im Vorfeld zu unterbinden. Wählen Sie dazu **Ausgeschaltete Warteschlange erstellen**. Es öffnet sich der Dialog (Bild 20).

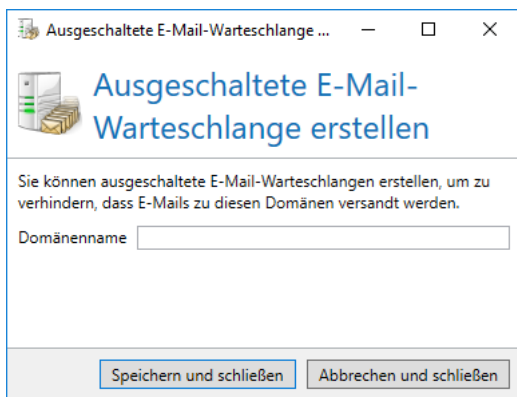


Bild 20: Erstellen einer "Ausgeschalteten Warteschlange"

Geben Sie unter **Domänenname für Warteschlange** den Domännennamen an (z.B. "netatwork.de") und speichern Sie danach die Einstellung, um die deaktivierte Warteschlange zu erstellen. Es werden danach alle E-Mails an "netatwork.de" in den Warteschlangen von NoSpamProxy pausiert, bis Sie die Warteschlange wieder aktivieren.

Eine Warteschlange kann auch gelöscht werden. Sie können beim Löschen entscheiden ob ein Nichtzustellbarkeitsbericht (NDR) gesendet wird oder nicht.

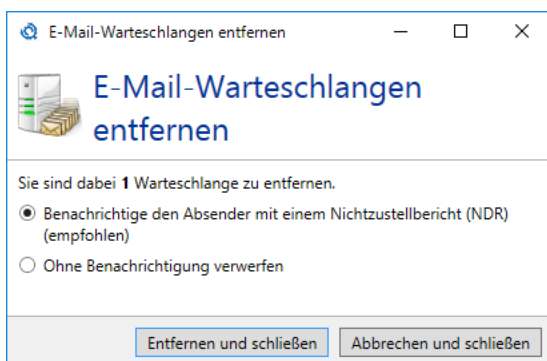


Bild 21: Entfernen von Warteschlangen

Angehaltene E-Mails



Wenn Sie NoSpamProxy Protection ohne NoSpamProxy Encryption verwenden, wird der Knoten nur eingeblendet, wenn auch Large Files lizenziert sind.

Unter bestimmten Bedingungen können E-Mails auch angehalten werden. Das bedeutet, dass bis auf weiteres die E-Mail weder zugestellt noch abgelehnt wird, sondern auf das Eintreffen bestimmter

Bedingungen wartet. Angehaltene E-Mails entstehen bei fehlenden kryptographischen Schlüsseln, Vorfällen durch Dateianhänge und bei Vorfällen der qualifizierten Signatur oder De-Mail. Im Knoten 'Angehaltene E-Mails' werden all diese E-Mails aufgelistet ([Bild 22](#)).

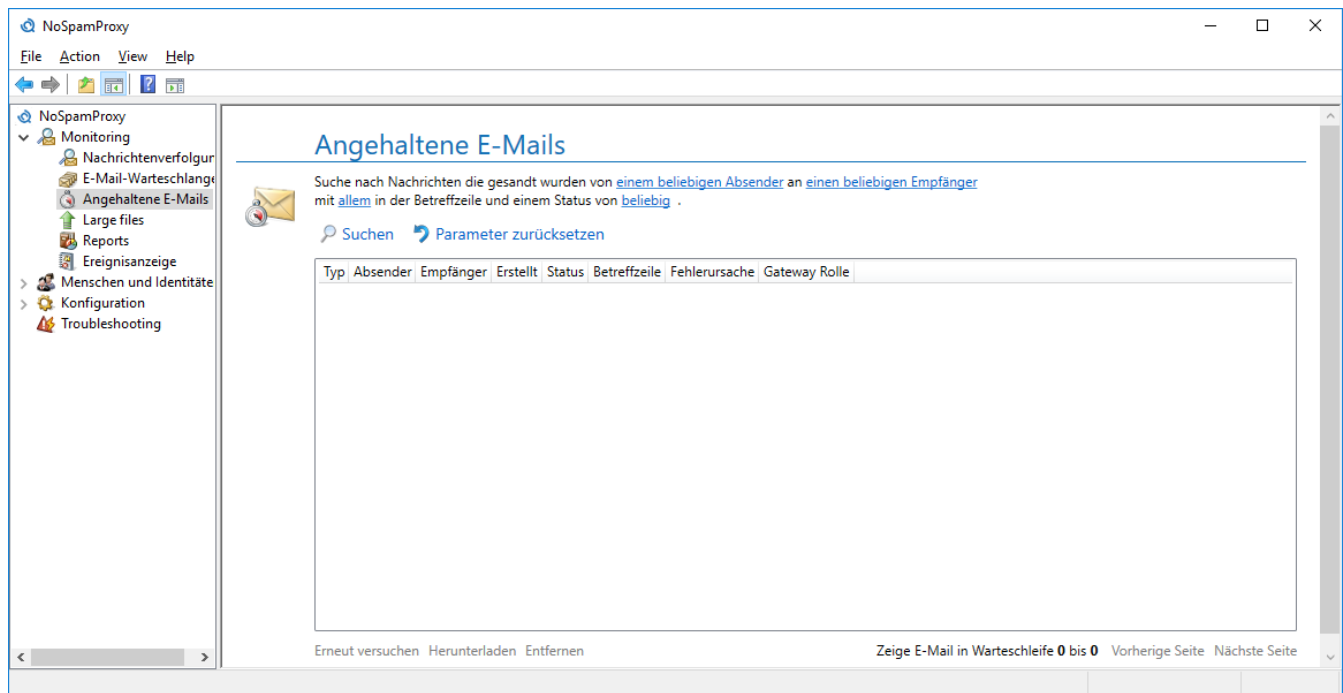


Bild 22: Die Liste aller angehaltenen E-Mails

Sie können angehaltene E-Mails suchen und filtern. Als Filter stehen Ihnen die Richtung, die Absender- und Empfängeradresse, die Betreffzeile und der Status der E-Mail zur Verfügung. Für die Adressen und Betreffzeile müssen nur Teile des zu suchenden Textes eingegeben werden. Es wird automatisch nach allen Adressen und Betreffzeilen gesucht, in denen die angegebenen Teile auftauchen.

Wenn Sie Large Files lizenziert haben, werden Dateien, bei denen das Hochladen fehlschlug, hier in der Liste angezeigt.

Sie können eine erneute Verarbeitung von markierten E-Mails durch einen Klick auf **Erneut versuchen** veranlassen. Sollten erneut Vorfälle auftreten, werden die betroffenen E-Mails erneut in die Liste eingetragen.

Sie können die vollständige E-Mail mit allen zugehörigen Dokumenten auch auf dem Computer, auf dem die Benutzeroberfläche läuft, herunterladen und abspeichern. Markieren Sie dazu einen Vorfall und wählen Sie dann **Herunterladen**.

Des Weiteren können Sie angehaltene E-Mails löschen. Dabei können Sie wählen, ob der Absender hierüber benachrichtigt wird, oder nicht.

Large files



Der Knoten ist verfügbar sofern Large Files lizenziert ist.

Der Abschnitt **Dateien auf dem Web Portal** ([Bild 23](#)) zeigt alle Dateien, die derzeit auf dem Web Portal gespeichert sind. Sie können an dieser Stelle Dateien löschen, die nicht mehr benötigt werden. Dateien, die die Freigabe eines Administrators benötigen, können zum Herunterladen freigegeben werden. Noch nicht freigegebene Dateien können hier vom Administrator heruntergeladen werden, um deren Inhalt zu überprüfen, falls Sie als **Untersuchbar** in der Liste markiert sind. Untersuchbare Dateien können über die Funktion **Erneut prüfen** auf Malware untersucht werden. Wird Malware gefunden, wird die Datei gelöscht und der Empfänger über das Ergebnis informiert. Die Spalte **Malware Überprüfung** zeigt den Zeitpunkt der letzten Überprüfung an.

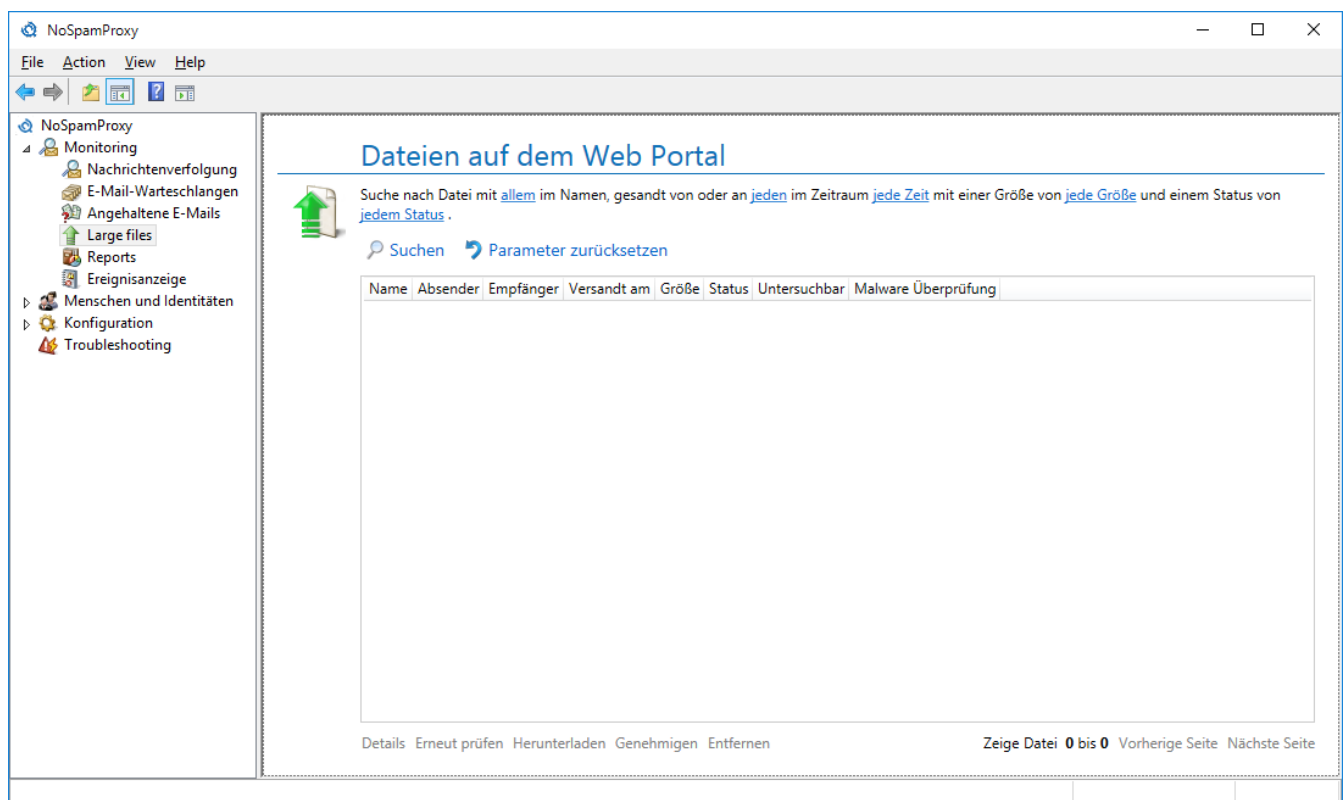


Bild 23: Die Dateien auf dem Web Portal

Bei der Suche können Sie auf die folgenden Eigenschaften filtern.

- **Dateiname**
Geben sie den Dateinamen oder Teile davon an.

- **Absender oder Empfängeradresse**

Geben Sie eine E-Mail-Adresse oder Teile davon an. In der Übersicht wird bei den Empfängeradressen nur die erste Empfängeradresse angezeigt, es wird aber nach allen Adressen gesucht.

- **Versandzeitraum**

Der Zeitraum kann eingeschränkt werden. Wenn er offen bleiben soll, deaktivieren Sie die Kontrollkästchen vor **Von** und **Bis**. Durch die Auswahl unter **Zeiträume** können oft benötigte Suchen schnell gewählt werden.

- **Dateigröße**

Schränken Sie die Dateigröße über die Schieberegler ein. Deaktivieren Sie die Einschränkung durch die Kontrollkästchen vor den Schieberegler.

- **Status**

Wählen Sie hier alle Dateien oder Dateien mit bestimmten Eigenschaften, wie z.B. niemals, teilweise und von allen Empfängern heruntergeladen. Es kann auch nach Dateien gesucht werden, die noch nicht genehmigt wurden oder bei denen Fehler während des Malwarescans auftraten.

Der Link **Details** zeigt weitere Empfänger an sowie eventuell aufgetretene Probleme während des Malwarescans.

Reports

Die Reports von NoSpamProxy geben Ihnen einen Überblick über den Verlauf Ihres E-Mail-Verkehrs ([Bild 24](#)). Mit wenigen Mausklicks sehen Sie, wie sich das Spam-Aufkommen über die Monate verändert hat und welche E-Mail-Adressen bzw. Domänen das höchste Spam-Aufkommen hatten.

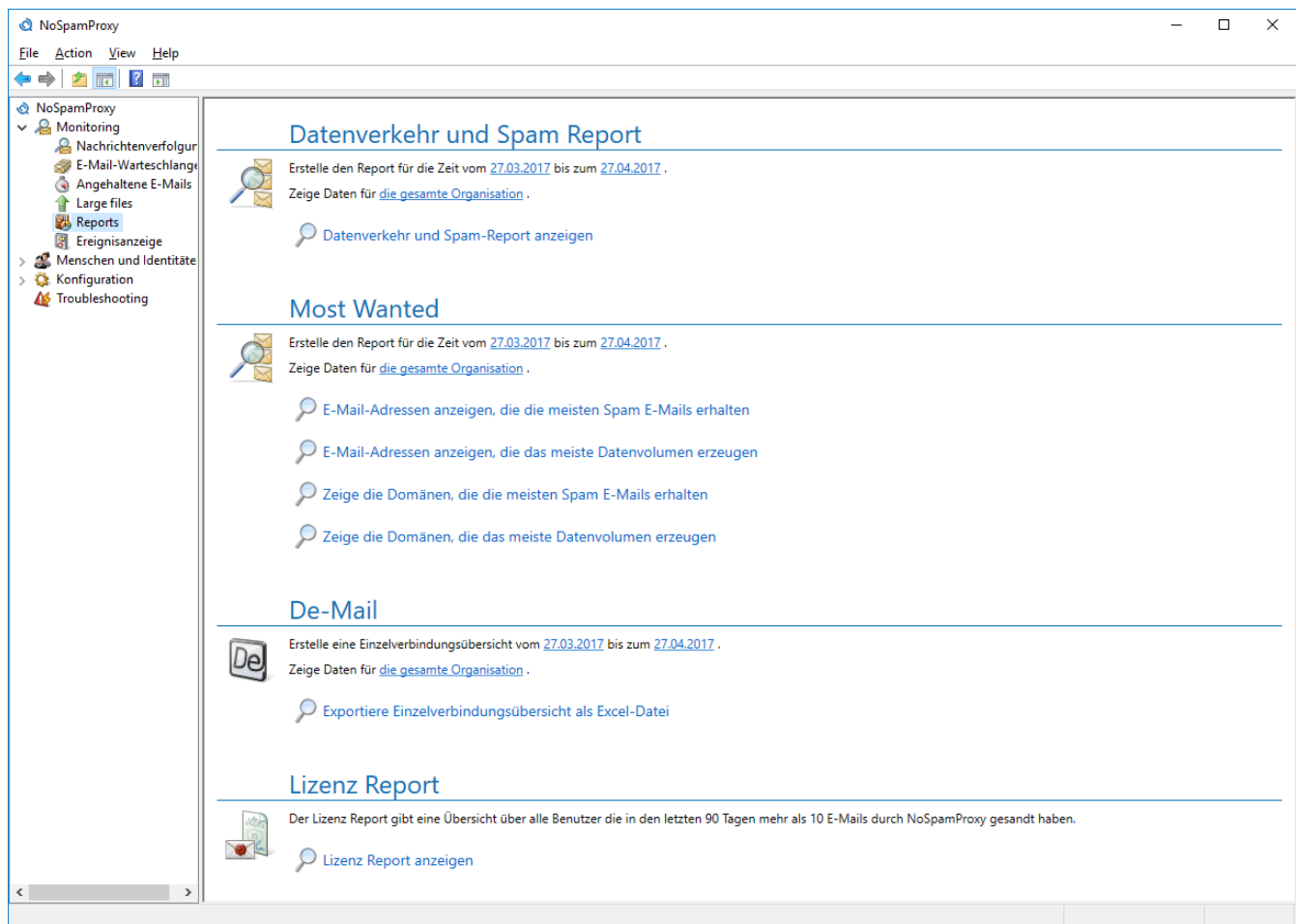
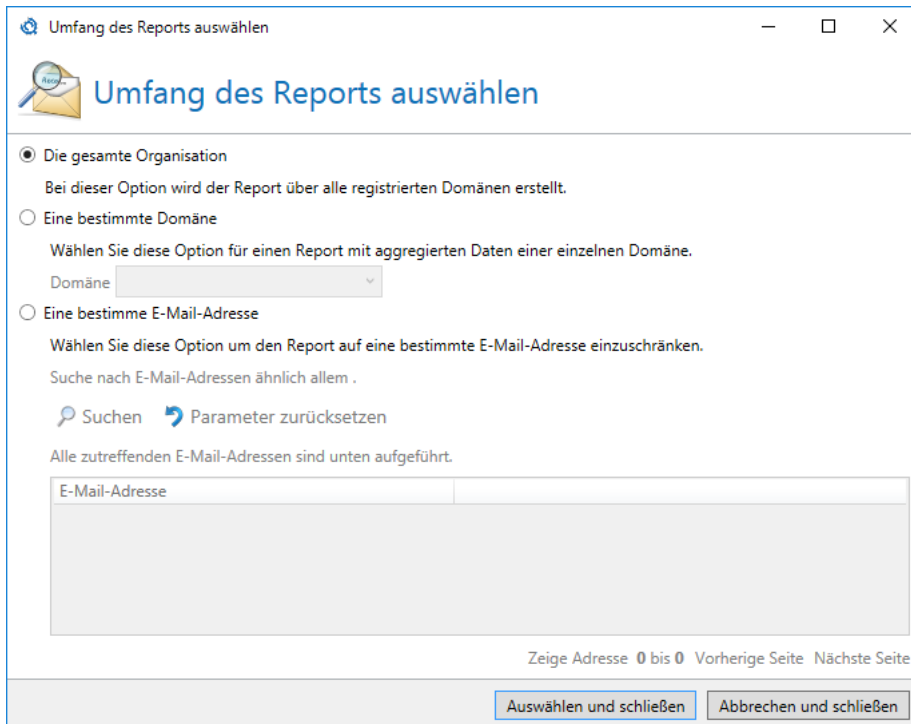


Bild 24: Auswertungen über die Daten der Nachrichtenverfolgung

Datenverkehr und Spam Report

Im Abschnitt "Datenverkehr und Spam Report" haben Sie die Möglichkeit einen Report erstellen zu lassen, der Ihnen den Verlauf des E-Mail-Verkehrs anzeigt. Der Report zeigt sowohl den Verlauf der Anzahl der E-Mails als auch den Verlauf des Datenvolumens. Um den Report zu erstellen, wählen Sie zunächst einen Zeitraum aus, für den Sie den Report erstellen möchten. Anschließend legen Sie den Umfang des Reports fest. Klicken Sie dazu auf den Link **die gesamte Organisation**.



Umfang des Reports auswählen

Umfang des Reports auswählen

☒ Die gesamte Organisation
Bei dieser Option wird der Report über alle registrierten Domänen erstellt.

☐ Eine bestimmte Domäne
Wählen Sie diese Option für einen Report mit aggregierten Daten einer einzelnen Domäne.
Domäne

☐ Eine bestimmte E-Mail-Adresse
Wählen Sie diese Option um den Report auf eine bestimmte E-Mail-Adresse einzuschränken.
Suche nach E-Mail-Adressen ähnlich allem .
 Suchen

Alle zutreffenden E-Mail-Adressen sind unten aufgeführt.

E-Mail-Adresse

Zeige Adresse 0 bis 0 Vorherige Seite Nächste Seite

Bild 25: Der Umfang des Datenverkehr und Spam Reports

In dem erscheinenden Dialog ([Bild 25](#)) können Sie sich entscheiden, ob Sie den Report für die gesamte Organisation, nur für eine bestimmte Domäne oder sogar nur für eine bestimmte E-Mail-Adresse erstellen möchten.



Es können nur Domänen und E-Mail-Adressen ausgewählt werden, die bereits E-Mails empfangen haben und somit in der Nachrichtenverfolungsdatenbank auftauchen. Es findet kein Zugriff auf die Konfiguration der Gateway Rolle statt.

Klicken Sie anschließend auf **Auswählen und speichern**, um die Einstellungen abzuspeichern. Anschließend klicken Sie auf **Report anzeigen**, um den Report zu erstellen.

Most wanted

Im Abschnitt **Most wanted** bietet NoSpamProxy Ihnen vier Reports an, die zum Beispiel die E-Mail-Adressen bzw. Domänen mit dem höchsten Spam-Anteil aufweisen. Des Weiteren gibt es Reports, die Ihnen die E-Mail-Adressen bzw. Domänen anzeigen, die das meiste Datenvolumen erzeugt haben ([Bild 26](#)) Wie auch im Abschnitt **Datenverkehr & Spam Report** können Sie den Zeitraum und den Umfang des jeweiligen Reports festlegen.

NoSpamProxy

File

Action

View

Help

←

→

📁

🔍

📄

Net at Work Mail Gateway

Monitoring

Nachrichtenverfolgung

E-Mail-Warteschlange

Angehaltene E-Mails

Reports

Ereignisanzeige

Menschen und Identitäten

Konfiguration

Troubleshooting

🔍

Zurück zur Report Auswahl

📄

◀

▶

1

of 1

◀

⌂

📄

📄

📄

📄

100%

Find

Next

E-Mail Adressen die den höchsten Spam Anteil aufweisen

vom 04.02.2010 bis zum 04.03.2010

	Datenvolumen		E-Mails			Spam Anteil
	Empfangen	Gesendet	Angenommen	Abgelehnt		
sagittis.Curabitur@sit.eu	41,22 MB	99,37 MB	244	2.340	90,56%	
pede.interdum@sit.eu	0,68 MB	0,00 MB	14	2.059	99,32%	
tellus.tempus@sit.eu	2,82 MB	0,00 MB	48	1.993	97,65%	
dui.sagittis@sit.eu	157,22 MB	32,53 MB	1.562	1.832	53,98%	
a.nec@sit.eu	0,11 MB	0,01 MB	9	1.776	99,50%	
bibendum.Duis@Duis.de	0,03 MB	0,00 MB	1	1.669	99,94%	
vitae.ante@sit.eu	8,28 MB	0,47 MB	53	1.601	96,80%	
porta.nascetur@sit.eu	5,48 MB	0,00 MB	144	1.479	91,13%	
bibendum.Duis@sit.eu	43,61 MB	0,00 MB	287	1.430	83,28%	
et.metus@sit.eu	0,01 MB	0,00 MB	1	1.394	99,93%	
ultrices.imperdiet@sit.eu	0,00 MB	0,00 MB	0	1.355	100,00%	
Duis.Maecenas@sit.eu	11,21 MB	9,17 MB	75	1.279	94,46%	
commodo@sit.eu	0,72 MB	0,00 MB	22	1.270	97,54%	

Bild 26: Die Adressen mit dem größten Spam Anteil

Die zur Verfügung stehenden Reports sind folgende:

- E-Mail-Adressen anzeigen, die die meisten Spam E-Mails erhalten.
- E-Mail-Adressen anzeigen, die das größte Datenvolumen erzeugen.
- Zeige die Domänen, die die meisten Spam E-Mails erhalten.
- Zeige die Domänen, die das größte Datenvolumen erzeugen.

Klicken Sie anschließend auf den gewünschten Report, um ihn zu generieren.

De-Mail

Mit dem De-Mail-Report können Sie eine Einzelverbindungsübersicht für gesendete De-Mails als Excel-Report erzeugen. Um den Report zu erstellen, wählen Sie zunächst aus, ob Sie eine Übersicht für die ganze Organisation oder für eine bestimmte Domäne erstellen möchten. Außerdem können Sie den Zeitraum für die Übersicht einschränken. Klicken Sie anschließend auf **Einzelverbindungsübersicht erstellen**. Im folgenden Dialog wählen Sie aus, wo Sie die Excel-Datei speichern möchten.

Lizenz-Report

Der Lizenz-Report ermöglicht es, die Anzahl der lizenzierten Benutzer auf die tatsächlich benötigten Lizenzen anzupassen. (Bild 27).

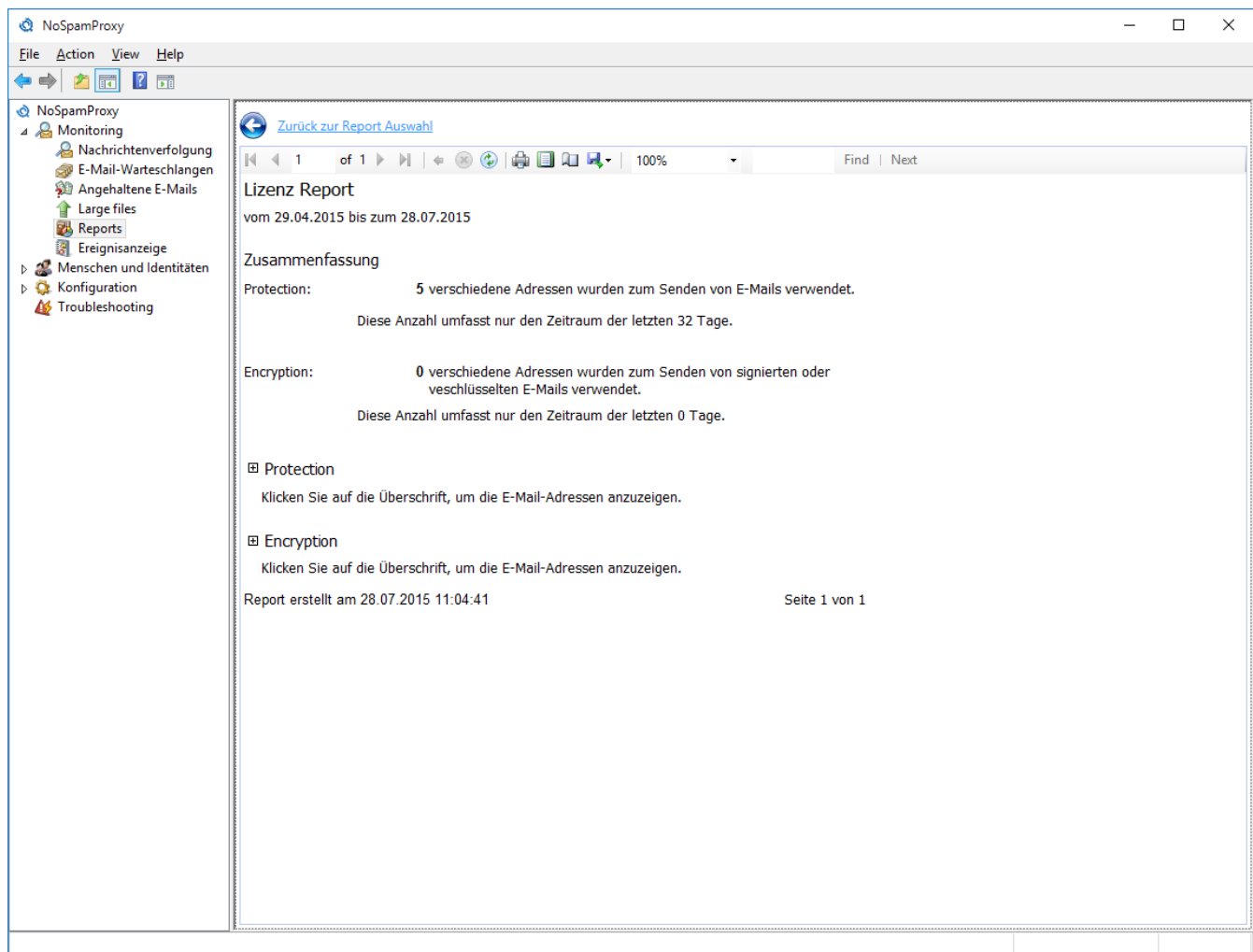


Bild 27: Der Report der tatsächlich genutzten Lizenzen

Der Lizenz-Report summiert alle Benutzer, die in den letzten 90 Tagen mehr als 10 E-Mails versandt haben.

Die Benutzerzahlen aus diesem Report geben Ihnen die Möglichkeit, die Lizenzen von NoSpamProxy an das Wachstum Ihres Unternehmens anzupassen.

Für Fragen zu diesem Thema steht Ihnen unser Team unter info@netatwork.de gerne zur Verfügung.

Ereignisanzeige

Die für NoSpamProxy relevanten Server-Ereignisse sind in der Oberfläche unter dem Knoten "Ereignisanzeige" verfügbar ([Bild 28](#)).

Ereignisanzeige

Suche nach [alle Einträge](#) für [alle Rollen](#) .

[Suchen](#) [Parameter zurücksetzen](#)

Schwere	Ereigniskennung	Datum und Uhrzeit	Rolle oder Dienst	Servername
Warnung	5634	28.07.2015 10:54:27	Intranet Role	WIN-NOU0K4P18VB
Information	6305	28.07.2015 10:54:26	Intranet Role	WIN-NOU0K4P18VB
Information	0	28.07.2015 10:54:25	Gateway Role	WIN-NOU0K4P18VB
Fehler	4593	28.07.2015 10:54:24	Gateway Role	WIN-NOU0K4P18VB
Information	6305	28.07.2015 10:54:23	Gateway Role	WIN-NOU0K4P18VB
Warnung	6423	28.07.2015 10:54:23	Gateway Role	WIN-NOU0K4P18VB
Information	0	28.07.2015 10:51:09	Management Service	WIN-NOU0K4P18VB
Information	0	28.07.2015 10:51:09	Intranet Role	WIN-NOU0K4P18VB
Information	0	28.07.2015 10:51:09	Intranet Role	WIN-NOU0K4P18VB
Information	0	28.07.2015 10:51:08	Gateway Role	WIN-NOU0K4P18VB
Fehler	1213	28.07.2015 10:34:33	Intranet Role	WIN-NOU0K4P18VB
Information	1210	28.07.2015 10:34:33	Intranet Role	WIN-NOU0K4P18VB

Zeige Ereignis **1** bis **50** [Vorherige Seite](#) [Nächste Seite](#)

Details

Markierte Einträge in die Zwischenablage kopieren

Bild 28: Die Ereignisanzeige zeigt die Ereignisse aller Rollen von NoSpamProxy an

Sie können die hier angezeigten Einträge einerseits nach den Rollen bzw. Diensten filtern, andererseits aber auch die Art der angezeigten Ereignisse einschränken. Die wählbaren Kategorien sind **Fehler**, **Informationen** und **Warnungen**. Um weiter zurückliegende Einträge anzuschauen, können Sie mit den Funktionen **Zurück** und **Weiter** durch das Ergebnis der Suche blättern.

Um die Details eines Eintrags anzuzeigen, müssen Sie diesen nur mit der Maus markieren. Die Details werden im unteren Teil der Seite eingeblendet.

8. Menschen und Identitäten

Der Knoten **Menschen und Identitäten** beinhaltet alle externen und internen Firmen und Personen sowie deren E-Mail-Adressen ([Bild 29](#)).

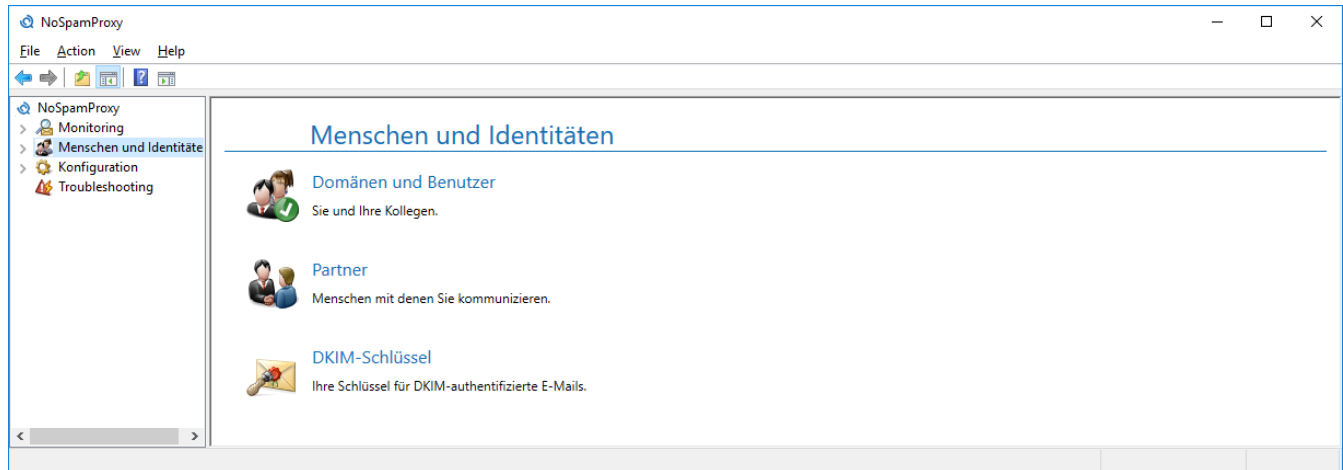


Bild 29: Die Bereiche unter dem Knoten Menschen und Identitäten

Domänen und Benutzer

Im Knoten für **Domänen und Benutzer** können Sie Ihre eigenen Domänen und eine Liste mit gültigen E-Mail-Empfängern und den zugehörigen Adressen pflegen ([Bild 30](#)). Diese Liste wird verwendet, wenn Sie in den Regeln auf "Lokale Adressen" statt "Eigene Domänen" filtern. Darüber hinaus können Sie hier den automatischen Import von Benutzerdaten konfigurieren.

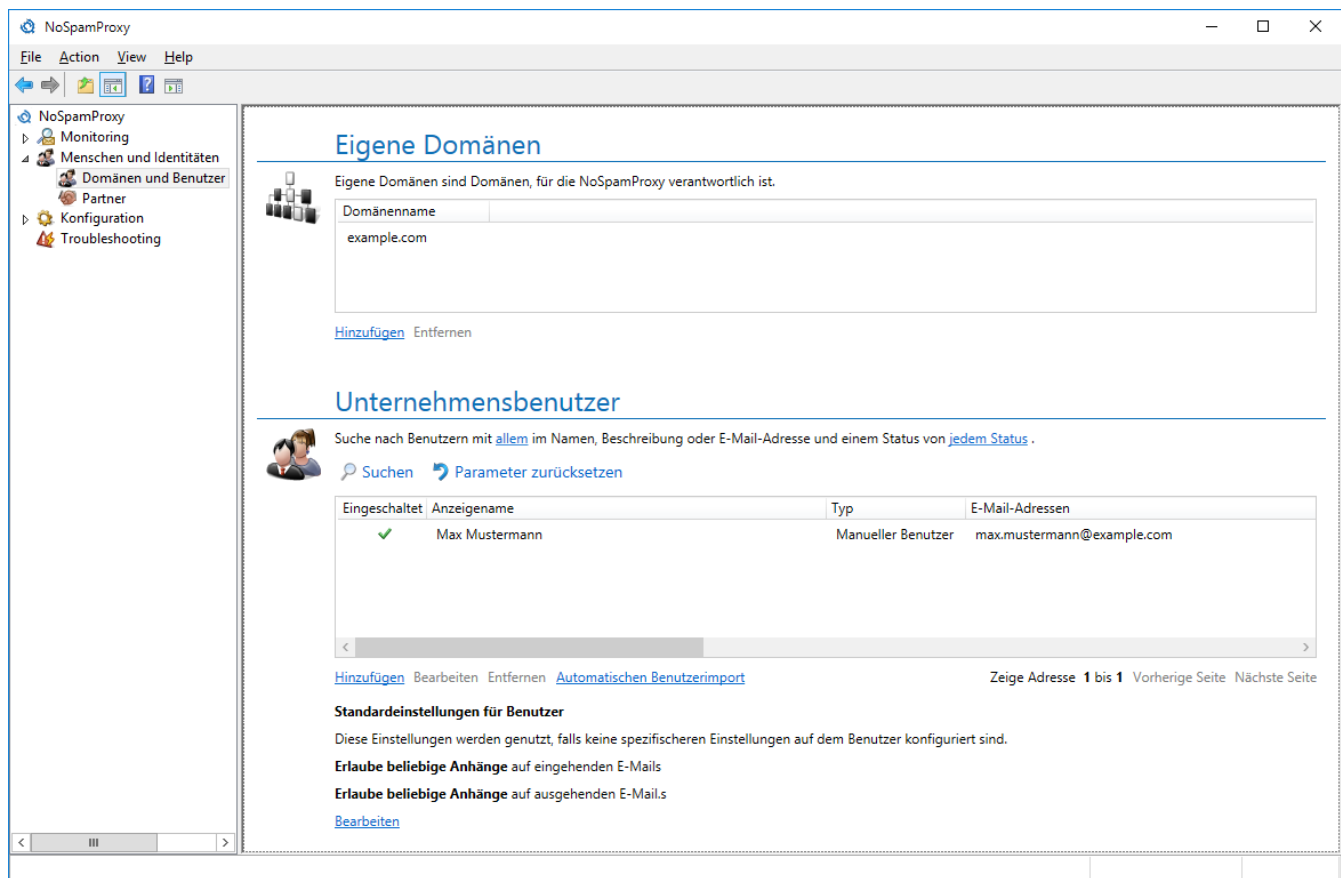


Bild 30: Die Liste der eigenen Domänen und die Unternehmensbenutzer

Eigene Domänen

Tragen Sie in die Liste der eigenen Domänen alle Domänen ein, für die Sie E-Mails empfangen wollen. Sie können diese Liste später auch in den Regeln verwenden. Andernfalls wird NoSpamProxy solche Verbindungen als Relay-Missbrauch erkennen und diese E-Mails nicht annehmen.



Alle lokalen Domänen müssen eingetragen werden. Nur dadurch werden alle lokalen E-Mails sicher als solche erkannt und nicht als Relay-Missbrauch abgewiesen.

Eigene Domänen hinzufügen

Die Aktion **Hinzufügen** öffnet den Eingabedialog ([Bild 31](#)).

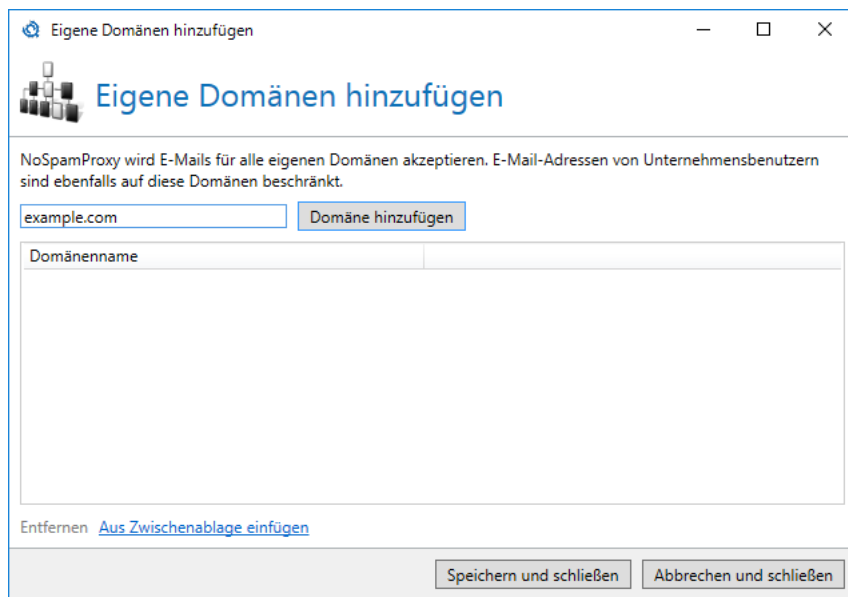


Bild 31: Dialog für neue eigene Domänen

Tragen Sie hier alle Ihre lokalen Domänen ein.



Beim Löschen von lokalen Domänen werden auch alle E-Mail-Adressen dieser Domäne aus den Unternehmensbenutzern gelöscht. Falls die Nutzer danach keine E-Mail-Adressen mehr besitzen, werden die Benutzer ebenfalls gelöscht.

DomainKeys Identified Mail

Die DomainKeys Identified Mail (DKIM) sichert ausgehende E-Mails mit einer elektronischen Signatur. Durch die Auswertung dieser Signatur kann der Empfänger erkennen, ob die E-Mail von der richtigen Domäne versandt wurde (sicherstellen der Authentizität) und ob sie während des Transports verändert wurde (sicherstellen der Integrität). DKIM-signierte E-Mails können auch von E-Mail-Empfängern gelesen werden, die die DKIM-Signatur nicht auswerten können. Für diese Empfänger sehen DKIM-signierte E-Mails genau so aus wie E-Mails ohne DKIM-Signatur.

Die für diesen Vorgang notwendigen Schlüssel können Sie auf dem Knoten **DKIM-Schlüssel** selbst erstellen. Der geheime private Teil des asymmetrischen Schlüssels wird dabei sicher in den NoSpamProxy-Einstellungen gespeichert und ist dadurch nur Ihnen bekannt.

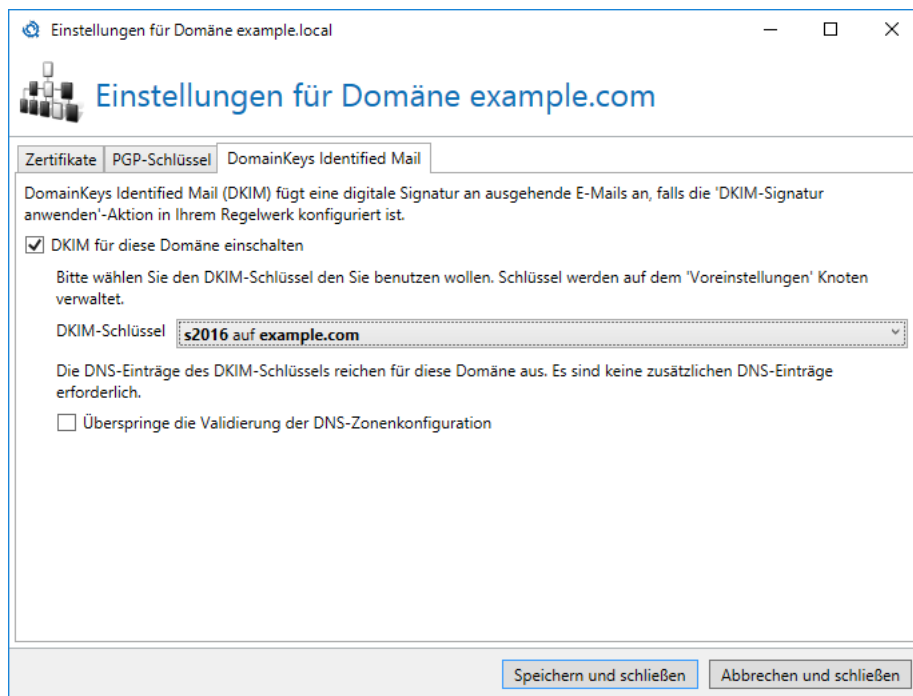


Bild 32: Die Auswahl eines DKIM-Schlüssels für die aktuelle eigene Domäne

Die bereits erstellten Schlüssel können auf der Karteikarte **DomainKeys Identified Mail** der Domäne zugeordnet werden ([Bild 32](#)). Aktivieren Sie dazu DKIM für die Domäne und wählen danach einen der bereits erstellten Schlüssel aus der Liste der **DKIM-Schlüssel** aus. Falls die Domäne des DKIM-Schlüssels identisch zu der jetzt konfigurierten Domäne ist, reicht der DNS-Eintrag, den Sie bei der Erstellung des Schlüssels veröffentlicht haben. Falls sich die Domänen unterscheiden, zeigt die Konfigurationsseite einen weiteren notwendigen DNS-Eintrag an ([Bild 33](#)). Wenn Sie weitere DNS-Einträge veröffentlichen müssen, bereitet NoSpamProxy den benötigten Eintrag vor, so dass Sie ihn in die Zwischenablage kopieren können um ihn im DNS zu veröffentlichen. Die DKIM-Konfiguration für diese Domäne muss danach erst einmal abgebrochen werden. Sie müssen die Konfiguration nur abbrechen, falls DNS-Einträge fehlen, ansonsten können Sie mit der Konfiguration ohne Unterbrechung fortfahren.

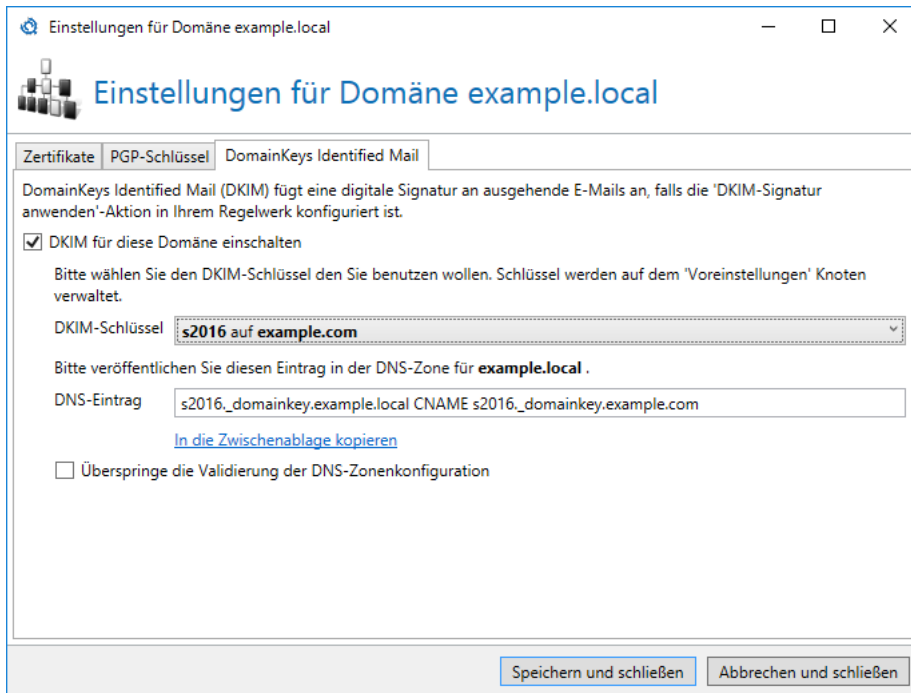


Bild 33: Die Auswahl eines DKIM-Schlüssels von einer anderen Domäne

Wenn alle notwendigen DNS-Einträge veröffentlicht und im Internet bekannt sind, starten Sie die Auswahl des DKIM-Schlüssels bitte erneut. Wählen Sie wieder den Schlüssel für den Sie die DNS Einträge veröffentlicht haben. Während des Speicherns wird die DNS-Konfiguration überprüft. Falls diese Validierung fehlschlägt, werden Ihnen die Unstimmigkeiten angezeigt. Beachten Sie bitte die folgenden Hinweise.



Bei der Veröffentlichung von DNS-Einträgen dauert es einige Zeit, bis alle DNS-Server im Internet diese Änderungen empfangen haben. Warten Sie deshalb nach der Änderung Ihrer DNS-Einträge mindestens 24 Stunden, bevor Sie die Einträge überprüfen und anwenden. Falls Sie DKIM aktivieren und Ihre DNS-Konfiguration fehlerhaft ist, können E-Mails an Empfänger, die DKIM-Signaturen auswerten, nicht mehr zugestellt werden.



Die DKIM-Signatur benötigt zwingend die Aktion **DKIM-Signatur anwenden** in Ihrem Regelwerk. Dies ermöglicht es Ihnen, durch unterschiedlich konfigurierte Regeln für einen Teil Ihrer E-Mails DKIM einzusetzen und für einen anderen Teil DKIM zu unterdrücken.

Unternehmensbenutzer

Analog zu den "Eigenen Domänen" kann NoSpamProxy auch die einzelnen Empfänger prüfen und E-Mails an nicht existierende Empfänger direkt abweisen. Dazu ist es aber erforderlich, dass das Gateway

alle internen Empfänger kennt. Wenn Sie ein Active Directory verwenden, können Sie auf eine einfache Art und Weise die Unternehmensbenutzer importieren.

Die Liste der **Unternehmensbenutzer** wird verwendet, wenn Sie in den Regeln auf **Lokale Adressen** statt **Eigene Domänen** filtern.



Damit NoSpamProxy die **Unternehmensbenutzer**-Liste auch verwendet, muss in den entsprechenden [Regeln](#) für eingehenden E-Mail-Verkehr auf der Registerkarte **Nachrichtenfluss** der **Bereich** von **an eine eigene Domäne** auf **an eine E-Mail-Adresse des Unternehmens** umgestellt werden. Erst jetzt nutzt das Gateway die Liste der Unternehmensbenutzer für die Ermittlung gültiger E-Mail-Adressen.

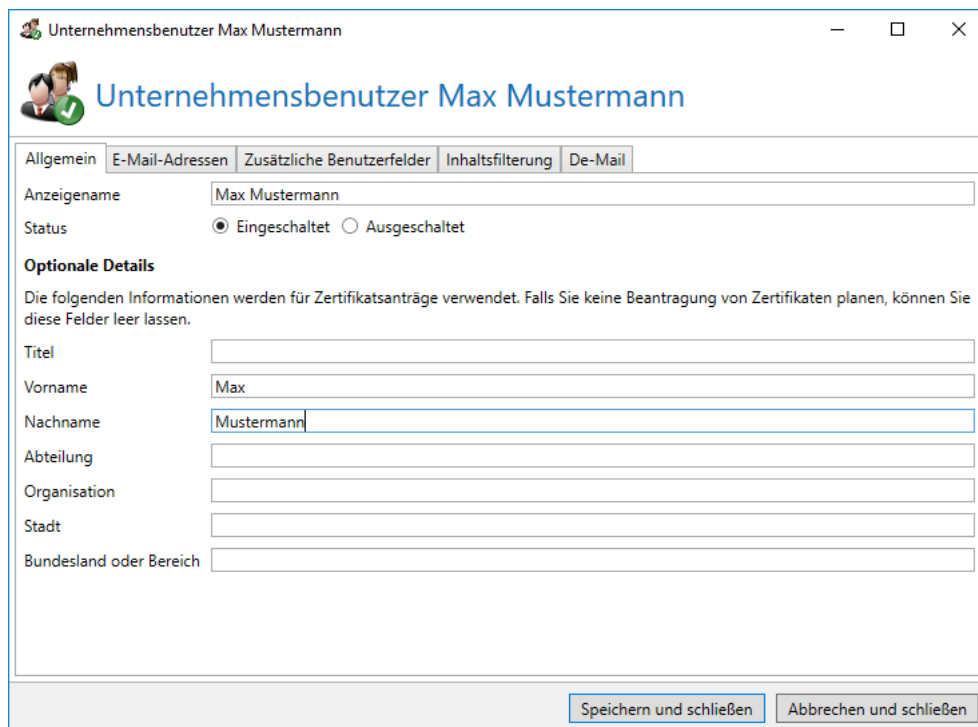
Die Liste der Unternehmensbenutzer kann zwei unterschiedliche **Typen** von Benutzern beinhalten:

- **Manuell eingetragener Benutzer**
Sie können in manuell eingetragenen Benutzern alle Eigenschaften in NoSpamProxy verwalten. Diese Benutzer können beliebig verändert und gelöscht werden.
- **Replizierter Benutzer**
Replizierte Benutzer werden aus einem Verzeichnisdienst wie dem Active Directory importiert. Die Eigenschaften des Benutzers müssen in der ursprünglichen Quelle verändert werden, da in NoSpamProxy bei replizierten Benutzern nur eine Lese-Ansicht der meisten Eigenschaften verfügbar ist. Alle Änderungen werden dann beim erneuten Durchlaufen der [Benutzerimporte](#) übernommen. Sie können in replizierten Benutzern sowohl den Aktivitäts-Status des kompletten Benutzers umstellen, als auch den Aktivitäts-Status von einzelnen E-Mail-Adressen.

Suchen Sie nach Benutzern, indem Sie nach Worten oder Wortbestandteilen im Namen, Beschreibung oder E-Mail-Adresse suchen lassen. Zusätzlich kann bei der Suche auch zwischen aktivierten oder deaktivierten Benutzern unterschieden werden.

Benutzer hinzufügen

Beim Hinzufügen von Benutzern unterstützt Sie ein Assistent. Geben Sie zuerst ([Bild 34](#)) den Namen ein. Der Name ist ein Pflichtfeld. Die optionalen Details werden für die Beantragung von Zertifikaten benötigt.



Unternehmensbenutzer Max Mustermann

Unternehmensbenutzer Max Mustermann

Allgemein | E-Mail-Adressen | Zusätzliche Benutzerfelder | Inhaltsfilterung | De-Mail

Anzeigenname: Max Mustermann

Status: ☒ Eingeschaltet ☐ Ausgeschaltet

Optionale Details

Die folgenden Informationen werden für Zertifikatsanträge verwendet. Falls Sie keine Beantragung von Zertifikaten planen, können Sie diese Felder leer lassen.

Titel:

Vorname: Max

Nachname: Mustermann

Abteilung:

Organisation:

Stadt:

Bundesland oder Bereich:

Speichern und schließen | Abbrechen und schließen

Bild 34: Der Name und die Daten des Benutzers

Geben Sie im nächsten Schritt alle E-Mail-Adressen des Benutzers ein ([Bild 35](#)).

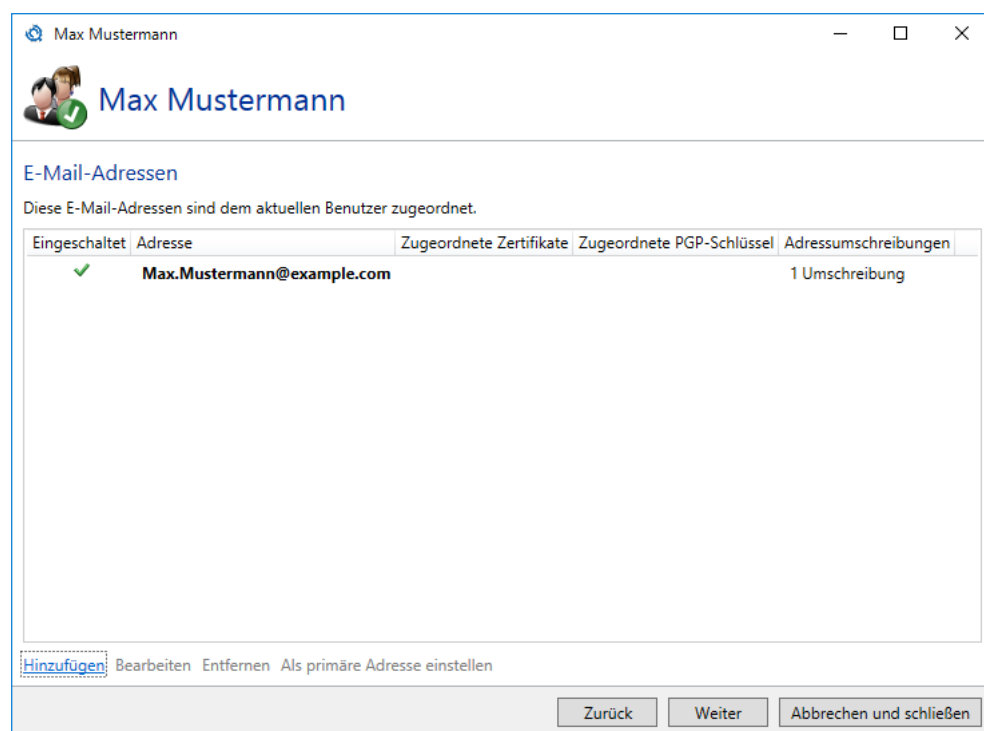
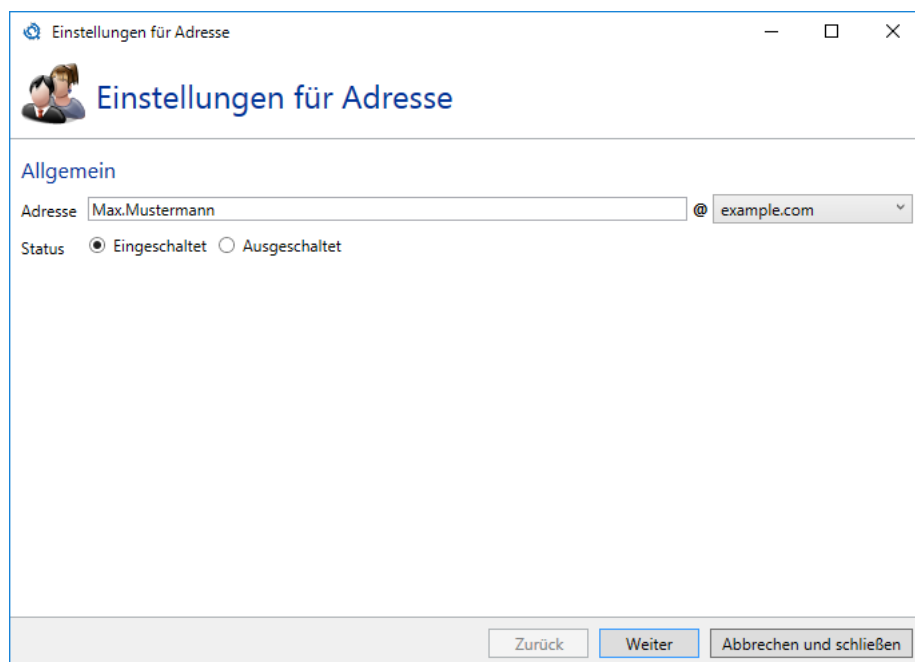


Bild 35: Alle E-Mail-Adressen, die dem Benutzer zugeordnet sind

Geben Sie den lokalen Teil der E-Mail-Adresse ein und wählen Sie danach die Domäne aus der Auswahlliste der bereits eingegeben eigenen Domänen. Über **Status** kann die Adresse auch deaktiviert werden ([Bild 36](#)).



Die erste eingegebene Adresse wird als primäre Adresse markiert. Sie können dieses in der Liste der E-Mail-Adressen über die Aktion **Als primäre Adresse einstellen** ändern. Die primäre Adresse wird für andere Funktionen, wie z.B. De-Mail verwendet.



Einstellungen für Adresse

Einstellungen für Adresse

Allgemein

Adresse @

Status ☒ Eingeschaltet ☐ Ausgeschaltet

Zurück Weiter Abbrechen und schließen

Bild 36: Eingabe einer neuen E-Mail-Adresse

Verfügen Sie über Lizenzen für NoSpamProxy Large Files oder NoSpamProxy Protection, können Sie jetzt einen Inhaltsfilter auswählen. Falls der Benutzer keine bestimmten Inhaltsfilter zugewiesen bekommen soll, können Sie hier auch die [Standardeinstellungen für Benutzer](#) verwenden. Die Inhaltsfilter werden auf dem Knoten [Inhaltsfilter](#) definiert.

Der letzte Schritt ([Bild 37](#)) bestimmt alle [Adressumschreibungen](#) für diese E-Mail-Adresse.

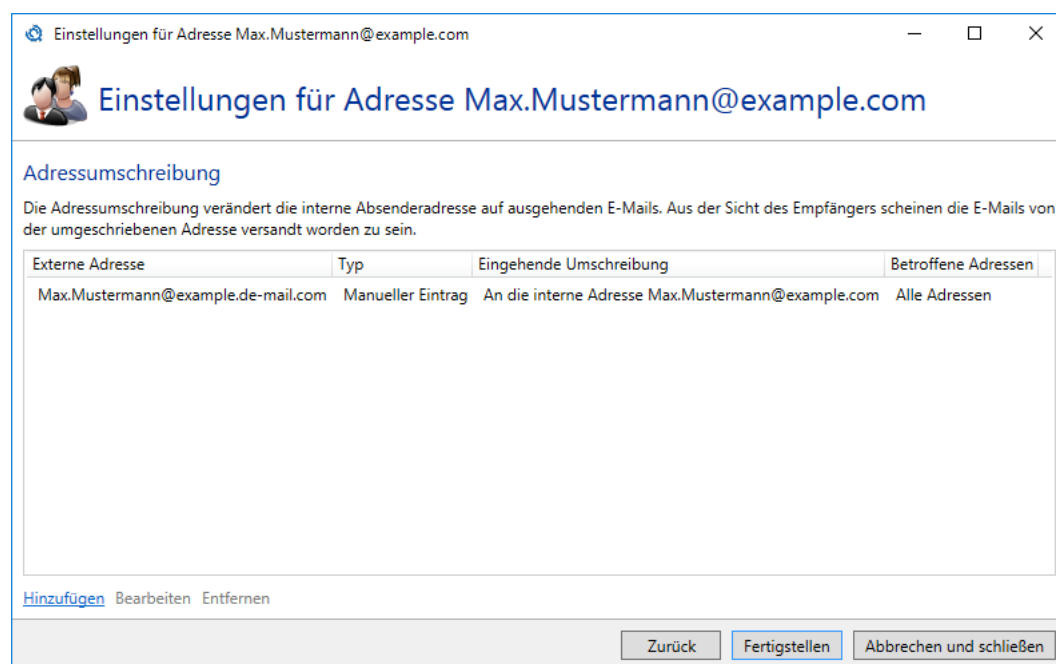
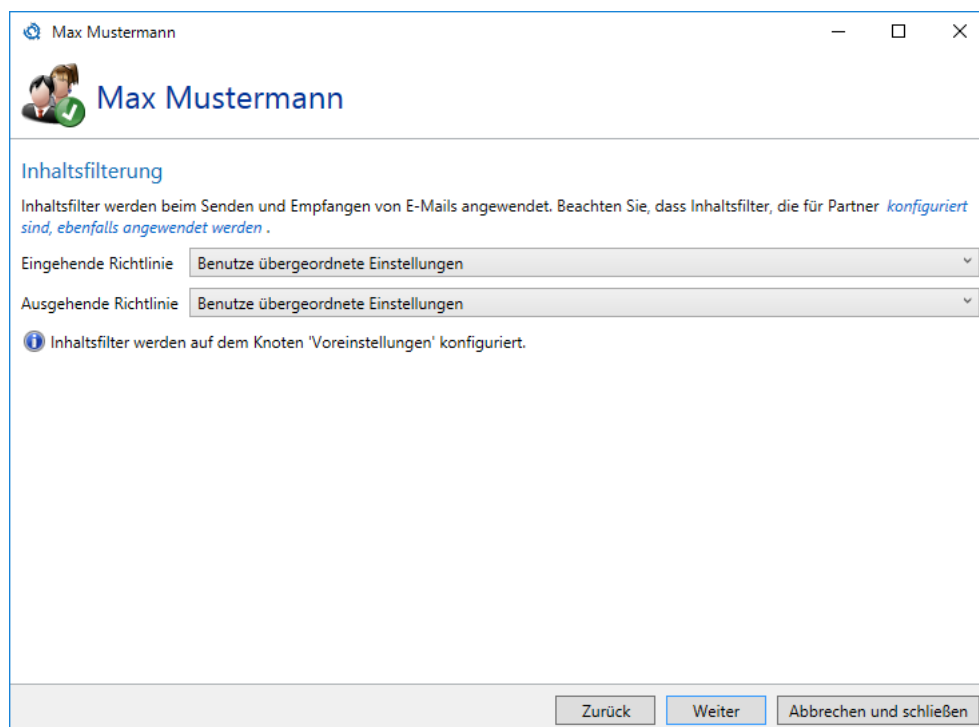


Bild 37: Die Liste aller Adressumschreibungen

Die **Zusätzlichen Benutzerfelder** können vom Administrator mit Werten gefüllt werden.

Lesen Sie im Kapitel über den [Disclaimer](#), wie sie **Zusätzliche Benutzerfelder** für einen Benutzer konfigurieren.

Verfügen Sie über Lizenzen für NoSpamProxy Large Files oder NoSpamProxy Protection, können Sie auf der folgenden Seite die verwendeten Inhaltsfilter auswählen([Bild 38](#)). Sie können entweder die übergeordneten Einstellungen verwenden, alle Anhänge zulassen, oder einen auf dem Knoten **Voreinstellungen** konfigurierten Inhaltsfilter auswählen.



The screenshot shows a web-based configuration window titled 'Max Mustermann'. The window has a header with the user's name and a profile picture. Below the header, the section 'Inhaltsfilterung' (Content Filtering) is displayed. It contains a paragraph explaining that content filters are applied when sending and receiving emails, and that filters configured for partners are also applied. Below this text are two dropdown menus: 'Eingehende Richtlinie' (Incoming Policy) and 'Ausgehende Richtlinie' (Outgoing Policy), both set to 'Benutze übergeordnete Einstellungen' (Use parent settings). An information icon and text state that filters are configured on the 'Voreinstellungen' (Default Settings) node. At the bottom, there are three buttons: 'Zurück' (Back), 'Weiter' (Next), and 'Abbrechen und schließen' (Cancel and Close).

Max Mustermann

Inhaltsfilterung

Inhaltsfilter werden beim Senden und Empfangen von E-Mails angewendet. Beachten Sie, dass Inhaltsfilter, die für Partner *konfiguriert sind, ebenfalls angewendet werden*.

Eingehende Richtlinie: Benutze übergeordnete Einstellungen

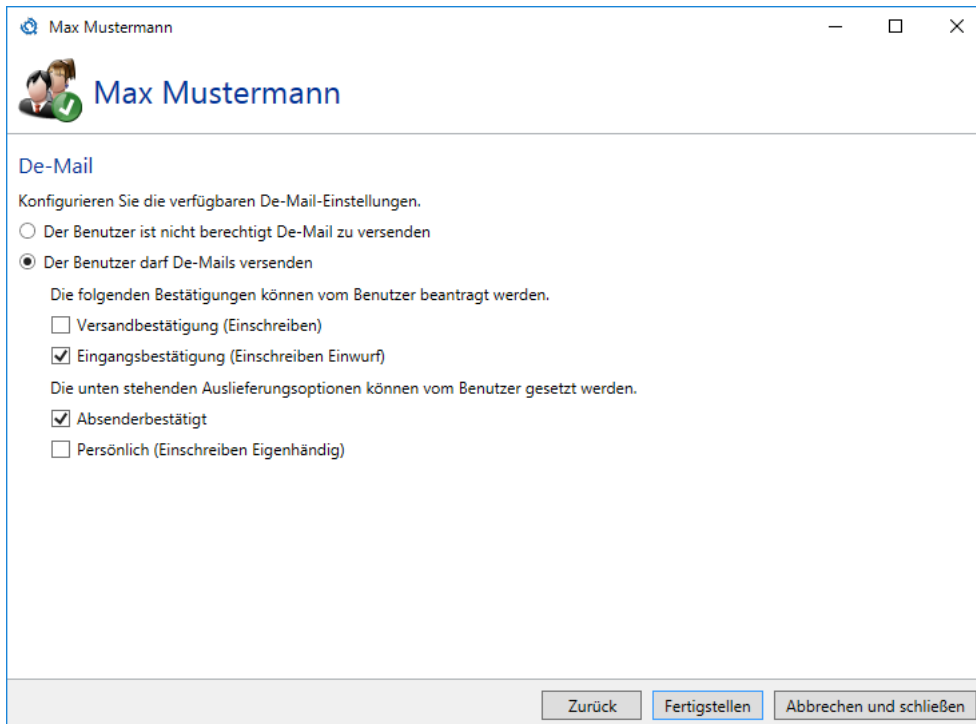
Ausgehende Richtlinie: Benutze übergeordnete Einstellungen

i Inhaltsfilter werden auf dem Knoten 'Voreinstellungen' konfiguriert.

Zurück Weiter Abbrechen und schließen

Bild 38: Konfiguration der Inhaltsfilter für den Benutzer

Auf der Seite **De-Mail** ([Bild 39](#)) legen Sie fest, welche De-Mail-Funktionen für diesen manuell angelegten Benutzer verfügbar sind. Stellen Sie zuerst ein, ob der Benutzer generell berechtigt ist, De-Mails zu versenden. Legen Sie dann gegebenenfalls alle Bestätigungen und Auslieferungsoptionen fest, die dieser Benutzer anfordern kann.



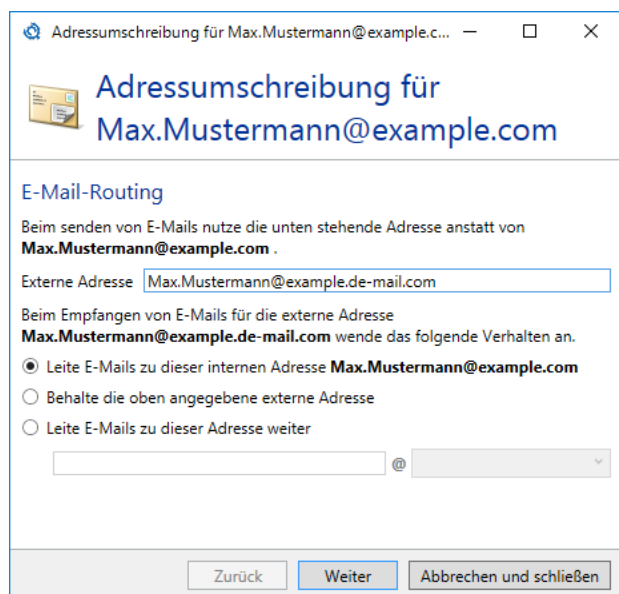
The screenshot shows a window titled 'Max Mustermann' with a user icon and name. Below the header, the section 'De-Mail' is active. The text 'Konfigurieren Sie die verfügbaren De-Mail-Einstellungen.' is followed by two radio button options: 'Der Benutzer ist nicht berechtigt De-Mail zu versenden' (unselected) and 'Der Benutzer darf De-Mails versenden' (selected). Under the selected option, there are two sub-sections. The first, 'Die folgenden Bestätigungen können vom Benutzer beantragt werden.', contains two checkboxes: 'Versandbestätigung (Einschreiben)' (unchecked) and 'Eingangsbestätigung (Einschreiben Einwurf)' (checked). The second sub-section, 'Die unten stehenden Auslieferungsoptionen können vom Benutzer gesetzt werden.', contains two checkboxes: 'Absenderbestätigt' (checked) and 'Persönlich (Einschreiben Eigenhändig)' (unchecked). At the bottom, there are three buttons: 'Zurück', 'Fertigstellen', and 'Abbrechen und schließen'.

Bild 39: Verfügbare De-Mail-Funktionen für den Benutzer

Neue Adressumschreibung

Die Adressumschreibung schreibt die E-Mail-Adresse eines Unternehmensbenutzers auf eine andere E-Mail-Adresse um. Dadurch kann ein lokaler Nutzer gegenüber externen E-Mail-Empfängern mit einer anderen E-Mail-Adresse als seiner eigenen auftreten. Die E-Mail scheint dann von der umgeschriebenen Adresse versandt worden zu sein. Bei E-Mails an lokale Adressen wird geprüft, ob der Empfänger ein Eintrag aus den externen Adressen der Adressumschreibung ist. Im Anschluss wird die Adresse an die lokale Adresse des Eintrags gesandt. Ein weiterer Anwendungsfall sind sogenannte Gruppenmailboxen. In diesem Fall werden verschiedene lokale E-Mail-Adressen auf eine Adresse (z.B. info@example.com) umgeschrieben.

Legen Sie bei einer Adressumschreibung zuerst die **Externe Adresse** fest. Diese wird genutzt, falls die E-Mail-Adresse umgeschrieben wird ([Bild 40](#)). Wählen Sie danach, wie E-Mails an lokale Adressen behandelt werden.



Adressumschreibung für Max.Mustermann@example.com

E-Mail-Routing

Beim senden von E-Mails nutze die unten stehende Adresse anstatt von **Max.Mustermann@example.com**.

Externe Adresse

Beim Empfangen von E-Mails für die externe Adresse **Max.Mustermann@example.de-mail.com** wende das folgende Verhalten an.

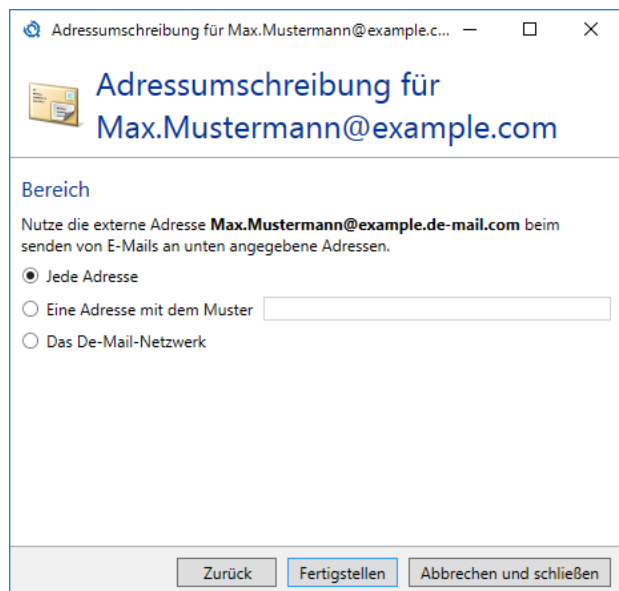
- ☒ Leite E-Mails zu dieser internen Adresse **Max.Mustermann@example.com**
- ☐ Behalte die oben angegebene externe Adresse
- ☐ Leite E-Mails zu dieser Adresse weiter

@

Zurück Weiter Abbrechen und schließen

Bild 40: Externe und lokale Adressen

Im nächsten Schritt wird ausgewählt, bei welchen Empfängeradressen diese Umschreibung genutzt wird ([Bild 41](#)). Entspricht die Empfängeradresse nicht Ihrer Auswahl, wird die Adressumschreibung nicht ausgeführt. In der Auswahl **Eine Adresse mit dem Muster** können Sie Platzhalter ('*' und '?') nutzen.



Adressumschreibung für Max.Mustermann@example.com

Bereich

Nutze die externe Adresse **Max.Mustermann@example.de-mail.com** beim senden von E-Mails an unten angegebene Adressen.

- ☒ Jede Adresse
- ☐ Eine Adresse mit dem Muster
- ☐ Das De-Mail-Netzwerk

Zurück Fertigstellen Abbrechen und schließen

Bild 41: Gewählte Empfängeradressen dieser Umschreibung



Das Löschen von Benutzern ist für replizierte Benutzer nicht verfügbar.

Standardeinstellungen für Benutzer

Bei lizenziertem NoSpamProxy Large Files oder NoSpamProxy Protection können Sie in den Standardeinstellungen einen Inhaltsfilter auswählen. Dieser wird immer angewendet, falls der Unternehmensbenutzer keine abweichenden Einstellungen besitzt. Die Inhaltsfilter werden auf dem Knoten [Inhaltsfilter](#) definiert.

Automatischer Benutzerimport

Über den Link **Automatischer Benutzerimport** haben Sie die Möglichkeit den Import von Benutzerdaten zu automatisieren. ([Bild 42](#)).

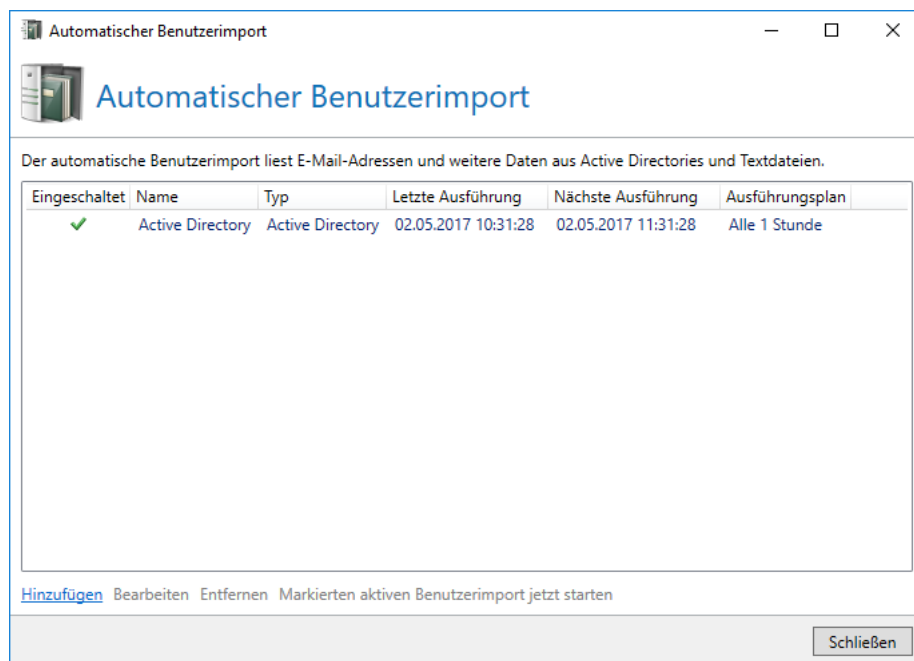


Bild 42: Die Liste aller eingerichteten Benutzerimporte

Sie können in der Intranet Rolle mehrere Benutzerimporte einrichten. Dies ermöglicht es Ihnen, die Unternehmensbenutzer in der Gateway Rolle von NoSpamProxy differenziert auf dem aktuellen Stand zu halten. So können Sie z.B. einen Import einrichten, der alle aktiven Benutzer aus dem Active Directory in die Unternehmensbenutzer importiert. So können Sie automatisiert sicherstellen, dass nur die von Ihnen gewünschten Adressen aus dem Internet erreichbar sind.

Neuer Benutzerimport

In einem Benutzerimport legen Sie fest, welche E-Mail-Adressen importiert werden sollen. Als Quelle können Sie entweder ein Active Directory oder eine Textdatei angeben. Des Weiteren legen Sie fest, wann oder in welchen zeitlichen Abständen ein Durchlauf stattfinden soll.

Beim Hinzufügen eines neuen Benutzerimports legen Sie im ersten Schritt den Typ fest. ([Bild 43](#)). Sie können aus dem Active Directory, einer generischen LDAP-Quelle, wie zum Beispiel Lotus Notes, oder einer Textdatei importieren.

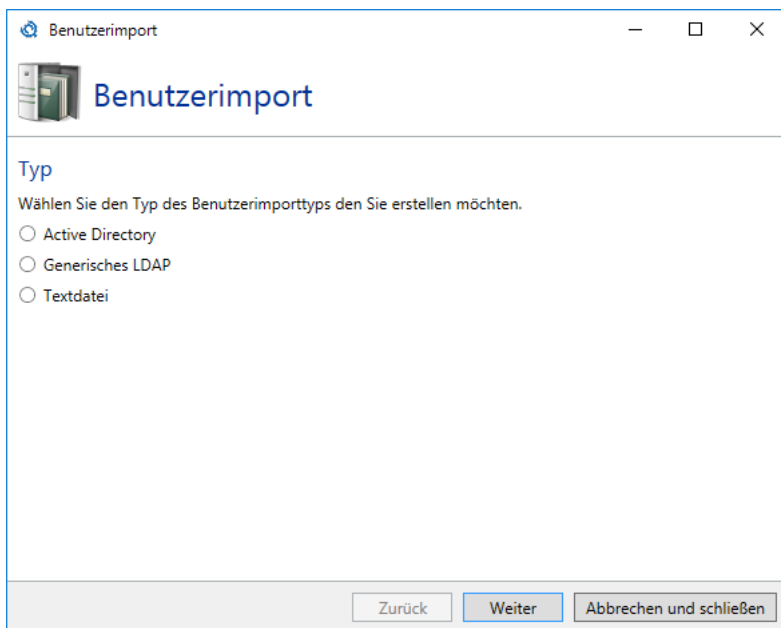


Bild 43: Typ des Benutzerimports

Im Schritt **Allgemein** ([Bild 44](#)) geben Sie einen eindeutigen Namen für den Benutzerimport an. Legen Sie dann unter **Aktualisierungszyklus** fest, wann der Benutzerimport durchgeführt wird. Über **Status** können Sie den Import auch abschalten ohne ihn zu löschen.

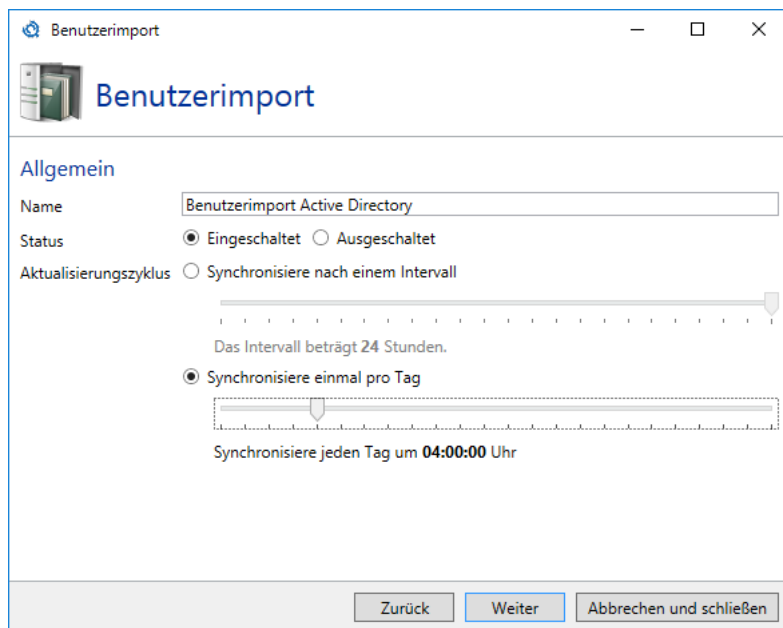
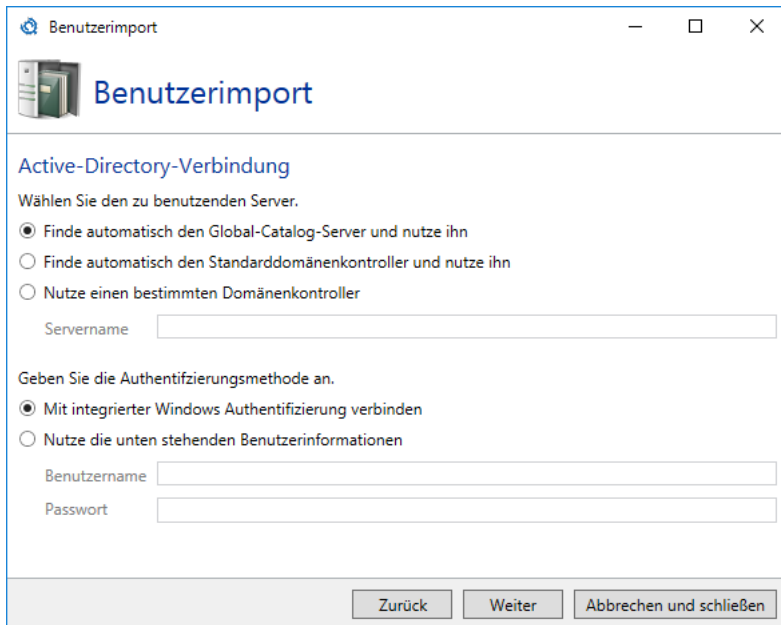


Bild 44: Allgemeine Einstellungen

Lesen Sie jetzt bitte, je nach ausgewähltem Typ, in dem Kapitel [Active Directory](#), [Generisches LDAP](#) oder [Textdatei](#) weiter.

Active Directory

In der **Active-Directory-Verbindung** stellen Sie die Verbindung mit Ihrem Domänenkontroller her ([Bild 45](#)). Wählen Sie dazu die Art des Servers und den Benutzer, der darauf zugreifen darf. Wenn Sie einen bestimmten Domänenkontroller eintragen möchten, können Sie eine IP-Adresse oder einen Servernamen eintragen. Bei Auswahl der integrierten Windows Authentifizierung nutzt NoSpamProxy den Netzwerkdienst, falls es auf einem Domänenkontroller installiert wurde. Andernfalls wird das Computerkonto zur Authentifizierung verwendet.



Benutzerimport

Active-Directory-Verbindung

Wählen Sie den zu benutzenden Server.

☒ Finde automatisch den Global-Catalog-Server und nutze ihn

☐ Finde automatisch den Standarddomänenkontroller und nutze ihn

☐ Nutze einen bestimmten Domänenkontroller

Servername

Geben Sie die Authentifizierungsmethode an.

☒ Mit integrierter Windows Authentifizierung verbinden

☐ Nutze die unten stehenden Benutzerinformationen

Benutzername

Passwort

Zurück Weiter Abbrechen und schließen

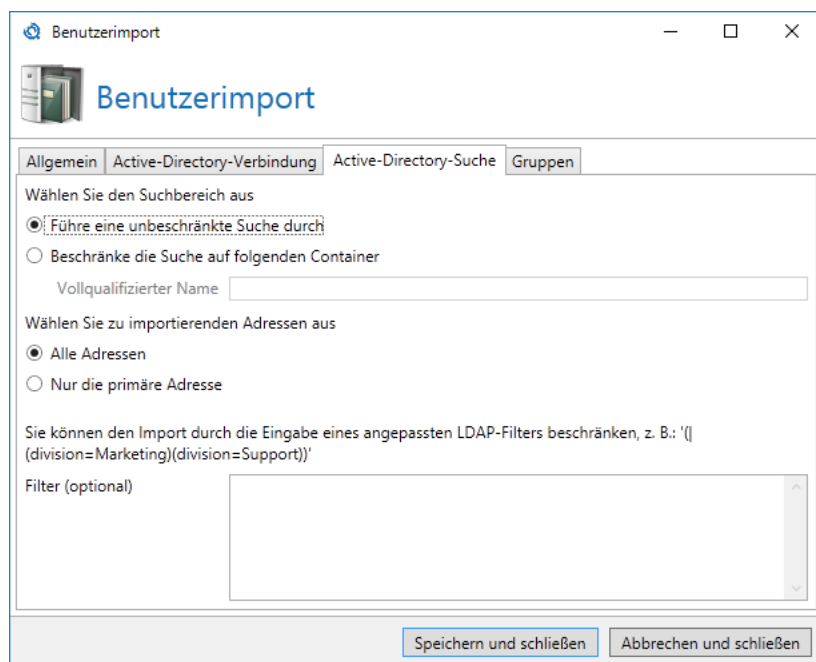
Bild 45: Die Verzeichnisverbindung

Die **Active-Directory-Suche** wählt die Benutzer aus, die importiert werden. Sie können hier auf bestimmte Container filtern, z.B.:

OU=Vertrieb, OU=User, DC=domäne, DC=DE.

Ersetzen Sie bei der Benutzung des Beispiels "Vertrieb", "User", "domäne" und "DE" mit passenden Werten.

In den meisten Fällen werden Sie alle E-Mail-Adressen der Benutzer importieren wollen. Sie können den Import aber auch auf die primäre Adresse einschränken, in dem Sie die auf dieser Seite stehende Option auswählen.



Benutzerimport

Benutzerimport

Allgemein Active-Directory-Verbindung Active-Directory-Suche Gruppen

Wählen Sie den Suchbereich aus

☒ Führe eine unbeschränkte Suche durch

☐ Beschränke die Suche auf folgenden Container

Vollqualifizierter Name

Wählen Sie zu importierenden Adressen aus

☒ Alle Adressen

☐ Nur die primäre Adresse

Sie können den Import durch die Eingabe eines angepassten LDAP-Filters beschränken, z. B.: '(division=Marketing)(division=Support)'

Filter (optional)

Speichern und schließen Abbrechen und schließen

Bild 46: Die Auswahl der zu importierenden Active Directory Benutzer

Sie können außerdem einen zusätzlichen LDAP-Filter angeben, um nur Benutzer zu importieren, die ein bestimmtes Attribut mit einem bestimmten Wert gefüllt haben.

In den **Gruppen** ([Bild 47](#)) geben Sie an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.

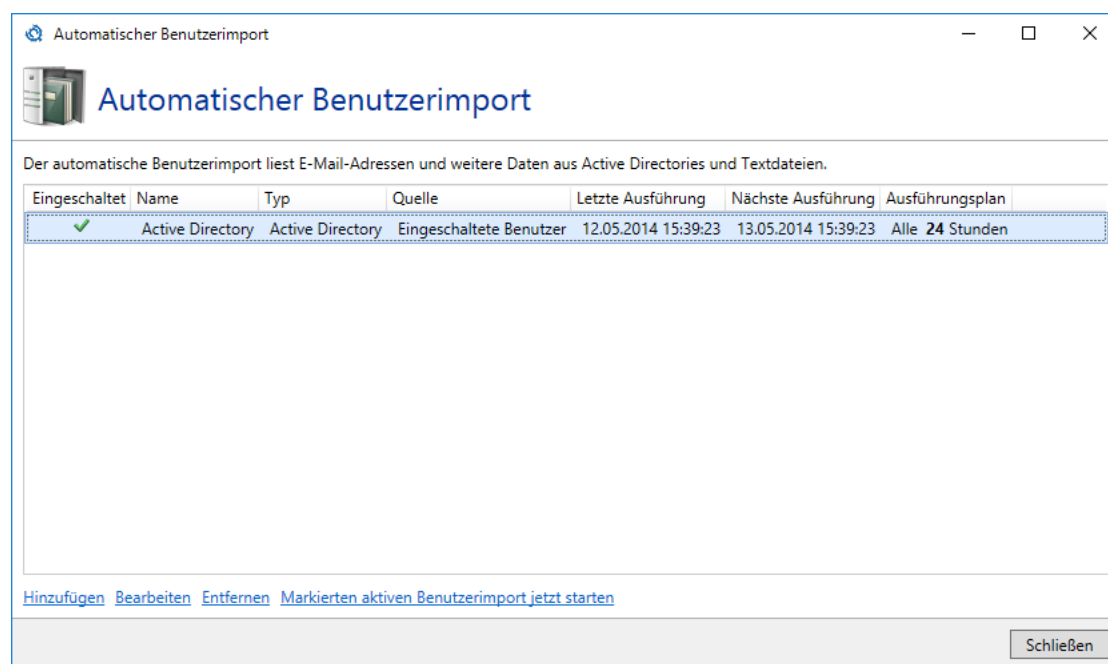
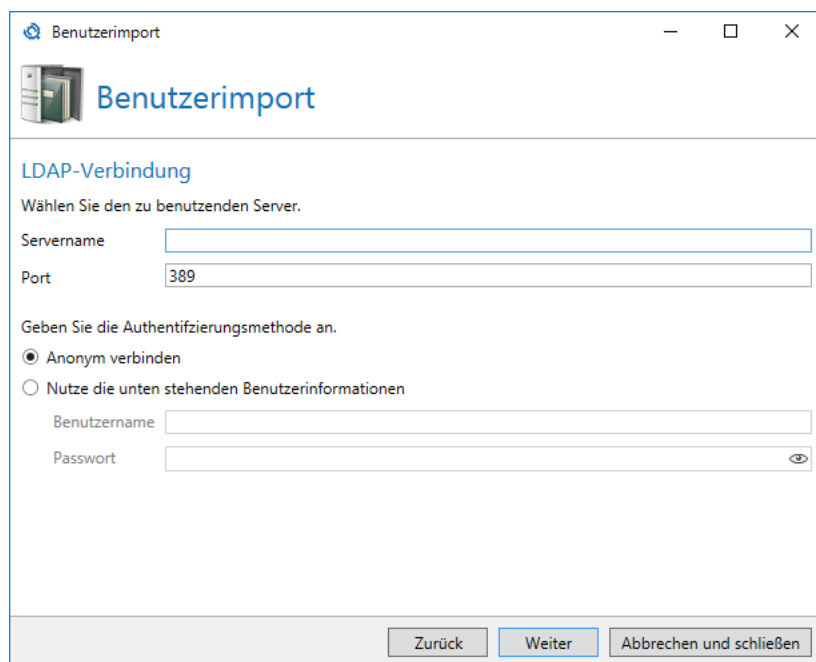


Bild 47: Berechtigte Gruppen für De-Mail

Generisches LDAP

Die **LDAP-Verbindung** ([Bild 48](#)) baut die Verbindung zu Ihrem Server auf. Geben Sie den Server und die zu benutzenden Anmeldeinformationen ein.



Benutzerimport

LDAP-Verbindung

Wählen Sie den zu benutzenden Server.

Servername

Port

Geben Sie die Authentifizierungsmethode an.

☒ Anonym verbinden

☐ Nutze die unten stehenden Benutzerinformationen

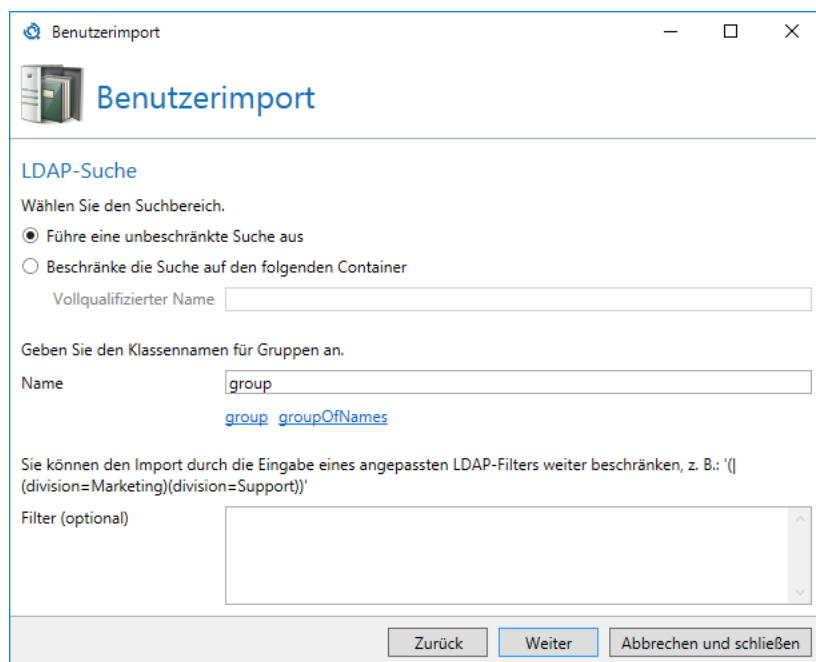
Benutzername

Passwort

Zurück Weiter Abbrechen und schließen

Bild 48: Verbindung zum LDAP-Server

In der **LDAP-Suche** ([Bild 49](#)) können Sie die Suche im Verzeichnis auf bestimmte Container einschränken. Geben Sie bitte Klassennamen an, unter dem die Gruppen zu finden sind. Zusätzlich können Sie mit einem Filter die Suche auf Benutzer mit bestimmten Eigenschaften beschränken.



Benutzerimport

LDAP-Suche

Wählen Sie den Suchbereich.

☒ Führe eine unbeschränkte Suche aus

☐ Beschränke die Suche auf den folgenden Container

Vollqualifizierter Name

Geben Sie den Klassennamen für Gruppen an.

Name

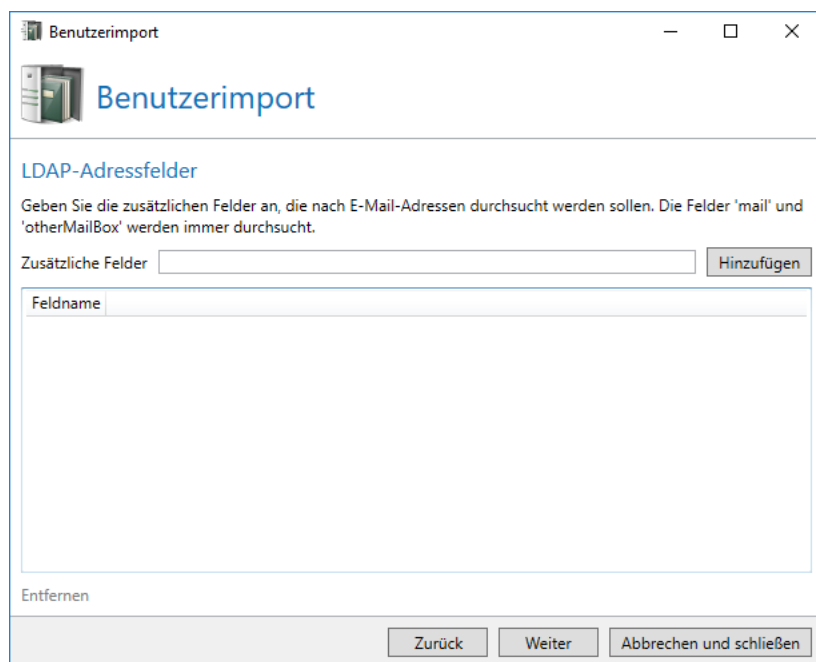
[group](#) [groupOfNames](#)

Sie können den Import durch die Eingabe eines angepassten LDAP-Filters weiter beschränken, z. B.: '([division=Marketing])(division=Support))'

Filter (optional)

Bild 49: Anpassen der LDAP-Suche

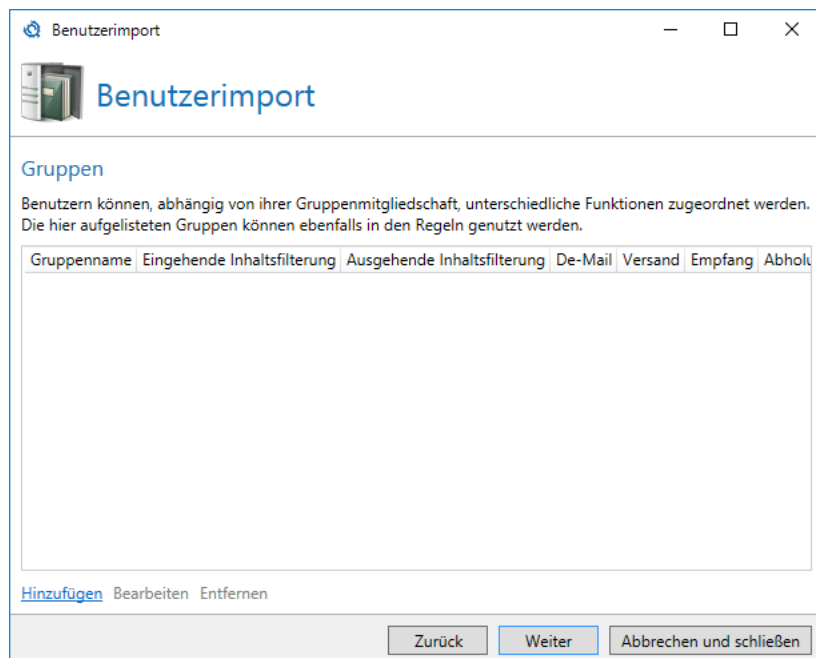
Auf der Seite der **LDAP-Adressfelder** können Sie zusätzliche LDAP-Felder angeben, in denen nach E-Mail-Adressen gesucht werden soll ([Bild 50](#)). Dies ist notwendig, falls Ihr System die E-Mail-Adressen nicht in den Standardfeldern 'mail' bzw. 'otherMailBox' speichert.



The screenshot shows the 'Benutzerimport' window with the 'LDAP-Adressfelder' tab selected. The window title is 'Benutzerimport'. Below the title bar, there is a header area with a server icon and the text 'Benutzerimport'. The main content area is titled 'LDAP-Adressfelder' and contains the following text: 'Geben Sie die zusätzlichen Felder an, die nach E-Mail-Adressen durchsucht werden sollen. Die Felder 'mail' und 'otherMailBox' werden immer durchsucht.' Below this text is a text input field labeled 'Zusätzliche Felder' and a 'Hinzufügen' button. Below the input field is a table with one column labeled 'Feldname'. The table is currently empty. At the bottom of the table area is a link labeled 'Entfernen'. At the bottom of the window are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 50: Konfiguration zusätzlicher Adressfelder

In den **Gruppen** geben Sie an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf ([Bild 51](#)). Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.



The screenshot shows the 'Benutzerimport' window with the 'Gruppen' tab selected. The window title is 'Benutzerimport'. Below the title bar, there is a header area with a server icon and the text 'Benutzerimport'. The main content area is titled 'Gruppen' and contains the following text: 'Benutzern können, abhängig von ihrer Gruppenmitgliedschaft, unterschiedliche Funktionen zugeordnet werden. Die hier aufgelisteten Gruppen können ebenfalls in den Regeln genutzt werden.' Below this text is a table with the following columns: 'Gruppenname', 'Eingehende Inhaltsfilterung', 'Ausgehende Inhaltsfilterung', 'De-Mail', 'Versand', 'Empfang', and 'Abhol'. The table is currently empty. At the bottom of the table area are three links: 'Hinzufügen', 'Bearbeiten', and 'Entfernen'. At the bottom of the window are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 51: Berechtigte Gruppen für De-Mail

Zusätzliche Benutzerfelder

Die **Zusätzlichen Benutzerfelder** eines Benutzers können durch den Benutzerimport direkt mit Werten gefüllt werden.

Lesen Sie im Kapitel über den [Disclaimer](#), wie sie **Zusätzliche Benutzerfelder** innerhalb eines automatischen Benutzerimports konfigurieren.

Textdatei

In den Einstellungen für den Benutzerimport durch Textdateien geben Sie bitte den Pfad zu der Datei mit den Benutzeradressen an ([Bild 52](#)).

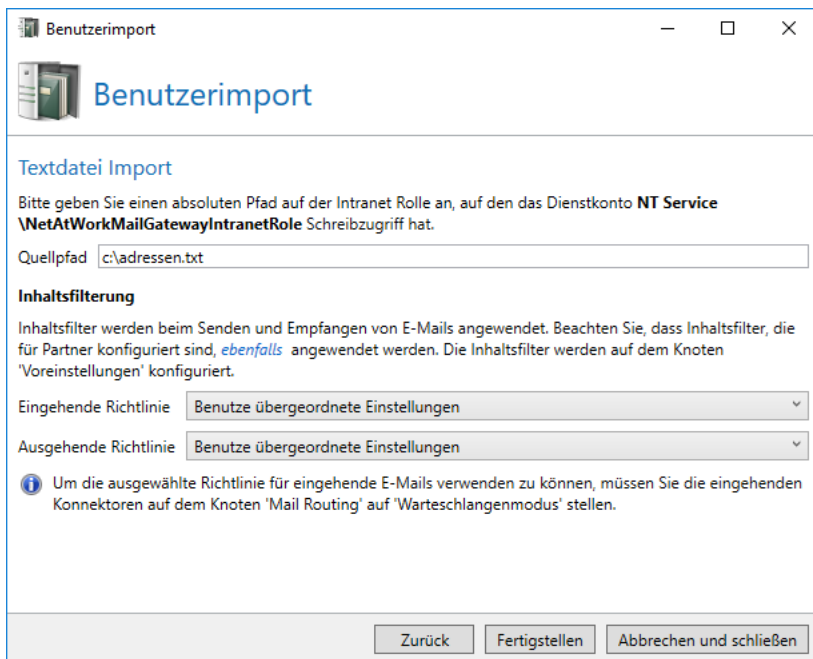


Bild 52: Die Angabe des Pfads zur Textdatei



Die Text-Datei benötigt kein spezielles Format. Alle E-Mail-Adressen werden formatunabhängig gefunden und importiert.

Verfügen Sie über eine Lizenz für NoSpamProxy Large Files oder NoSpamProxy Protection, können Sie hier auch einen Inhaltsfilter für alle zu importierenden Benutzer auswählen. Die Inhaltsfilter werden auf dem Knoten [Inhaltsfilter](#) definiert.



Es werden nur E-Mail-Adressen importiert, wenn die Domäne auch in den [Eigenen Domänen](#) von NoSpamProxy hinterlegt ist. Alle anderen werden nicht importiert.

Partner

Partnerabschnitt

Ein Partner definiert, wie mit externen Kommunikationspartnern E-Mails ausgetauscht werden sollen. Diese Einstellungen können auf allen Partnern, einer Partnerdomäne sowie einer E-Mail-Adresse eines Partners erfolgen. Die Einstellungen auf einer E-Mail-Adresse haben dabei Vorrang vor den Einstellungen auf einer Domäne und die Einstellungen auf einer Domäne haben Vorrang vor der Einstellung für alle Partner.

Standardeinstellungen für Partner

Auf den **Standardeinstellungen für Partner**, den Domäneneinstellungen und den E-Mail-Adressen kann jeweils ein Inhaltsfilter ([Bild 53](#)) für E-Mail-Anhänge gewählt werden. Inhaltsfilter werden auf dem Knoten [Inhaltsfilter](#) definiert.

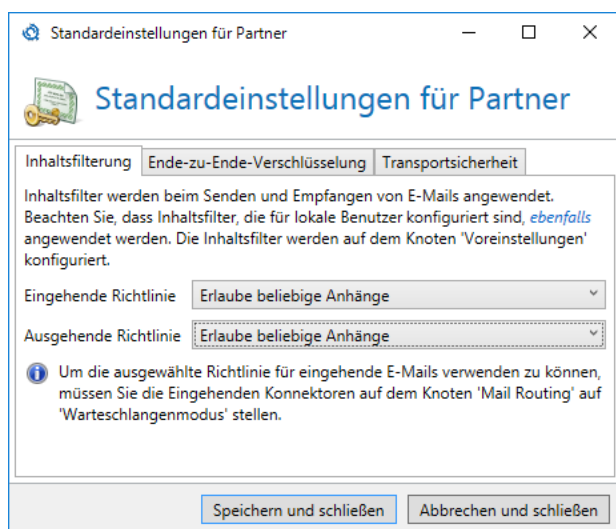


Bild 53: Standardeinstellung der Inhaltsfilter

Für die Benutzung von 'DNS-based Authentication of Named Entities' (DANE) muss in den **Standardeinstellungen für Partner** auch die Benutzung eines DNSSEC-fähigen DNS-Server eingestellt werden ([Bild 54](#)). Durch die Benutzung von DANE werden die TLS-Zertifikate der Transportverschlüsselung überprüft, so dass nur Zertifikate akzeptiert werden, die der Empfänger der E-Mail auch als vertrauenswürdig eingestuft hat. Die Konzepte hinter DANE sind unter https://de.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities nachzulesen.



Um die Absicherung der TLS-Zertifikate über DANE zu erreichen, müssen Sie einen DNSSEC-fähigen DNS-Server auf dem Knoten [Verbundene Systeme](#) im Abschnitt [DNS-Server](#) konfigurieren.

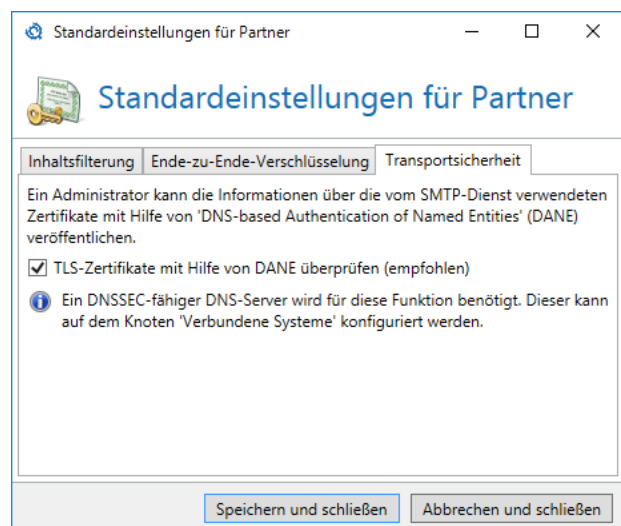


Bild 54: Einstellung für DANE mit TLS-Zertifikaten

Partnerdomänen

Die Liste der Partner ist nach den Domänen gruppiert ([Bild 55](#)). Jede Domäne beinhaltet einerseits Einstellungen für Inhaltsfilter sowie die notwendige Transportsicherheit und das Vertrauen zwischen den Domänen.

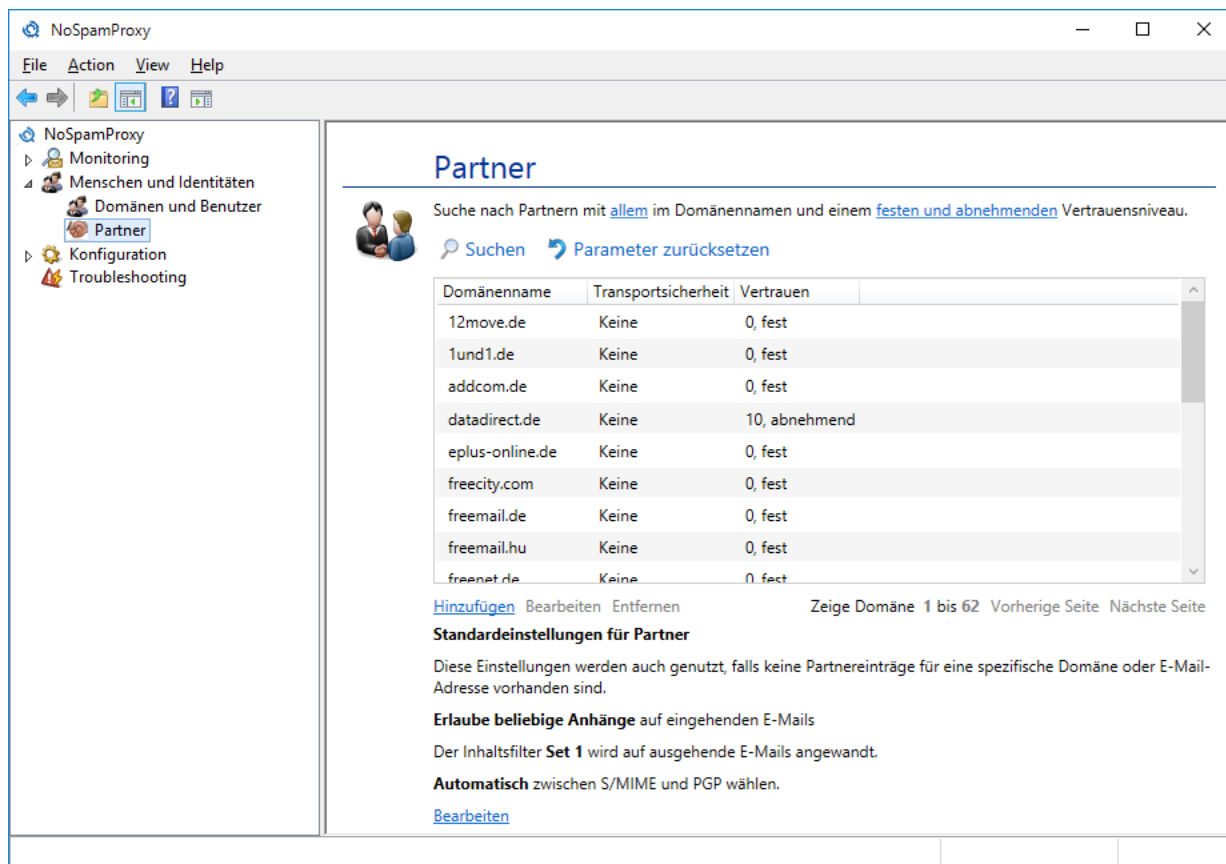


Bild 55: Die Übersicht über alle Partner

Die Einstellungen auf Domänenebene gelten für alle Partner, die keine abweichenden Einstellungen auf ihrer E-Mail-Adresse in den **Benutzereinträgen** konfiguriert haben. Die Einstellungen in einem Benutzereintrag haben Vorrang vor den Einstellungen der Domäne.

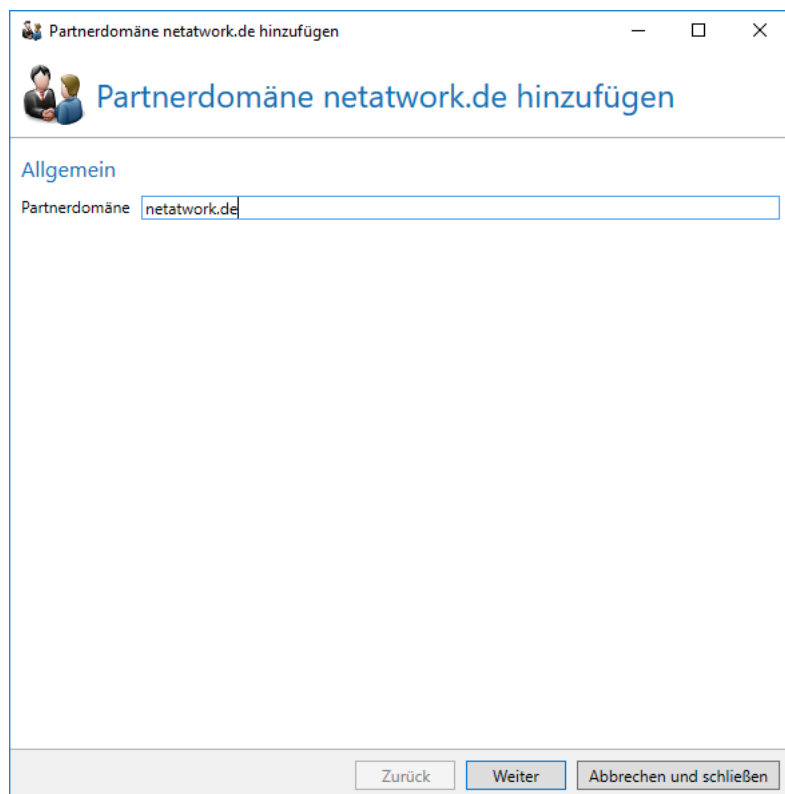
Beim Anlegen einer neuen Partnerdomäne werden die Standardeinstellungen für die komplette Domäne voreingestellt. Dadurch müssen Sie die Einstellungen, die für die meisten Partneradressen gelten sollen, nur einmal konfigurieren. Abweichende Einstellungen auf den Adressen haben Vorrang vor den Einstellungen auf der Domäne.

Die **Notwendige Transportsicherheit** bestimmt, ob E-Mails während des Transports von Server zu Server verschlüsselt werden müssen. Sie können zusätzlich auch Anforderungen an das verwendete Zertifikat stellen und zusätzliche erlaubte Zertifikate hinterlegen. Die notwendige Transportsicherheit wird immer für die gesamte Domäne festgelegt.

Durch NoSpamProxy Protection können Sie das **Vertrauen** in diese Domäne einstellen. Vertrauen wird automatisch durch die laufende E-Mail-Kommunikation mit einem Partner aufgebaut. Vertrauen wird für die gesamte Domäne festgelegt.

Neue Partnerdomäne

Beim Hinzufügen einer Partnerdomäne geben Sie zuerst den Domänennamen an ([Bild 56](#)). Der Domänenname muss hier mit US-ASCII-Zeichen geschrieben werden.



Partnerdomäne netatwork.de hinzufügen

Partnerdomäne netatwork.de hinzufügen

Allgemein

Partnerdomäne

Zurück Weiter Abbrechen und schließen

Bild 56: Der Domänenname

Verfügen Sie über eine Lizenz für NoSpamProxy Large Files oder NoSpamProxy Protection, können Sie im nächsten Schritt die verwendeten Inhaltsfilter auswählen. Die Inhaltsfilter werden auf dem Knoten [Inhaltsfilter](#) definiert.

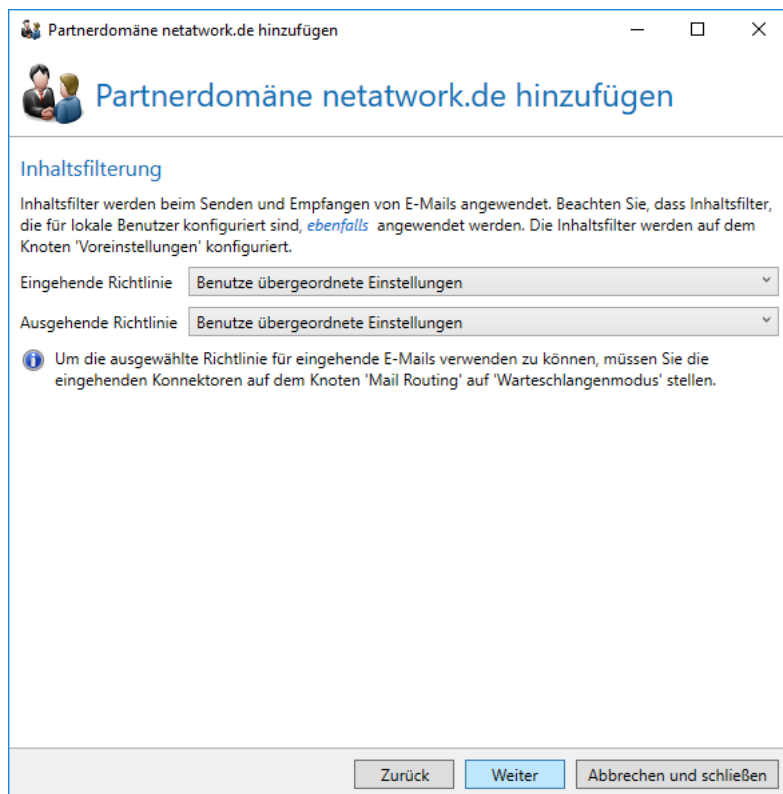


Bild 57: Konfiguration der Inhaltsfilter

Die Transportsicherheit legt fest, ob die Kommunikation zu den Server der Partnerdomäne verschlüsselt erfolgen muss und welchen Zertifikaten gegebenenfalls vertraut wird ([Bild 58](#)). Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielservers eingesetzt werden können. Zum Deaktivieren der Transportsicherheit müssen Sie die Häkchen aus allen Kontrollkästchen entfernen.



Wenn Sie im [E-Mail-Routing](#) als Zustellmethode für externe Adressen **Zustellung über einen speziellen Server** für SMTP ausgewählt haben und in den Einstellungen der Partnerdomäne **Erfordere Verschlüsselung** gewählt haben, wird der Versand an diese Domäne fehlschlagen. NoSpamProxy kann in diesem Fall nicht sicherstellen, dass die Kommunikation bis zum E-Mail-Server des Empfängers verschlüsselt ist.

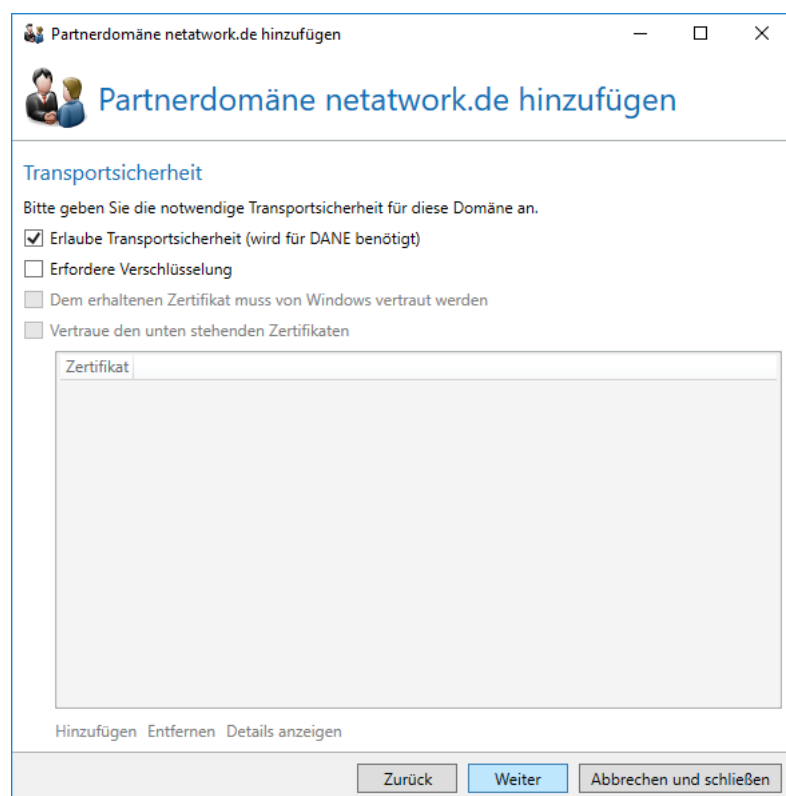


Bild 58: Transportsicherheit

Das **Vertrauen** in eine Domäne ([Bild 59](#)) wird durch an die Domäne gesandte E-Mails stärker und nähert sich ohne weitere E-Mail-Kommunikation mit der Zeit wieder dem Wert '0' an. Sie können das Vertrauen auch auf einen festen Wert einstellen. Ein positiver Wert steht in diesem Fall für Vertrauen, also Bonuspunkte, negative Werte für Misstrauen, also Malus Punkte.

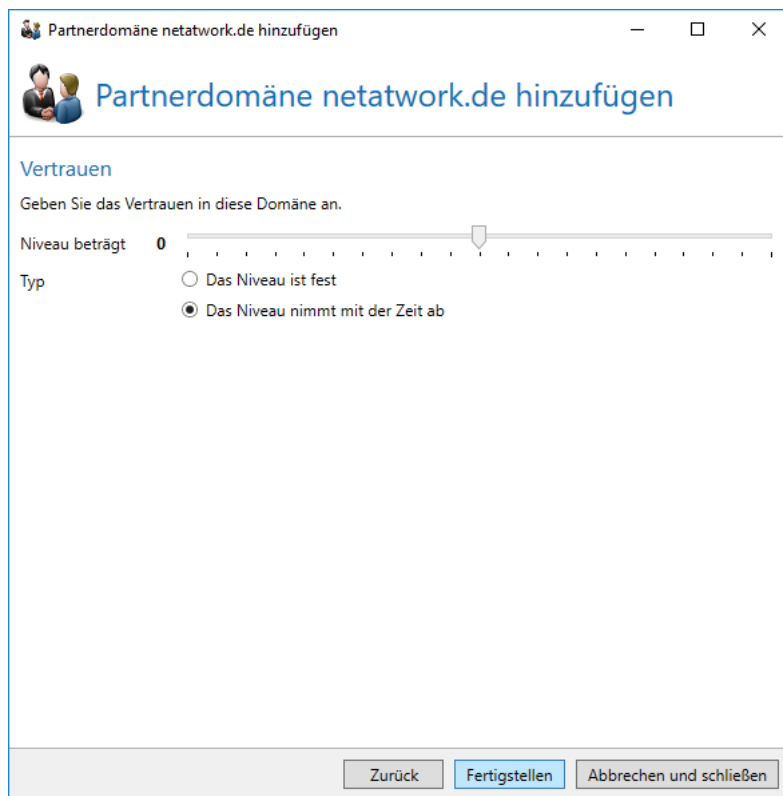


Bild 59: Das Vertrauen in eine Domäne

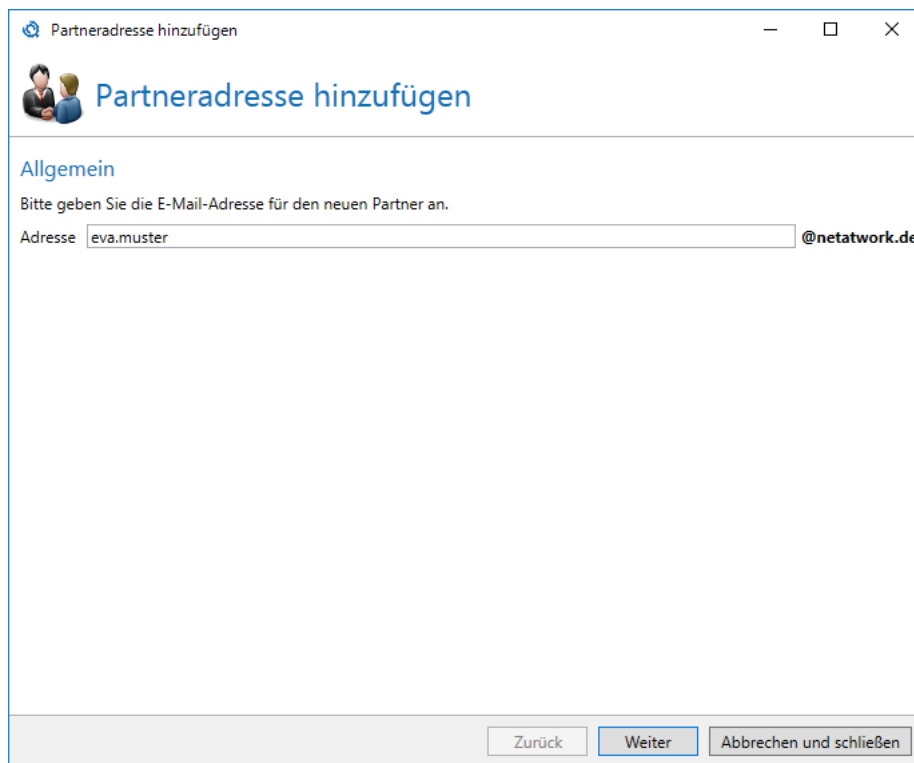
Partnerdomäne bearbeiten

Beim Bearbeiten eines Partners können die Einstellungen aus der [Domäne](#) angepasst werden. Beim Bearbeiten eines Partners sind zusätzliche Bereiche verfügbar.

Benutzereintrag einer Partnerdomäne

Das Anlegen eines Benutzereintrags läuft analog zur Anlage einer [Domäne](#). Ein Benutzereintrag ist dabei einer E-Mail-Adresse zugeordnet und überstimmt die Einstellungen auf der Domäne, wenn mit dieser E-Mail-Adresse kommuniziert wird.

Zuerst wird die E-Mail-Adresse eingegeben ([Bild 60](#)). Bitte geben Sie den lokalen Teil (vor dem @-Zeichen) der E-Mail-Adresse in das Feld **Partneradresse** ein. Der Domänenteil wird bereits hinter dem Eingabefeld angezeigt.



Partneradresse hinzufügen

Partneradresse hinzufügen

Allgemein

Bitte geben Sie die E-Mail-Adresse für den neuen Partner an.

Adresse @netatwork.de

Zurück Weiter Abbrechen und schließen

Bild 60: Hinzufügen einer E-Mail-Adresse eines Partners

Im nächsten Schritt legen Sie einen Inhaltsfilter fest.

Open Keys Web Service nutzen

Der Open Keys Web Service ist die zentrale Sammelstelle für öffentliche Zertifikate und der beste Weg, öffentliche Zertifikate abzufragen und zu erhalten. Wir empfehlen Ihnen, Open Keys zu nutzen.

Der Open Keys Web Service wird standardmäßig genutzt, um öffentliche Zertifikate abzufragen. Sollte der Dienst deaktiviert sein, gehen Sie folgendermaßen vor:

Klicken Sie unter **Öffentliche Schlüsselserver/Open Keys** auf **Bearbeiten**.



Bild 61: Den Open Keys Web Service nutzen

Setzen Sie das Häkchen neben **Nutze Open Keys (empfohlen)** und klicken Sie dann **Speichern und schließen**.

Zusätzliche Benutzerfelder



Für die Benutzung der zusätzlichen Benutzerfelder müssen Sie den Disclaimer lizenziert haben.

Sie können die Daten Ihrer Unternehmensbenutzer um zusätzliche Felder erweitern. Diese Felder können Sie anschließend in Ihren Disclaimer-Vorlagen als Platzhalter einfügen. Beim Anhängen des Disclaimers an eine E-Mail werden diese Platzhalter dann durch die Daten des Absenders ersetzt.

Bei manuell angelegten Benutzern können Sie die hier definierten Felder direkt auf dem Benutzer-Objekt bearbeiten. Importieren Sie Ihre Benutzer aus einem entfernten System, so können Sie über den [Automatischen Benutzerimport](#) festlegen, wie diese Felder gefüllt werden.

Bei Bedarf können Sie einen Standardwert vorgeben. Dieser Wert wird verwendet, wenn auf dem Benutzer selbst kein Wert gesetzt wird.

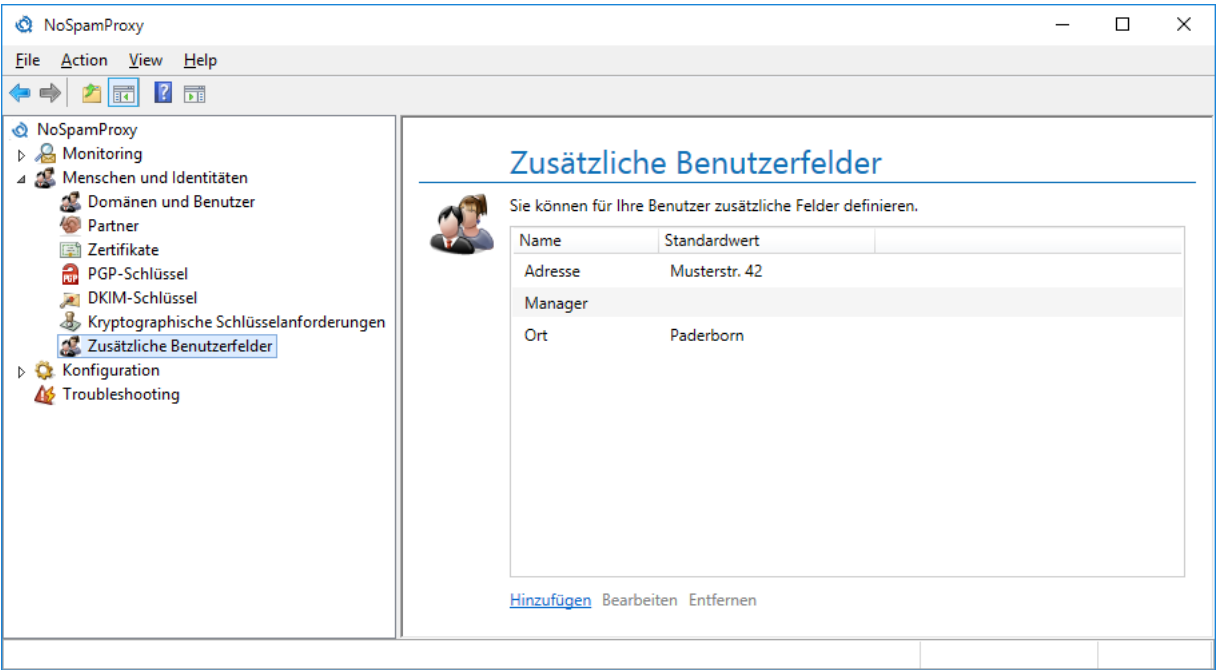


Bild 62: Liste aller benutzerdefinierten Felder

9. Konfiguration

Unter dem Knoten **Konfiguration** der Intranet Rolle befinden sich Einstellungen für Verbindung zu anderen Rollen, Einstellungen der Datenbank sowie Benachrichtigungsadressen. ([Bild 63](#)).

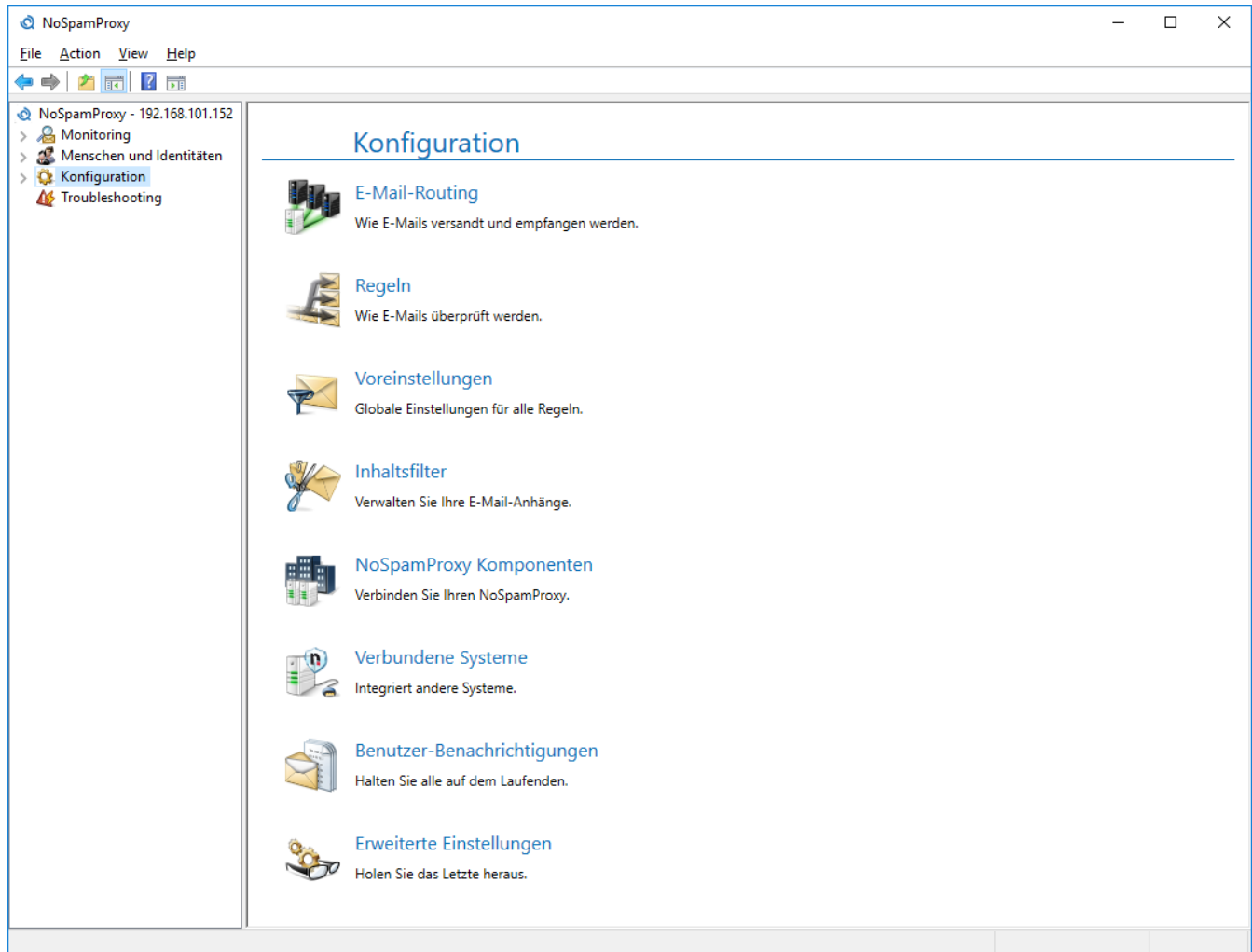


Bild 63: Einstellungen der Intranet Rolle

E-Mail-Routing

Unter dem Knoten **E-Mail-Routing** ([Bild 87](#)) befinden sich die Konnektoren für die Zustellung [lokaler](#) sowie [externer](#) E-Mails. Unter dem Punkt [Empfangskonnektoren](#) können Sie einstellen, wie NoSpamProxy E-Mails empfängt. Zusätzlich konfigurieren Sie hier die lokalen Server.

Lokale E-Mail-Server

Hier geben Sie alle E-Mail-Server an, die eigene Domänen als Absender für E-Mails nutzen dürfen. Lokale Server werden über verschiedene Wege identifiziert:

- **IP-Adresse**
Ein Server gilt als lokal, sofern er von der angegebenen IP-Adresse sendet ([Bild 65](#)).
- **Subnetz**
Ein Server gilt als lokal, sofern er von einer Adresse im angegebenen Subnetz sendet. Ein Subnetz wird in der CIDR-Schreibweise angegeben, z.B. 192.168.100/24 ([Bild 65](#)).
- **DNS-Domänenname**
Ein Server gilt als lokal, sofern der hier konfigurierte DNS-Hostname auf die Adresse des Servers verweist ([Bild 65](#)).
- **TLS-Zertifikat**
Ein Server gilt als lokal, sofern er während der Verbindung eine TLS-Authentifizierung mit Client-Zertifikat durchführt. Wird hier ein Stamm- oder Zwischenzertifikat eingetragen, dann muss sich der Server mit einem Zertifikat melden, dass das konfigurierte Zertifikat in seiner Zertifikatskette enthält. Wird ein End-Zertifikat eingetragen, so muss sich der Server mit exakt diesem Zertifikat melden ([Bild 66](#)).
- **Office 365**
Hierüber können Sie Office 365 als lokalen Server eintragen. Ein Server gilt als lokal, wenn es sich um einen offiziellen "Office 365"-Server handelt ([Bild 67](#)).



Wenn Sie Office 365 als lokalen Server konfigurieren, so wird die Zustellung lokaler Nachrichten automatisch auf die [Zustellung über Warteschlangen](#) umgestellt, da direkte Zustellung nicht möglich ist. Des Weiteren wird ein Sendekonnektor für Office 365 konfiguriert.

Beim Hinzufügen von neuen lokalen E-Mail-Servern wählen Sie zunächst die Art des Servers aus ([Bild 64](#)). Im zweiten Schritt konfigurieren Sie die typspezifischen Einstellungen. Anschließend können Sie auswählen, ob der Konnektor nur für bestimmte eigene Domänen zuständig ist, oder für alle ([Bild 69](#)). Abschließend können Sie noch einen Kommentar verfassen ([Bild 70](#)).

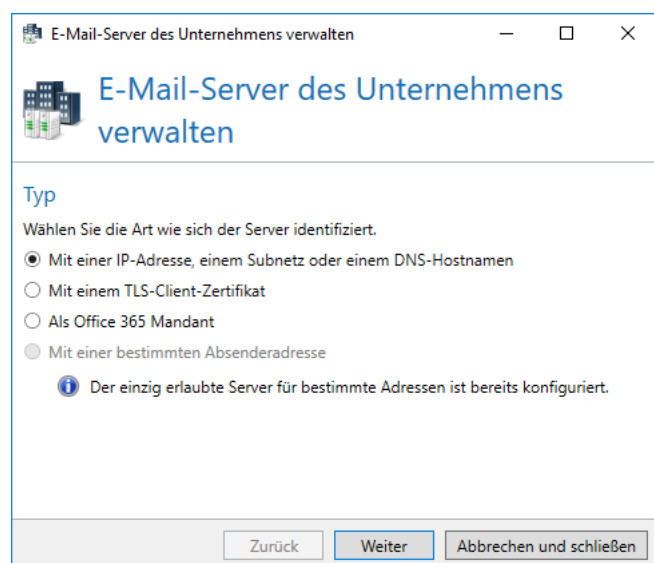


Bild 64: Die Auswahl des Server-Typs

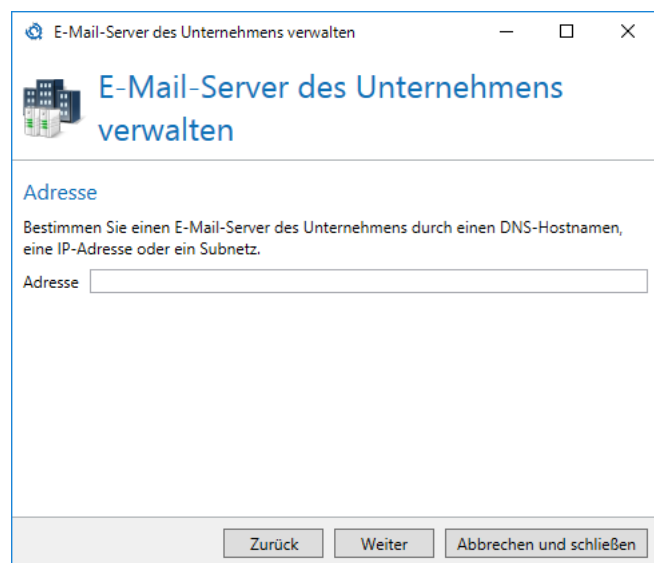


Bild 65: Authentifizierung über IP-Adresse, Subnetz-Zugehörigkeit oder DNS-Hostname

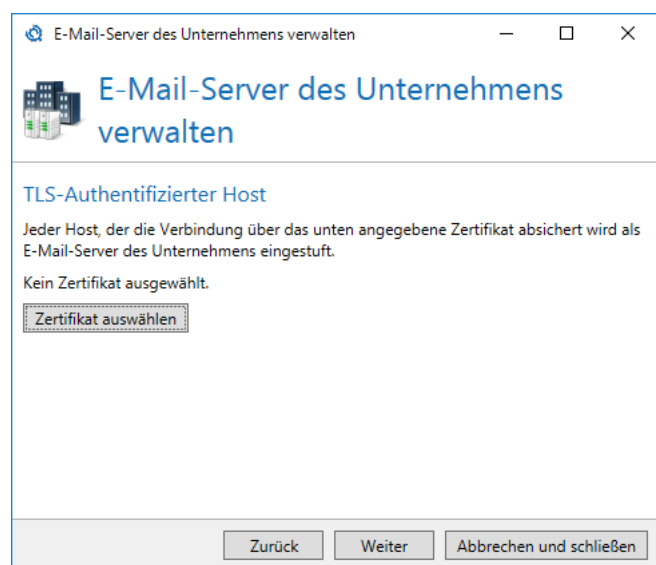


Bild 66: Authentifizierung über TLS-Zertifikat

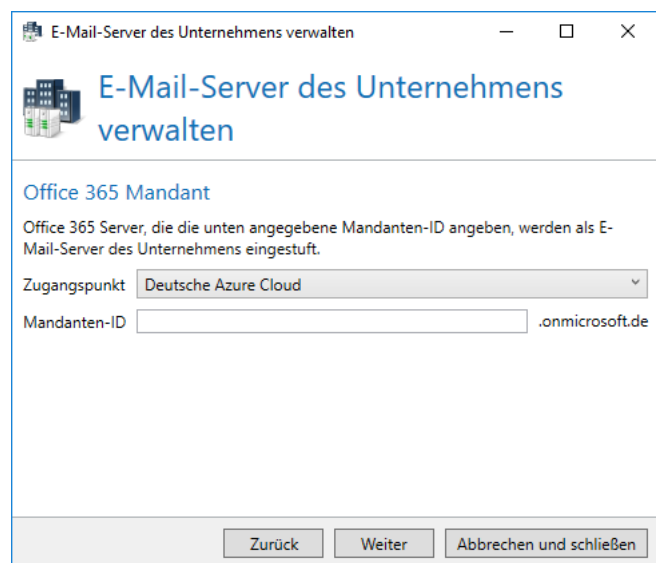


Bild 67: Authentifizierung über Office-365-Mandanten-ID

The screenshot shows a window titled 'E-Mail-Server des Unternehmens verwalten'. The main heading is 'E-Mail-Server des Unternehmens verwalten'. Below it, the section is 'Bestimmte Absenderadresse'. The text explains that any server using a 'From' address matching a specified pattern will be treated as a company email server. A warning icon and text state that 'From' addresses can be easily spoofed and this option should only be used if no other way to identify the server exists, and that the rule set must be adjusted to prevent relay abuse. There is a large text input field labeled 'Adresse'. At the bottom left are links 'Hinzufügen' and 'Entfernen'. At the bottom right are buttons 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 68: Authentifizierung über eine bestimmte E-Mail-Adresse

The screenshot shows the same window, but the section is 'Zugeordnete eigene Domänen'. The text states that the email server can be restricted to specific domains. There are two radio button options: 'Der Server kann E-Mails mit beliebigen Absenderdomänen versenden.' (selected) and 'Nur die unten markierten Domänen können verwendet werden.' Below the options is a list box with the header 'Name' containing four entries, each with a checkbox: 'beispiel1.local', 'beispiel2.local', 'beispiel3.local', and 'beispiel4.local'. At the bottom right are buttons 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 69: Geben Sie an, mit welchen eigenen Domänen der Server E-Mails versenden darf

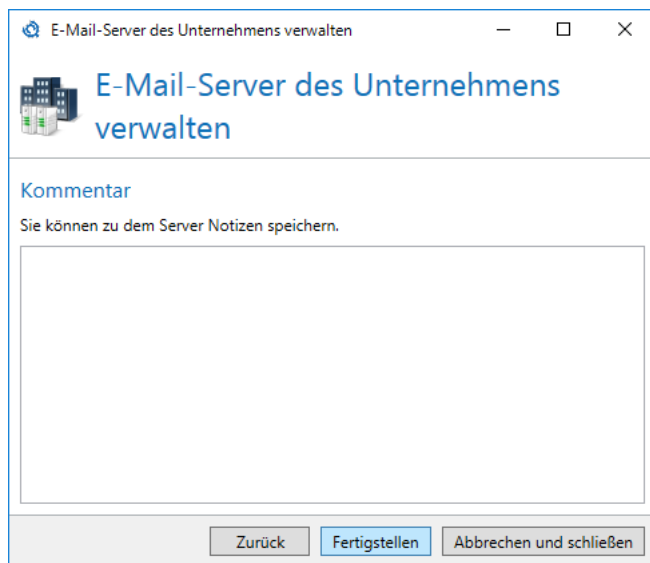


Bild 70: Sie können optional einen Kommentar verfassen

Mehrfach verwendete Einstellungen der Konnektoren

Einige Einstellungen werden in unterschiedlichen Konnektoren mehrfach verwendet. Diese werden in den folgenden Kapiteln erläutert.

Name

Sie müssen über das Feld **Name** jedem Konnektor einen eigenen Namen geben. Der Name muss gegenüber anderen Konnektoren aus dem gleichen Bereich eindeutig sein. Der Name hilft Ihnen dabei, unterschiedliche Konnektoren zu unterscheiden. Sie können ihn dazu nutzen, die Funktion des Konnektors kurz zu beschreiben.

Bindung an Gateway Rollen

Je nach Typ des Konnektors kann er entweder auf mehreren Gateway Rollen parallel oder nur auf einer einzelnen Rolle verwendet werden. Wählen Sie hier die Gateway Rollen aus, auf denen Sie den Konnektor betreiben möchten.

Kosten

Die **Kosten** werden genutzt, wenn mehrere Sendekonnektoren für die Zustellung einer E-Mail genutzt werden können. In einem solchen Fall wird der Konnektor mit den geringsten Kosten genutzt. Sollte die E-Mail über diesen Konnektor nicht zugestellt werden können, ist die E-Mail-Zustellung endgültig fehlgeschlagen. In diesem Fall werden keine weiteren Konnektoren mit höheren Kosten genutzt.

Verbindungssicherheit

Die Verbindungssicherheit ([Bild 71](#)) legt die Verschlüsselung der Transportverbindung fest. Der hier beschriebene Dialog wird bei den unterschiedlichen Konnektoren mehrfach benutzt. Dabei sind in einigen Konnektoren einzelne Konfigurationsoptionen ausgeblendet.



Hierbei handelt es sich um die Verschlüsselung auf dem Transportweg. Eine Ende-zu-Ende-Verschlüsselung ist hier nicht gemeint.

Empfangskonnektor

Verbindungssicherheit

Sicherheitseinstellungen

- ☒ Erlaube StartTLS als Verbindungssicherheit (empfohlen)
- ☐ Verlange StartTLS als Verbindungssicherheit
- ☐ Verlange SMTPS als Verbindungssicherheit
- ☐ Verbindungssicherheit abschalten

Server-Identität

Kein Zertifikat ausgewählt.

Falls sich Ihr Zertifikat auf einer Smartcard befindet, benötigen Sie im Allgemeinen eine PIN, um darauf zuzugreifen.

Zertifikats PIN

Notwendige Client-Identität

Verbindungen von jedem Server sind erlaubt.

Notwendige Client-Identität bearbeiten

Bild 71: Einstellungen für die Verbindungssicherheit

SMTP Sicherheitseinstellungen

Im Abschnitt **Sicherheitseinstellungen** können Sie den Sicherheitsgrad für die Übermittlung von E-Mails an lokale Adressen festlegen. Folgende Einstellungen sind möglich:

- **Verbindungssicherheit durch StartTLS erlauben (empfohlen)**
In diesem Modus ist die Verschlüsselung der Verbindungen möglich, aber nicht erzwungen. Dem einliefernden Server ist es freigestellt, die Verbindung via StartTLS zu verschlüsseln. In diesem Modus müssen Sie Empfangskonnektoren ein Zertifikat im Bereich [Server-Identität](#) zur Verfügung stellen. Sendekonnektoren können Sie optional ein Zertifikat im Bereich [Client-Identität](#)

zur Verfügung stellen, um die Identität des sendenden Servers für den empfangenden Server sicher zu stellen.

- **Verbindungssicherheit durch StartTLS verlangen**

Wenn Sie sicherstellen möchten, dass alle Verbindungen über den entsprechenden Empfangskonnektor verschlüsselt werden, müssen Sie diese Option auswählen. Nun verlangt NoSpamProxy zwingend eine verschlüsselte Verbindung vom einliefernden Server via StartTLS. Auch in diesem Modus müssen Sie dem Gateway ein Zertifikat im Abschnitt [Server-Identität](#) zur Verfügung stellen.

- **TLS als Verbindungssicherheit nutzen**

Mit dieser Einstellung erwartet ein SMTP-Konnektor einen Verbindungsaufbau mittels SMTPS. Ein POP3 Konnektor erwartet POP3S. Verwenden Sie diese Einstellung nur dann, wenn es zwingende Gründe dafür gibt. Das StartTLS-Verfahren ist das modernere und mittlerweile gängige Verfahren zur Verbindungsverschlüsselung. Normalerweise wird für SMTPS ein separater Port (üblicherweise 465) verwendet, da die Verbindung automatisch verschlüsselt erwartet wird, ähnlich wie bei HTTPS über den Port 443.

- **Verbindungssicherheit abschalten**

Mit dieser Einstellung werden Verbindungen niemals verschlüsselt. NoSpamProxy bietet dann einliefernden Servern keine Verbindungssicherheit an.



SMTPS auf Port 25 ist nicht RFC konform. Nutzen Sie stattdessen einen eigenen Empfangskonnektor, den Sie auf den Port 465 legen.



Das notwendige Verschlüsselungsniveau für Verbindung mit StartTLS oder SMTPS beträgt mindesten 128 Bit. Verbindungen mit einer kleineren Verschlüsselungsstärke werden nicht angenommen. Des Weiteren werden nur TLS-Verbindungen zugelassen. SSL-Verbindungen werden nicht unterstützt, da sie nicht mehr als sicher gelten.

Server- oder Client-Identität

Für die Verschlüsselung der Transportverbindung werden SSL-Zertifikate benötigt. Der empfangende E-Mail-Server benötigt zwingend ein Zertifikat als Server-Identität, um die Verschlüsselung der Verbindung zu ermöglichen. Der sendende E-Mail-Client kann mit einem Zertifikat seine eigene Client-Identität belegen.

- **Server-Identität**

Ein SSL-Zertifikat im Empfangskonnektor wird genutzt, um eine Verbindungssicherheit bereitstellen zu können. Mithilfe des Zertifikats als Server-Identität beim empfangenden E-Mail-Server wird die Verschlüsselung durch StartTLS bzw. TLS ermöglicht. Ohne Zertifikat muss die Verschlüsselung für Verbindungen deaktiviert werden.

- **Client-Identität**

Ein SSL-Zertifikat in SMTP Sendekonnektoren wird genutzt, um die Identität des sendenden E-Mail-Servers sicher zu stellen. Auch ohne Zertifikat als Client-Identität kann die Verbindungssicherheit durch StartTLS bzw. TLS genutzt werden, da das Zertifikat der Server-Identität des empfangenden Servers für die Verschlüsselung der Transportverbindung ausreicht.



Beim Hinzufügen eines Zertifikats für die Transportverschlüsselung durch StartTLS benötigt die Gateway Rolle Leserechte auf den privaten Schlüssel. Diese Rechte für die Rolle werden automatisch erteilt. Sie müssen allerdings einmal die Gateway Rolle stoppen und wieder starten, damit diese Änderung wirksam wird und die Gateway Rolle Leserechte auf dem privaten Schlüssel des genutzten Zertifikats erhält. Es erscheint auch ein entsprechender Warnhinweis in der Oberfläche.

Nach der Auswahl des Zertifikats müssen Sie ggf. einen PIN-Code in das Feld **Zertifikats PIN (optional)** eingeben, falls der Zertifikatsspeicher die Zertifikate mit einem solchen geschützt hat.



Bitte kontrollieren Sie die Eingabe Ihrer PIN sehr sorgfältig, da viele der durch einen PIN-Code geschützten Zertifikate durch dreimalige Falscheingabe unwiderruflich zerstört werden.

Wird für Verbindungen SSL erzwungen, so können Sie im Punkt **Notwendige Client-Identität** noch einschränken, welche Clients sich verbinden dürfen indem Sie den Zugriff nur erlauben sofern sich die Gegenstelle mit einem passenden Zertifikat authentifiziert ([Bild 72](#)):

- **Erlaube Verbindungen von jedem Server**
Jeder Server darf sich verbinden.
- **Verlange ein Zertifikat**
Das von der Gegenstelle vorzulegende Zertifikat hängt vom hier ausgewählten Zertifikat ab: Bei einem Zwischen- oder Stammzertifikat muss sich die Gegenstelle mit einem Zertifikat ausweisen, das das gewählte Zertifikat in der Zertifikatskette hat. Bei einem Endzertifikat muss sich die Gegenstelle mit exakt diesem Zertifikat ausweisen.
- **Verlange ein vertrautes Zertifikat**
Die Zertifikatskette des vorgelegten Zertifikats muss über die Zertifikate des Windows-Zertifikatsspeichers auflösbar sein.

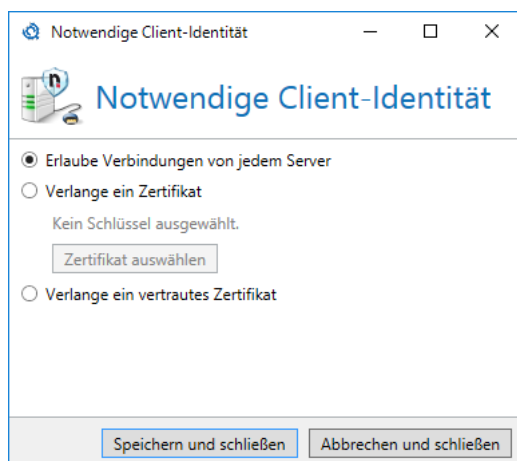


Bild 72: Festlegung der notwendigen Client-Identität

DNS Routing Einschränkungen durch Konnektor-Namensräume

Ein Sendekonnektor kann auch so konfiguriert werden, dass er E-Mails nur für einen Teilbereich des zur Verfügung stehenden DNS-Namensraums zustellt. Sollten mehrere Konnektoren auf eine E-Mail zutreffen, so wird der Konnektor mit den niedrigsten Kosten verwendet.

Standardmäßig wird in einem neuen Konnektor ein Namensraum von "*" als Absenderdomäne und "*" als Empfängerdomäne automatisch angelegt. Dadurch ergibt sich bei einem neuen Konnektor keine Einschränkung im DNS Namensraum, da der Platzhalter "*" jedem möglichen Namen entspricht. Falls der von Ihnen angelegte Konnektor nicht alle Domänen verwalten soll, müssen Sie den Standard-Namensraum löschen und durch einen anderen Namensraum ersetzen.

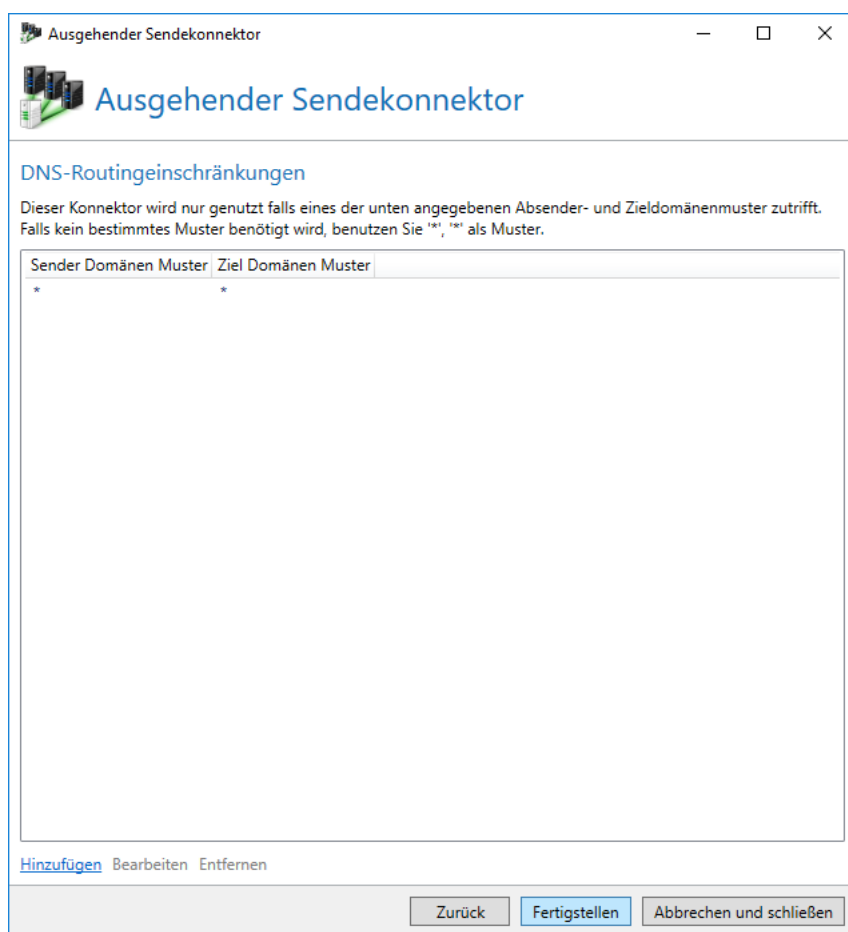


Bild 73: Die Konnektor-Namensräume bestimmen, welche Absender- oder Empfänger-Domänen von einem Konnektor verwaltet werden

Ein Konnektor-Namensraum ([Bild 74](#)) besteht aus einem Muster für sowohl die "Sender Domäne" als auch "Ziel Domäne". Dieses Muster darf auch Platzhalter ('*' und '?') enthalten.

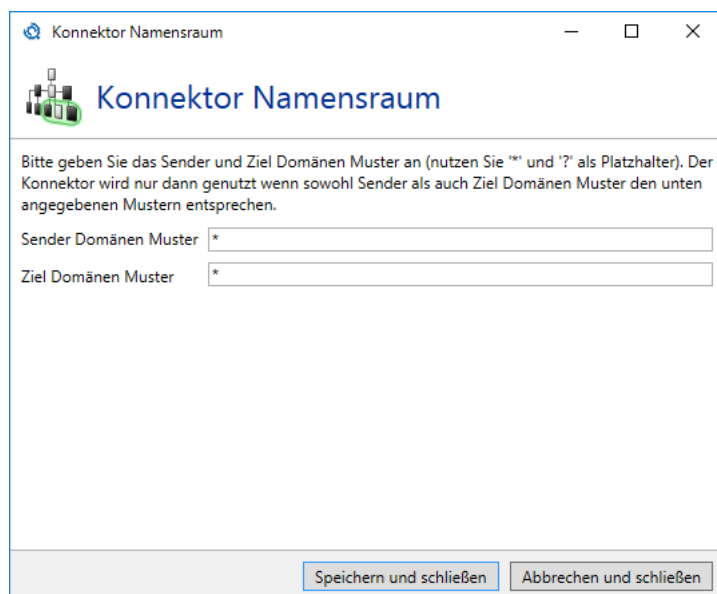


Bild 74: Eine Definition eines DNS Namensraums

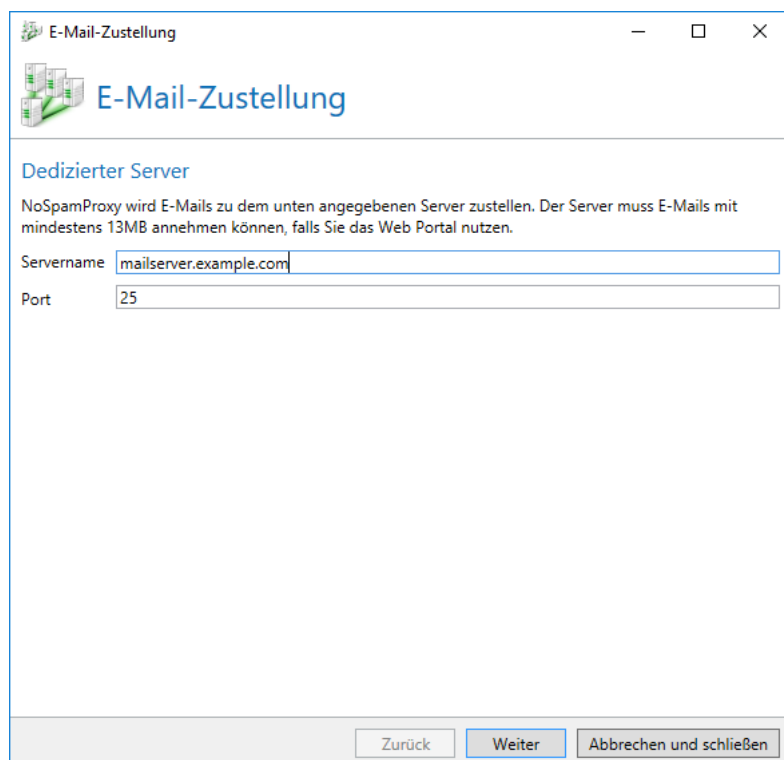
Beispiel: Um einen Sendekonnektor für externe Adressen zu bauen, der nur E-Mails von der Domäne "example.com" an die Domäne "netatwork.de" versendet, müssen folgende Einstellungen getätigt werden.

Sender Domänen Muster	Ziel Domänen Muster
example.com	netatwork.de

Smarthost: E-Mail-Zustellung über dedizierten Server

Ein Smarthost ist ein dedizierter Server für die Zustellung von E-Mails. Smarthosts stehen zum Beispiel bei Ihrem Internet Provider oder auch im eigenen Firmennetz, falls nur über diesen Server E-Mails versendet werden dürfen.

Geben Sie auf der Seite **Dedizierter Server** die IP-Adresse oder den Servernamen und den Port des dedizierten Servers ein ([Bild 75](#)). Dies ist in der Regel die IP-Adresse bzw. der Servername des nächsten Mailsystems für E-Mails.



E-Mail-Zustellung

Dedizierter Server

NoSpamProxy wird E-Mails zu dem unten angegebenen Server zustellen. Der Server muss E-Mails mit mindestens 13MB annehmen können, falls Sie das Web Portal nutzen.

Servername

Port

Bild 75: Verbindungseinstellungen für den dedizierten Server



Wir empfehlen, Adressen nach Möglichkeit nicht als IP-Adresse, sondern mit Servernamen einzugeben.

Für externe Smarthosts, wie zum Beispiel den Ihres Providers, werden häufig Benutzername und Kennwort für die Authentifizierung verlangt. Diese können Sie auf der Registerkarte **Authentifizierung** angeben ([Bild 76](#)).

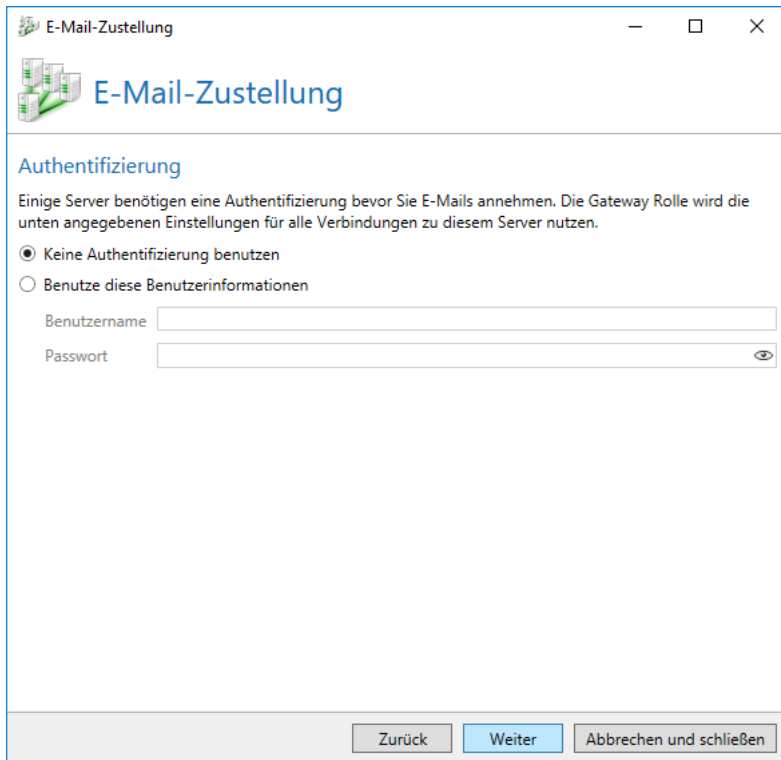


Bild 76: Hier können Sie ggf. Anmeldeinformationen für den dedizierten Server hinterlegen



NoSpamProxy unterstützt als Authentisierungsverfahren die Methode "Basic". Bei dieser Methode werden Benutzername und Kennwort unverschlüsselt über das Internet übertragen. Sofern Ihr Provider das unterstützt, sollten Sie die Verbindungssicherheit für die Verbindungen aktivieren.

Die Optionen für die Verbindungssicherheit zu Smarthosts müssen Sie, wie im Kapitel [Verbindungssicherheit](#) beschrieben, konfigurieren ([Bild 77](#)). SMTP-Sendekonnektoren für E-Mails an externe Adressen nutzen die zertifikatsbasierte Identität als [Client-Identität](#).

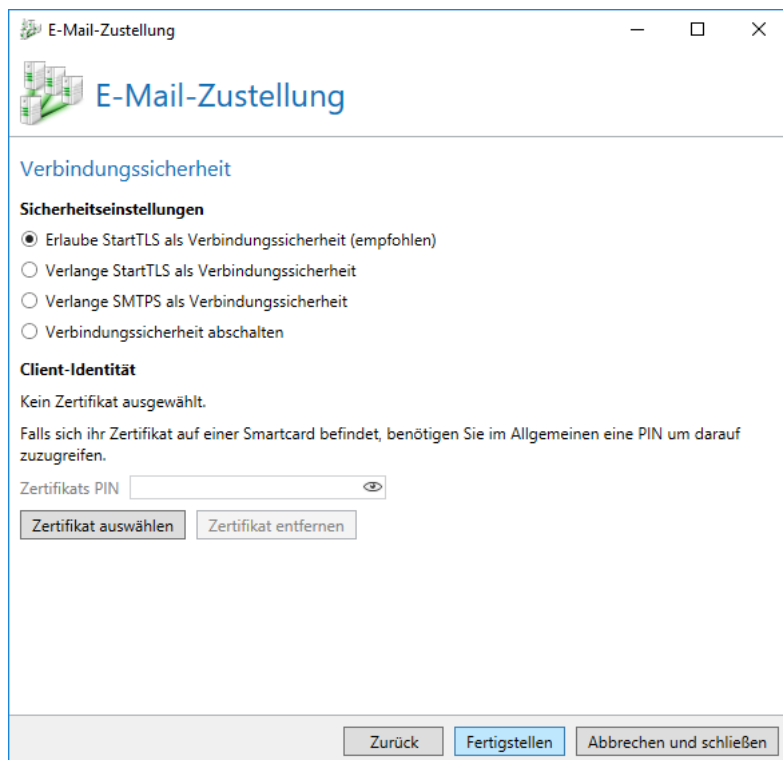


Bild 77: Verbindungssicherheit eines SMTP-Smarthosts



Wenn Sie die E-Mails an externe Adressen über einen weiteren Smarthost verschicken und in den Vertrauensstellungen bei einer Domäne die Verschlüsselung erzwingen, wird der Versand an diese Domäne fehlschlagen, sofern der Smarthost für die E-Mails keine Verschlüsselung unterstützt. Sie müssen also dafür sorgen, dass der Smarthost für die E-Mails StartTLS immer unterstützt.

Lokale Zustellung

Unter dem Punkt **lokale Zustellung** legen Sie fest, an welche Server E-Mails an lokale Adressen weitergeleitet werden.

Die lokale Zustellung von E-Mails kann hier entweder über das **Warteschlangensystem** erfolgen oder - wie bei einem Proxy - direkt zum lokalen E-Mail-Server zugestellt werden. Dabei ist zu beachten, dass die Zustellung über Warteschlangen mehrere Smarthosts und die direkte Zustellung nur einen Smarthost unterstützt. Genauer werden die Unterschiede in den folgenden Kapiteln erläutert.

Zustellung über Warteschlangen

In diesem Modus wird NoSpamProxy die E-Mail nach dem Empfang zunächst in eine Warteschlange legen und dann erst an den oder die konfigurierten Smarthosts weiterleiten. Für den erfolgreichen Empfang der E-Mail ist es nicht relevant, ob der nächste Smarthost erreichbar ist oder nicht.



Auch im Warteschlangenmodus wird die E-Mail noch während der Übertragung von NoSpamProxy Protection auf Viren und den Spamgehalt überprüft und gegebenenfalls abgewiesen.

Wenn Sie für den Sendekonnektor den Warteschlangenmodus auswählen, wird eine eventuell existierende Konfiguration durch den neu konfigurierten Warteschlangenmodus ersetzt. Wenn Sie zum Warteschlangenmodus wechseln, wird sofort der erste SMTP-Konnektor konfiguriert.

Wenn Sie [Office 365](#) zu den lokalen Servern hinzugefügt haben, dann sehen Sie hier einen "Office 365"-Konnektor. Dieser ist für die Zustellung lokaler E-Mails an Office 365 zuständig. Abgesehen von der Bindung an bestimmte Gateway Rollen können Sie diesen Konnektor nicht modifizieren oder löschen.

Allgemeine Einstellungen

Geben Sie einen [Namen](#) ein und wählen Sie eine oder mehrere [Gateway Rollen](#) aus. Legen Sie anschließend die [Kosten](#) des Konnektors fest.

SMTP Verbindungen

Unter den SMTP-Verbindungen können Sie mehrere Smarthosts konfigurieren. Es wird versucht, die E-Mail nacheinander an einen der konfigurierten Smarthosts zuzustellen. Die Reihenfolge ist hierbei weder konfigurierbar noch vom Benutzer beeinflussbar. Sobald ein Smarthost die E-Mail empfängt, ist die E-Mail erfolgreich zugestellt.

Konfiguration eines Smarthosts

Die Konfiguration eines Smarthosts für die lokale Zustellung läuft ab, wie im Kapitel [Smarthost: E-Mail-Zustellung über dedizierten Server](#) beschrieben. Der Sendekonnektor für lokale Adressen nutzt in der [Verbindungssicherheit](#) eine [Client-Identität](#).

DNS Routing Einschränkungen

Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter **DNS Routing Einschränkungen**. Die Konfiguration der Einschränkungen für die lokale Zustellung läuft ab, wie im Kapitel [DNS Routing Einschränkungen durch Konnektor-Namensräume](#) beschrieben.

Direkte Zustellung

Durch die "Direkte Zustellung" konfigurieren Sie, dass sich NoSpamProxy bei E-Mails an lokale Adressen wie ein SMTP-Proxy verhalten soll. Bei dieser Einstellung ist darauf zu achten, dass der konfigurierte Smarthost immer verfügbar ist um die E-Mails anzunehmen. Wenn das nicht der Fall sein sollte, wird NoSpamProxy die E-Mail nicht annehmen. Der einliefernde Smarthost wird die Zustellung zu einem späteren Zeitpunkt erneut versuchen. Des Weiteren ist es in diesem Modus nur möglich, einen lokalen E-Mail-Server anzugeben.

Die Konfiguration der direkten lokalen Zustellung läuft ab, wie im Kapitel [Smarthost: E-Mail-Zustellung über dedizierten Server](#) beschrieben.



Wenn Sie [Office 365](#) zu den lokalen Servern hinzugefügt haben, dann ist die direkte Zustellung nicht verfügbar.

Externe Zustellung

Unter dem Punkt **Externe Zustellung** legen Sie fest, wie E-Mails an einen externen Server versendet werden.

SMTP

Für die Zustellung zu normalen externen SMTP-Servern werden die SMTP-Konnektoren eingesetzt. Über diese kann entweder eine direkte Zustellung zu dem Ziel SMTP-Server konfiguriert werden oder eine Zustellung über einen dedizierten Server (Smarthost), der alle E-Mails des Konnektors annimmt, um sie zur Zustellung weiter zu leiten.

Allgemeine Einstellungen

Geben Sie einen [Namen](#) ein und wählen Sie eine oder mehrere [Gateway Rollen](#) aus. Legen Sie anschließend die [Kosten](#) des Konnektors fest. Wählen Sie danach als **Routing Methode** entweder die [Direkte Zustellung \(DNS\)](#) oder die [Auslieferung über einen dedizierten Server \(Smarthosts\)](#) ([Bild 78](#)).

Ausgehender Sendekonnektor

Ausgehender Sendekonnektor

Allgemeine SMTP-Einstellungen

Name

Zugeordnete Gateway Rollen ☒ GWRole01

Kosten

Wenn mehrere Konnektoren für das Routing einer E-Mail nutzbar sind, wird der mit den geringsten Kosten gewählt.

Die Kosten betragen **100**

Routing-Methode

Ausgehende E-Mails können entweder direkt zu ihren Ziel Servern zugestellt werden oder Sie können über einen dedizierten Server geleitet werden.

Methode

☒ Direkte Zustellung (DNS)

☐ Auslieferung über einen dedizierten Server (Smarthost)

Zurück Weiter Abbrechen und schließen

Bild 78: Namen, Kosten und Zustellmethode eines SMTP Sendekonnektors

Zustellung - Direkte Zustellung (DNS)

Bei der direkten Zustellung über DNS Server wird versucht, die E-Mails direkt zu Ihren Ziel-Servern zuzustellen. Legen Sie für diesen Konnektor die notwendige [Verbindungssicherheit](#) fest. Zusätzlich können Sie hier eine bestimmte [Client-Identität](#) hinterlegen, damit sich der NoSpamProxy zu anderen Servern authentifizieren kann ([Bild 79](#)).

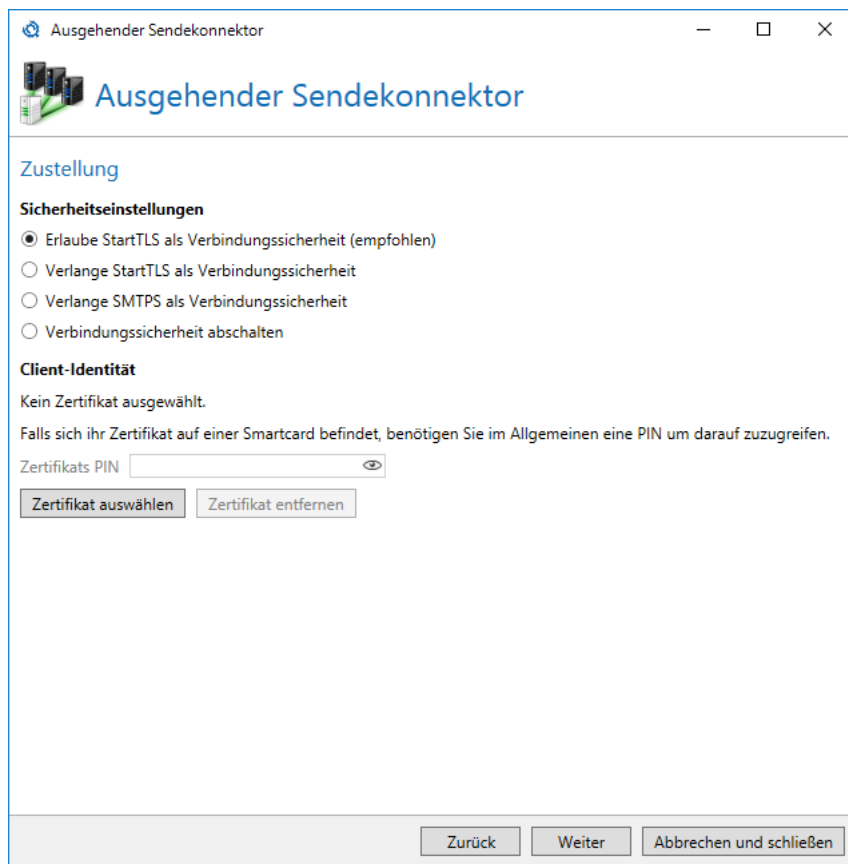


Bild 79: Verbindungssicherheit des SMTP-Sendekonnektors

Zustellung - Dedizierte Server (Smarthosts)

Die Konfiguration eines Smarthosts für die lokale Zustellung läuft ab, wie im Kapitel [Smarthost: E-Mail-Zustellung über dedizierten Server](#) beschrieben. Die Verbindungssicherheit für die Verbindung zu jeweiligen Smarthost besitzt die gleichen Optionen und Einschränkungen, wie im Kapitel [Zustellung - Direkte Zustellung \(DNS\)](#) beschrieben.

DNS Routing Einschränkungen

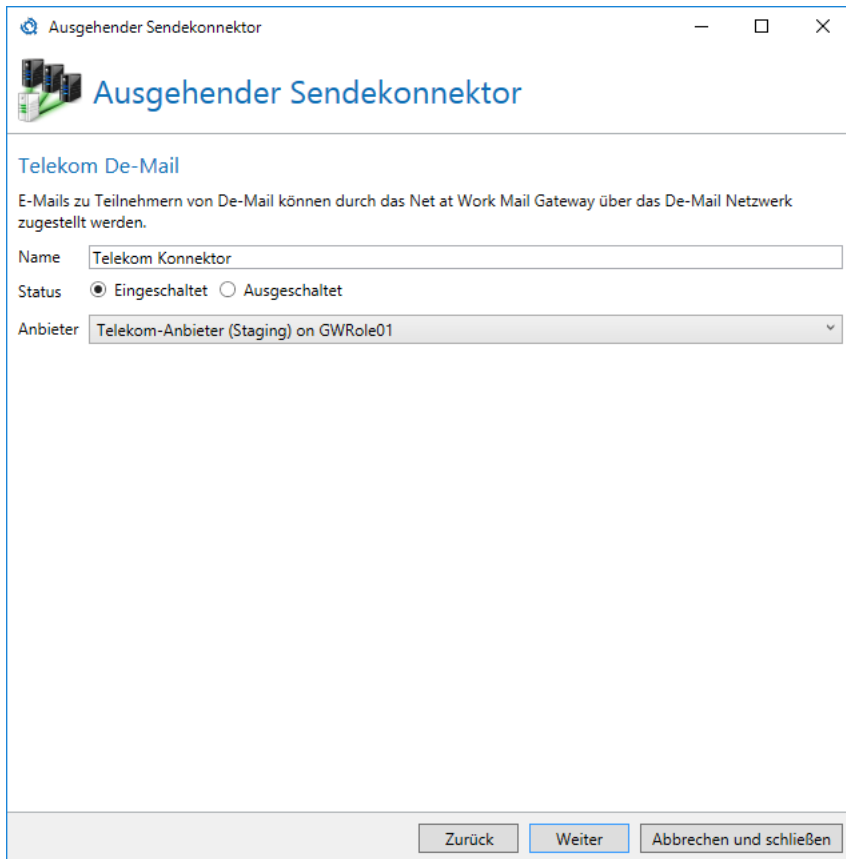
Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter **DNS Routing Einschränkungen**. Die Konfiguration der Einschränkungen für die lokale Zustellung läuft ab, wie im Kapitel [DNS Routing Einschränkungen durch Konnektor-Namensräume](#) beschrieben.

De-Mail über Telekom



Für die Anbindung an Telekom De-Mail müssen Sie zuerst einen [De-Mail-Anbieter](#) für eine **Telekom De-Mail-Verbindung** auf dem Knoten [Verbundene Systeme](#) einrichten.

Nutzen Sie diesen Konnektor wenn Sie De-Mails über die Telekom versenden möchten. Geben Sie als erstes den [Namen](#) und den Status des Konnektors an. Wählen Sie dann den bereits konfigurierten Anbieter aus der Liste aus. Die Anbieter werden in der Liste mit ihrem Namen, dem Zielsystem (T-Deutschland / T-Systems) und der Gateway Rolle auf der Sie liegen beschrieben ([Bild 80](#)). Als nächsten Schritt konfigurieren Sie, wie bei allen De-Mail-Sendekonnektoren, die [Zuordnung der eigenen Domänen](#).



The screenshot shows a window titled 'Ausgehender Sendekonnektor' with a standard Windows title bar. Below the title bar is a header area with a small icon of server racks and the text 'Ausgehender Sendekonnektor'. The main content area is titled 'Telekom De-Mail' and contains the following text: 'E-Mails zu Teilnehmern von De-Mail können durch das Net at Work Mail Gateway über das De-Mail Netzwerk zugestellt werden.' Below this text are three configuration fields: 'Name' with the value 'Telekom Konnektor', 'Status' with radio buttons for 'Eingeschaltet' (selected) and 'Ausgeschaltet', and 'Anbieter' with a dropdown menu showing 'Telekom-Anbieter (Staging) on GWRole01'. At the bottom of the window are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 80: Einstellungen eines Telekom De-Mail-Konnektors

De-Mail über Mentana-Claimsoft GmbH



Für die Anbindung an Mentana-Claimsoft De-Mail müssen Sie zuerst einen [De-Mail-Anbieter](#) für eine **Verbindung zu Mentana-Claimsoft** auf dem Knoten [Verbundene Systeme](#) einrichten.

Wählen Sie einen eindeutigen [Namen](#) für diesen Konnektor und bestimmen Sie, zu welchen [Gateway Rollen](#) er zugeordnet sein soll ([Bild 81](#)). Wählen Sie im nächsten Schritt die eigenen Domänen die mit diesem De-Mail-Konnektor E-Mails versenden können.

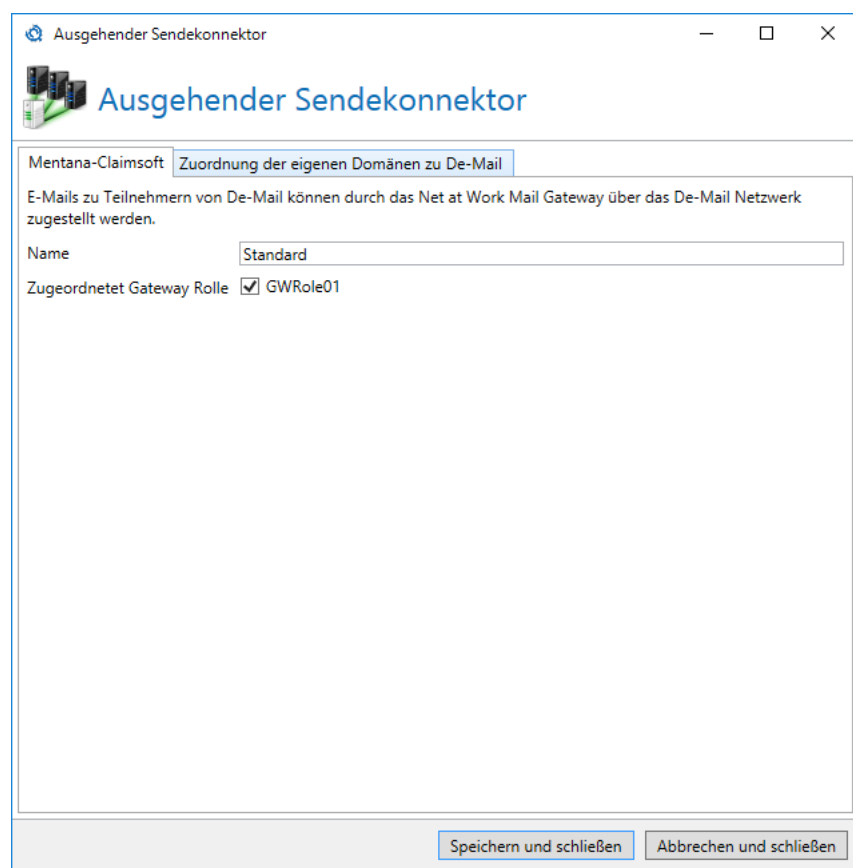


Bild 81: Mentana-Claimsoft De-Mail-Konnektor

Zuordnung der eigenen Domänen

Die Zuordnung der eigenen Domänen zu bestimmten De-Mail-Konnektoren dient dazu, jeweils eigene De-Mail-Konnektoren für die unterschiedlichen eigenen Domänen einrichten zu können. Falls Sie nur einen De-Mail-Sendekonnektor konfigurieren, fügen Sie diesem bitte alle eigenen Domänen hinzu. Bei mehreren De-Mail-Sendekonnektoren müssen Sie die passenden eigenen Domänen dem jeweiligen Konnektor hinzufügen, damit NoSpamProxy Encryption entscheiden kann über welchen De-Mail-Konnektor eine E-Mail versandt wird.

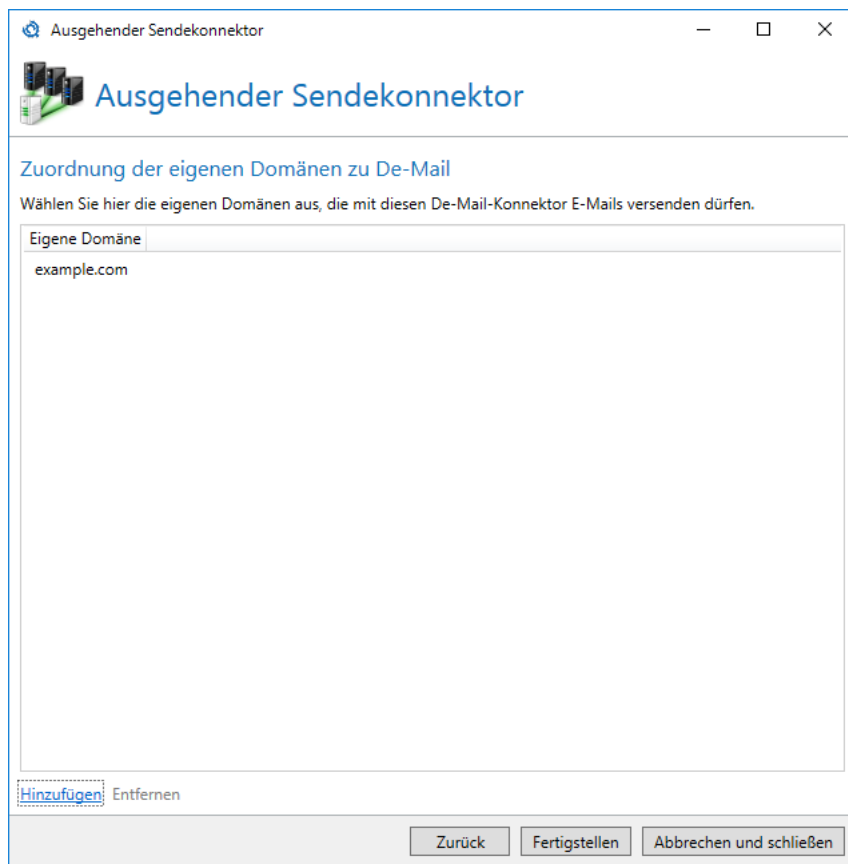


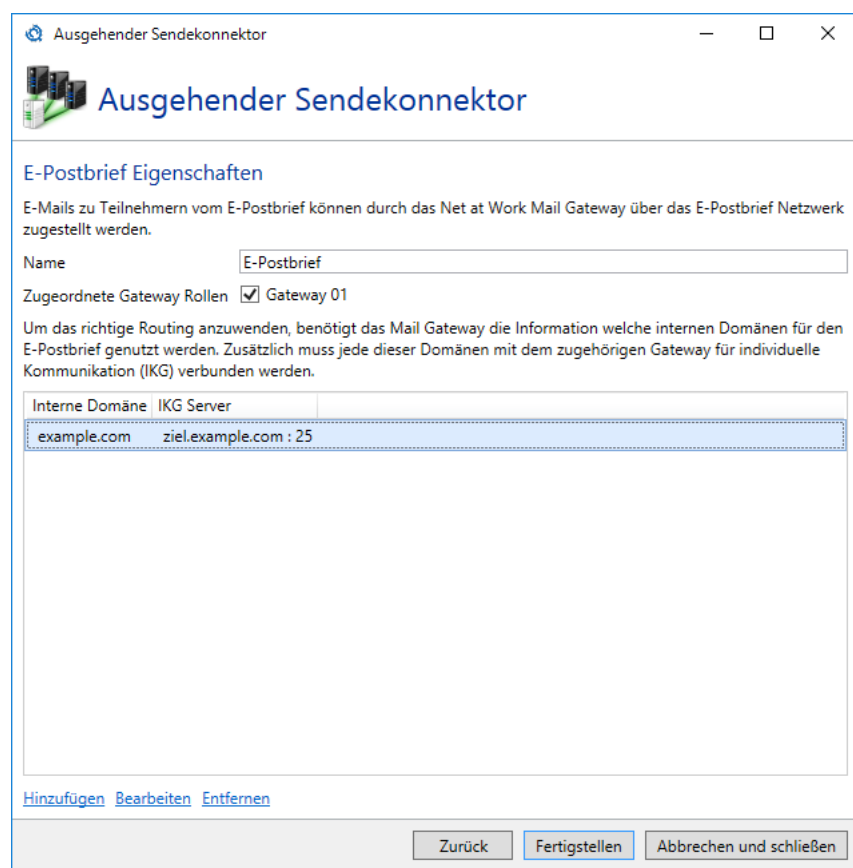
Bild 82: Zuordnung der eigenen Domänen zu den De-Mail-Sendekonnektor

E-Postbrief Konnektor

Die Deutsche Post ermöglicht mit dem E-Postbrief eine verbindliche, vertrauliche und verlässliche Kommunikation. Einzelheiten zu diesem Angebot finden Sie unter der Adresse <http://www.epostbrief.de>. Firmen haben die Möglichkeit der direkten Anbindung an die Infrastruktur der Deutschen Post über ein sogenanntes Individualkommunikationsgateway (IKG). Das IKG wird in Ihrem Unternehmen installiert und fungiert als SMTP Endpunkt für das E-Mail-Routing ins Netz der Deutschen Post.

Der E-Postbrief-Konnektor übernimmt das automatische Routing von E-Mails an ein IKG. Außerdem wird sichergestellt, dass E-Postbriefe nur von dem IKG aus angenommen werden. Dadurch wird gewährleistet, dass reguläre E-Mails, die aus dem Internet empfangen wurden, niemals als E-Postbriefe ausgegeben werden können.

Nach der Auswahl des E-Postbrief Konnektors können Sie auf der folgenden Seite für verschiedene interne Domänen festlegen, an welches IKG E-Postbriefe von dieser Domain geschickt werden. ([Bild 83](#)).



Ausgehender Sendekonnektor

E-Postbrief Eigenschaften

E-Mails zu Teilnehmern vom E-Postbrief können durch das Net at Work Mail Gateway über das E-Postbrief Netzwerk zugestellt werden.

Name:

Zugeordnete Gateway Rollen: ☒ Gateway 01

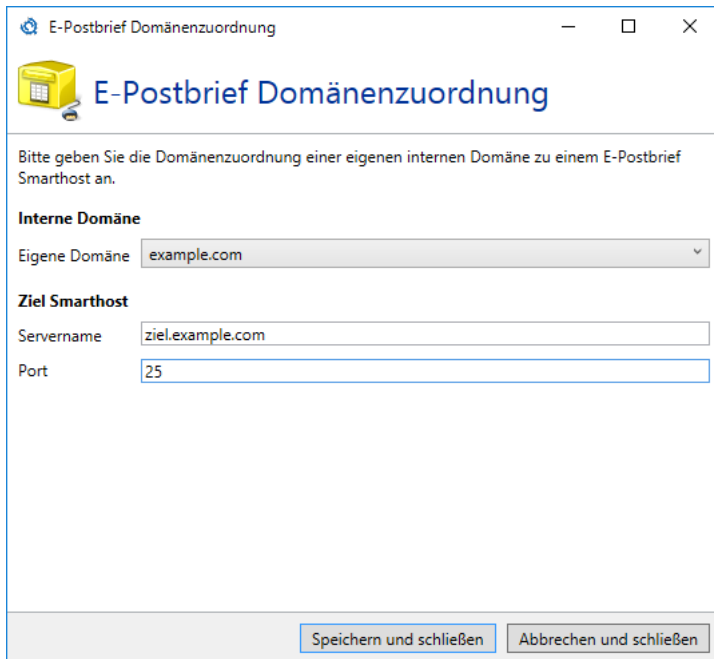
Um das richtige Routing anzuwenden, benötigt das Mail Gateway die Information welche internen Domänen für den E-Postbrief genutzt werden. Zusätzlich muss jede dieser Domänen mit dem zugehörigen Gateway für individuelle Kommunikation (IKG) verbunden werden.

Interne Domäne	IKG Server
example.com	ziel.example.com : 25

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Bild 83: Die Konfiguration für die Zustellung von E-Postbriefen

Die Zuordnung der eigenen Domänen zu den IKGs erfolgt über einen eigenen Dialog ([Bild 84](#)).



E-Postbrief Domänenzuordnung

Bitte geben Sie die Domänenzuordnung einer eigenen internen Domäne zu einem E-Postbrief Smarthost an.

Interne Domäne

Eigene Domäne: example.com

Ziel Smarthost

Servername: ziel.example.com

Port: 25

Speichern und schließen Abbrechen und schließen

Bild 84: Die Zuordnung einer eigenen Domäne zu einem IKG

Deutschland-Online - Infrastruktur Konnektor

Das Deutschland-Online - Infrastruktur (DOI) Projekt wird unter anderem von Kommunen zur sicheren Übertragung von Nachrichten verwendet. Wenn Sie kein Mitglied im DOI Projekt sind, dann haben Sie für diesen Konnektor keine Verwendung und können dieses Kapitel überspringen.

Der DOI-Konnektor lädt automatisch die aktuelle Tabelle aller Teilnehmer herunter und leitet E-Mails an andere Teilnehmer über das sichere DOI Netzwerk.

Um die Zustellung in das DOI Netzwerk zu aktivieren, erstellen Sie im Knoten E-Mail-Routing unter dem Punkt **Externe Zustellung** einen neuen Konnektor. Im folgenden Dialog wählen Sie als Typ **Deutschland-Online - Infrastruktur (DOI)** und klicken dann auf **Weiter**. Im nächsten Schritt müssen Sie die FTP- oder Web-Adresse eintragen, von der Sie die Mailer-Tabelle beziehen. Geben Sie dann unter **Authentifizierung** Ihren Benutzernamen und Ihr Kennwort an. Abschließend wählen Sie für die Kosten einen kleineren Wert als den, der bei dem Standard-Konnektor für E-Mails an externe Adressen eingetragen ist. So ist gewährleistet, dass nicht der Standard Routing-Konnektor das Routing für diese E-Mails übernimmt. Klicken Sie auf **Weiter**, wenn Sie alle Eingaben durchgeführt haben ([Bild 85](#)).

Ausgehender Sendekonnektor

DOI Konfiguration
E-Mails zu Teilnehmern der 'Deutschland-Online - Infrastruktur' können durch NoSpamProxy über das DOI Netzwerk zugestellt werden.

Allgemeine Einstellungen
Name:
Zugeordnete Gateway Rollen: ☒ GWR01
Wenn mehrere Konnektoren für die Zustellung einer E-Mail nutzbar sind, wird der mit den geringsten Kosten gewählt.
Die Kosten betragen **100**

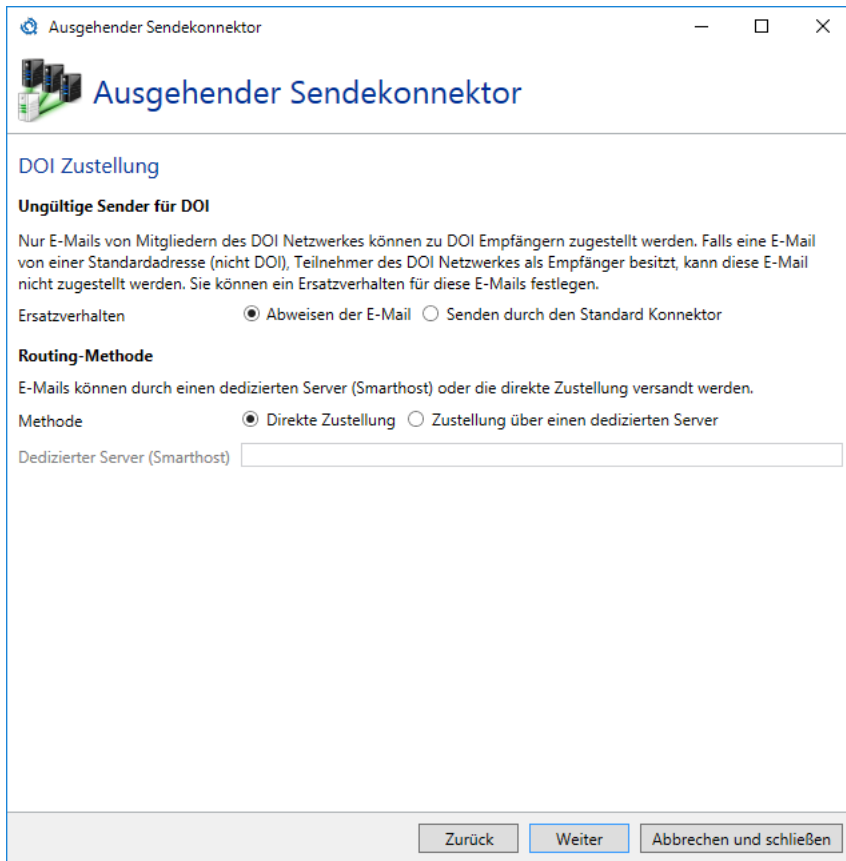
Mailer Tabelle
Es wird eine Liste aller E-Mail-Server des DOI-Netzwerkes und ihrer Domänen benötigt, um alle E-Mails des DOI Netzwerkes zu ihren passenden Zielen zuzustellen.
Adresse der DOI Mailer Tabelle:
[Nutze Standardadresse](#)

Authentifizierung
Sie können Benutzername und Kennwort angeben, falls Sie diese für den Zugriff auf die DOI Mailer Tabelle benötigen.
☒ Keine Authentifizierung verwenden
☐ Authentifizierung verwenden
Benutzername:
Passwort:

Back Next Cancel and close

Bild 85: Die Konfiguration für die Zustellung in das Netz von Deutschland-Online - Infrastruktur

Auf der Seite **DOI Zustellung** können Sie das Verhalten für ungültige Absender konfigurieren ([Bild 86](#)). Absender sind immer dann ungültig, wenn die Absenderdomäne nicht Teil des DOI-Netzwerkes ist. Diese E-Mails dürfen dann nicht über das DOI Netz zugestellt werden. Sie können nun wählen, ob diese E-Mails an den Absender zurückgehen oder ob sie über einen anderen Konnektor mit höheren Kosten gesendet werden. Des Weiteren können Sie auf dieser Seite festlegen, wie E-Mails zugestellt werden. Einerseits können die E-Mails direkt zugestellt werden, andererseits, und das ist die empfohlene Möglichkeit, kann ein Smarthost verwendet werden. Ein solcher Smarthost wird vom DOI Netz zur Verfügung gestellt.



Ausgehender Sendekonnektor

DOI Zustellung

Ungültige Sender für DOI

Nur E-Mails von Mitgliedern des DOI Netzwerkes können zu DOI Empfängern zugestellt werden. Falls eine E-Mail von einer Standardadresse (nicht DOI), Teilnehmer des DOI Netzwerkes als Empfänger besitzt, kann diese E-Mail nicht zugestellt werden. Sie können ein Ersatzverhalten für diese E-Mails festlegen.

Ersatzverhalten ☒ Abweisen der E-Mail ☐ Senden durch den Standard Konnektor

Routing-Methode

E-Mails können durch einen dedizierten Server (Smarthost) oder die direkte Zustellung versandt werden.

Methode ☒ Direkte Zustellung ☐ Zustellung über einen dedizierten Server

Dedizierter Server (Smarthost)

Zurück Weiter Abbrechen und schließen

Bild 86: Erweiterte Zustelloptionen für das DOI Netz



Bei einer Zustellung über das DOI Netzwerk wird die zugestellte E-Mail in der Nachrichtenverfolgung als "nicht verschlüsselt" beschrieben. Die E-Mail wird in diesem Fall über das DOI Netzwerk verschlüsselt und ist damit abhörsicher zugestellt. Diese Absicherung wird unter der Transportsicherheit nicht aufgeführt.

Empfangskonnektoren

Es können mehrere Empfangskonnektoren konfiguriert werden, um auf unterschiedlichen Netzwerkkarten E-Mails zu empfangen, aber auch um unterschiedliche Sicherheitsanforderungen für den E-Mail-Verkehr zu realisieren. Wenn Sie NoSpamProxy Encryption lizenziert haben, stehen Ihnen zusätzlich Konnektoren für De-Mail und POP3 Postfächer zur Verfügung.

E-Mail-Server des Unternehmens

Die unten angegebenen Server dürfen eine eigene Domäne in der Absenderadresse einer E-Mail verwenden.

Typ	Identität	Erlaubte Domänen	Kommentar
IP-Adresse	127.0.0.1	Alle	

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Eingehende Sendekonnektoren

Eingehende E-Mails werden direkt an den Server **localhost** auf Port **30** weitergeleitet.
Es wird **keine Authentifizierung** für die Verbindung zu diesem Smarthost genutzt.
Verbindungssicherheit ist **erlaubt**.
[Zustellung bearbeiten](#)
Anstatt die direkte Zustellung zu nutzen können Sie zur Zustellung über Warteschlangen wechseln. E-Mail können dann zu **On-Premise-Servern** oder zu **Office 365** zugestellt werden.
[Zur Zustellung über Warteschlangen wechseln](#)

Ausgehende Sendekonnektoren

E-Mails an externe Adressen werden durch die unten definierten Konnektoren geleitet. Falls mehrere Konnektoren für das Routing einer E-Mail geeignet sind, wird der mit den geringsten Kosten gewählt.

Typ	Name	Zuordnung	Zustellmethode	Kosten	DNS-Routingeinschränkungen
SMTP	Default connector for outbound mails	✓ GWRole01	Smarthost 127.0.0.1 : 30		Von * an *

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Empfangskonnektoren

Empfangskonnektoren verbinden die Gateway Rolle mit dem Internet um E-Mails zu empfangen.

Typ	Name	Zuordnung	Bindung	Zusätzliche Einstellungen	Verbindungssicherheit
SM...	SMTP on all addresses	✓ GWRole01	Alle : 25	Blockierung ist 30 Minuten Tarpittingniveau ist mittel	Erlaube StartTLS

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Bild 87: Die Übersicht über alle Konnektoren auf denen NoSpamProxy E-Mails empfängt und sendet.

SMTP-Konnektoren

Der SMTP-Empfangskonnektor definiert, auf welcher IP-Adresse und welchem Port E-Mails von NoSpamProxy empfangen werden. Er legt auch fest, wie mit ungültigen Anfragen von externen E-Mail-Servern verfahren wird und welche Verbindungssicherheit beim Transport der E-Mail angewendet werden soll.

SMTP-Einstellungen

Legen Sie die [Gateway Rollen](#) des Empfangskonnektors sowie die IP-Adresse und den Port des Konnektors ([Bild 88](#)) fest .

Im Eingabefeld **Bindung auf IP-Adresse** erfolgt die Angabe, unter welcher Adresse die Verbindungen angenommen werden sollen.

Mit der Angabe **Alle** wählen Sie alle vorhandenen IP-Adressen aus. Sie können stattdessen auch eine Auswahl aus der Menge der zugewiesenen IP-Adressen treffen. Klicken Sie hierzu auf das Pfeilsymbol und wählen Sie aus der Auswahlliste die gewünschte IP-Adresse aus.



Wenn Sie mehrere Gateway Rollen ausgewählt haben, dann können Sie keine Bindung auf einzelne IP-Adressen durchführen. Wählen Sie in diesem Fall **Alle** oder **Loopback** aus.

Bei **Port** können Sie den Port einstellen, auf dem NoSpamProxy E-Mails empfangen soll.

Empfangskonnektor

SMTP Einstellungen

Name: smtp example

Zugeordnete Gateway Rollen: ☒ Gateway 01

Adressbindung: ☒ Alle, ☐ Loopback, ☐ Bestimmte Adresse

Bestimmte Adresse: 192.168. [dropdown arrow]

ⓘ Eine bestimmte Adresse ist verfügbar wenn genau eine Gateway Rolle ausgewählt ist.

Binde an den Port: 25

Zurück Weiter Abbrechen und schließen

Bild 88: Die Verbindungssicherheit eines SMTP Empfangskonnektors

Ungültige Anfragen

Einige Teilnehmer im Internet versuchen andere E-Mail-Server durch das Senden von ungültigen Anfragen auszulasten (sogenannte 'Denial of Service'-Attacken) oder Sicherheitslücken auszunutzen, um in diesen Server einzubrechen. Um diese Angriffe zu minimieren, können Sie solche Anfragen

gezielt ausbremsen (z.B. durch sogenanntes "Tarpitting"). Die Karteikarte **Ungültige Anfragen** ([Bild 89](#)) zeigt die Konfigurationseinstellungen für diese ungültigen Anfragen.

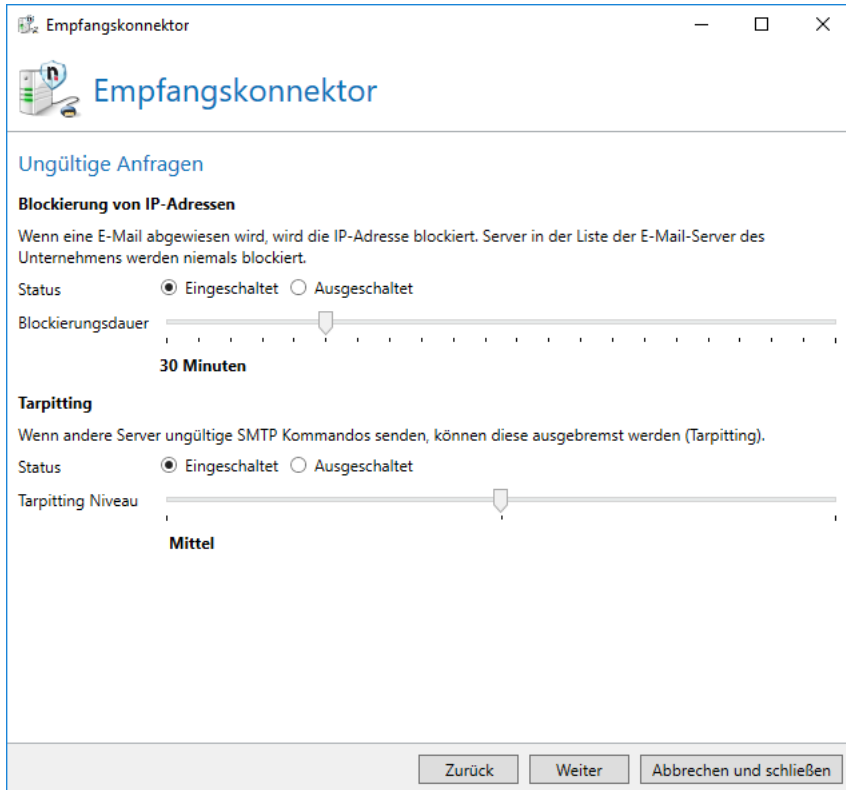


Bild 89: Bestimmen Sie die Verhaltensweise beim Empfang von ungültigen SMTP Kommandos

Die **Blockierung von IP-Adressen** dient dazu, bereits als Spam-Versender erkannte Server gezielt auszubremsen. Wenn ein Server eine E-Mail zu Ihrem NoSpamProxy sendet und diese als Spam eingestuft wird, werden nachfolgende E-Mails vom gleichen sendenden Server für den angegebenen Zeitraum blockiert. Ein normaler E-Mail-Versender wird nach diesem Zeitraum einen neuen Versuch unternehmen die E-Mail zuzustellen. Ein Spam-Versender wird wahrscheinlich die Zustellung abbrechen und sich auf ungeschützte E-Mail-Empfänger konzentrieren.

Stellen Sie über den Radiobutton **Blockierung für verdächtige IP-Adressen** die Option zur Blockierung ein oder aus. Mit dem Schieberegler für den **Blockierungszeitraum** können Sie die Dauer der Blockierung von 5 Minuten bis zu einem Tag (1440 Minuten) festlegen.

Das "Tarpitting" ist eine Methode, um E-Mail-Relays auszubremsen, die sich bei den SMTP-Befehlssätzen und/oder deren korrekte Reihenfolge nicht an die RFC halten. Sobald ein SMTP-Befehl falsch übermittelt oder an der falschen Stelle übermittelt wird, wartet NoSpamProxy bei jedem weiteren Befehl 5 Sekunden mit seiner Antwort. Die Übermittlung der Befehle wird also künstlich erschwert, als würden Sie einen Weg durch eine Teergrube nehmen, daher der Name Tarpitting.

Das **Verlangsamen von schlechten Verbindungen erlauben (Tarpitting)** können Sie mit den Radiobuttons **Eingeschaltet** und **Ausgeschaltet** ein- und ausschalten. Mit dem Schieberegler für

das **Tarpitting Niveau** können Sie einstellen, um wie viele Sekunden NoSpamProxy Protection die Antwortzeit verzögert. Stellen Sie den Schieberegler auf 'Niedrig', wartet das Gateway 2 Sekunden. In der Einstellung 'Mittel' wartet es 5 Sekunden und in der Position 'Hoch' wartet es 10 Sekunden.

Verbindungssicherheit

Der SMTP Empfangskonnektor nutzt in der [Verbindungssicherheit](#) eine [Server-Identität](#).

Wenn Sie StartTLS oder SMTPS als Verbindungssicherheit verlangen, können Sie zusätzlich auch die Identität des einliefernden Servers sicherstellen ([Bild 90](#)). Dabei sind folgende Einstellungen möglich:

- **Erlaube Verbindungen von jedem Server**
Die Identität des einliefernden Servers wird hier nicht beschränkt. Es werden E-Mails von allen Servern angenommen.
- **Verlange ein Zertifikat**
Das hier auszuwählende Zertifikat kann sowohl ein Endzertifikat, als auch ein Zwischen- oder Stammzertifikat sein. Wenn Sie ein Endzertifikat auswählen, muss der einliefernde Server seine Identität mit diesem belegen. Wenn Sie ein Zwischen- oder Stammzertifikat auswählen, muss er seine Identität mit einem Zertifikat belegen, dass das angegebene Zertifikat als Zwischen- oder Stammzertifikat in seiner Zertifikatskette besitzt.
- **Verlange ein vertrautes Zertifikat**
Der einliefernde Server muss seine Identität mit einem Zertifikat belegen, das im Zertifikatsspeicher des lokalen Computers als vertrauenswürdig hinterlegt ist.

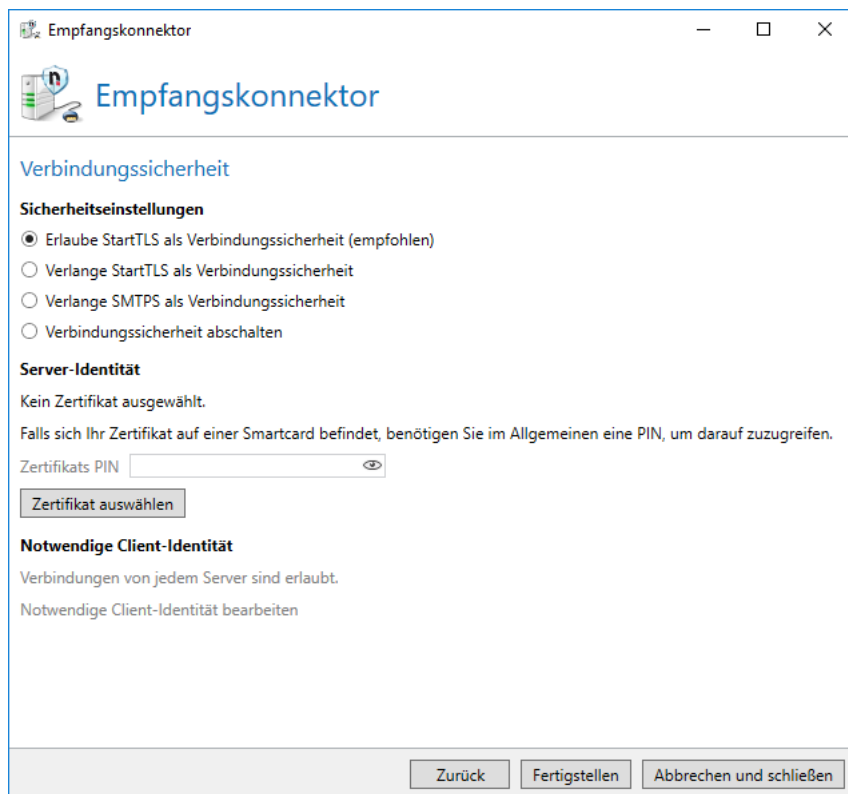


Bild 90: Die Verbindungssicherheit eines SMTP Empfangskonnektors

Regeln

Um eine E-Mail zu bearbeiten, wendet NoSpamProxy Regeln an, die Sie individuell konfigurieren können.

Nach der Neuinstallation von NoSpamProxy kann nach dem Einspielen der Lizenz ein Satz von Standardregeln erstellt werden. Diese ermöglichen es, das Gateway möglichst schnell und mit minimalem Administrationsaufwand die Funktion aufnehmen kann. Trotzdem sollten Sie diese Regeln überprüfen und ggf. an Ihre Bedürfnisse anpassen.

Die Regeln von NoSpamProxy sind modular aufgebaut. Sie können selbst Regeln erstellen und bereits bestehende Regeln ändern, indem Sie für jede einzelne Regel aus den zur Verfügung stehenden Filtern die gewünschten Filter auswählen. Innerhalb jeder Regel können Sie diese beliebig mit einem Multiplikator gewichten und ggf. konfigurieren.

Die Filter übernehmen bei der Prüfung der E-Mail die eigentliche Arbeit. Sie bewerten, wie stark die E-Mail ein bestimmtes Filterkriterium erfüllt und vergeben dafür Punkte. Wie diese Punkteverteilung genau vor sich geht, wird weiter unten erläutert. Sie können also Ihr eigenes Regelwerk mit ganz verschiedenen Filterkombinationen aufstellen und die Regeln auf bestimmte Sender und Empfänger einschränken. So können Sie sehr individuell und flexibel auf Spam-Attacken reagieren - nicht jede verdächtige E-Mail ist in jeder Situation für jedes Unternehmen Spam.

Wenn Sie z. B. einen Wortfilter einsetzen, ist der Ausdruck "Viagra" sehr wahrscheinlich auf Ihrer "schwarzen" Liste; Sie möchten E-Mails mit "Viagra"-Werbung blocken. Für ein Pharma-Unternehmen ist dieser Ausdruck jedoch nur sehr bedingt ein Spam-Kriterium. Mit NoSpamProxy Protection können Sie selbst aussuchen, ob Sie "Viagra" in den Wortfilter aufnehmen; oder ob Sie überhaupt einen Wortfilter einsetzen und wenn ja, wie stark Sie ihn mit dem Multiplikator gewichten.

Wenn eine E-Mail ansonsten seriös erscheint oder von einem bekannten E-Mail-Sender kommt, kann das Auftreten des verdächtigen Wortes unter Umständen akzeptabel sein. Sie können auch festlegen, dass die Regel mit dem Wortfilter nur für bestimmte IP-Adressen oder Empfänger gilt; zum Beispiel nur für Absender mit einer bestimmten TLD (Top Level Domain) oder IP-Adressen aus einem bestimmten Subnetz.

Die Reihenfolge der Regeln ist wichtig. Wenn eine Regel für eine zu überprüfende E-Mail zuständig ist, wird sie genutzt. Falls mehrere Regeln für eine E-Mail zutreffen, kommt diejenige Regel zur Anwendung, die in der Liste am weitesten oben steht.

Pos.	Regelname	Von	An	Aktion
1	"Allgemein"	*	max.mustermann@example.com	
2	"Japan"	*.jp	max.mustermann@example.com	

Regel 1, die wir hier "Allgemein" nennen, ist definiert auf alle E-Mails, die an max.mustermann@example.com adressiert sind. Regel 2 mit dem Namen "Japan" auf Position 2 ist ebenfalls auf Empfänger max.mustermann@example.com definiert, berücksichtigt aber nur Absender aus Japan.

Auf eine E-Mail aus Japan an "max.mustermann" treffen beide Regeln zu. Doch nur die Regel "Allgemein" wird zur Bewertung herangezogen, weil sie in der Liste oben steht. Auch wenn die Japan-Regel eigentlich "genauer" wäre - die Reihenfolge ist das entscheidende Kriterium.

Um die "Japan"-Regel anzuwenden, muss die Reihenfolge der Regel, wie unten angegeben, geändert werden. Dadurch wird die speziellere Regel zuerst angewandt.

Pos.	Regelname	Von	An	Aktion
1	"Japan"	*.jp	max.mustermann@example.com	
2	"Allgemein"	*	max.mustermann@example.com	

Filter

Für jede E-Mail werden die einzelnen Filter der zutreffenden Regel ausgeführt. Die Filter bewerten und vergeben Malus- und Bonus-Punkte für die zu überprüfende E-Mail. Diese Punkte werden mit dem Multiplikator der Filter gewichtet und dann zu einem Gesamtwert addiert. Überschreitet dieser Wert den eingestellten Schwellenwert (SCL) der Regel, wird die E-Mail abgewiesen. Den Schwellenwert können Sie individuell für jede Regel einstellen.

Welche Filter zur Verfügung stehen und wie sie genau funktionieren, erfahren Sie in Kapitel [Filter in NoSpamProxy](#).

Aktionen

Aktionen für die Spam-Prüfung

Nachdem anhand der Filter bestimmt wurde, ob die E-Mail abgewiesen wird oder sie passieren darf, werden die konfigurierten Aktionen aufgerufen. Aktionen können unter anderem die E-Mails verändern, um zum Beispiel eine Fußzeile zu ergänzen oder unerwünschte Anlagen zu entfernen. Aktionen können aber auch E-Mails, die nach der Bewertung durch die Filter eigentlich passieren würden, trotzdem abweisen. Damit kann beispielsweise ein Virens Scanner die E-Mail noch abweisen, obwohl sie nicht als Spam erkannt wurde.

Dies bedeutet, dass Aktionen übergeordnete Einstellungen sind, mit denen Filter gegebenenfalls überstimmt werden können.

Alle Aktionen werden im Kapitel [Aktionen in NoSpamProxy](#) detailliert beschrieben.

Wie NoSpamProxy Protection eine E-Mail als Spam klassifiziert

In den Regeln können Sie verschiedene Filter und Aktionen konfigurieren. Die Filter innerhalb einer Regel sind die Prüfstellen, welche nach bestimmten Kriterien den Spam-Charakter einer E-Mail bewerten. Je höher die Spamwahrscheinlichkeit ist, desto höher wird das Punktergebnis für diese E-Mail. Wird eine E-Mail hingegen als eher vertrauenswürdig bewertet, dann kann das Ergebnis auch negativ werden. Der Wertebereich liegt zwischen -10 und +10 Punkten. Die Filter können Sie innerhalb der Regeln mit dem Multiplikator verschieden gewichten. Die Bewertung des Filters wird mit dem Multiplikator verrechnet. Auf diese Art und Weise können Sie den Einfluss (=Punktbeitrag) eines wichtigen Filters innerhalb einer Regel erhöhen.

Anhand der ermittelten Gesamtpunktzahl wird ein "Spam Confidence Level" (SCL) ermittelt. Ein SCL von 0 besagt, dass die E-Mail neutral eingestuft wurde. Je größer der Wert ist, desto mehr wurde die E-Mail als Spam klassifiziert. Ist der Wert kleiner 0, dann wurde die E-Mail als vertrauenswürdig eingestuft. Erreicht diese Gesamtgewichtung den Schwellenwert der Regel, wird die E-Mail als Spam behandelt und abgewiesen.

Hier ein Beispiel:

Sie haben eine Regel erstellt mit einem aktiven Filter: dem Wortfilter. Außerdem ist das Level-of-Trust-System für diese Regel aktiviert. Der Wortfilter überprüft eine E-Mail auf unerwünschte Ausdrücke.

Nehmen wir an, eine E-Mail enthält eine Vielzahl von unerwünschten Ausdrücken. Der Wortfilter wird daher bei dieser E-Mail Alarm schlagen und einen hohen Malus-Wert liefern, zum Beispiel **6**. Wäre der Wortfilter der einzige Filter in dieser Regel, würde die E-Mail nun einen Gesamtwert von **6** haben. Wenn Sie in der Regel beispielsweise den Schwellenwert mit der Zahl **4** eingestellt haben, würde die E-Mail jetzt geblockt und abgewiesen werden. Der Absender würde eine Unzustellbarkeitsnachricht erhalten.

Nun ist in dieser Regel noch das Level-of-Trust-System aktiviert. Die E-Mail kommt von einem sehr verlässlichen Mailpartner, mit dem Sie bereits viele E-Mails ausgetauscht haben. Das Level-of-Trust-System bewertet diese E-Mail mit **-4** SCL-Punkten. Das Level-of-Trust-System hat immer einen

Multiplikator, der der Summe der Multiplikatoren aller auf der Regel aktivierten Filter plus **1** entspricht. Dies ergibt einen Faktor von **2** in unserem Beispiel. Der SCL Wert ergibt sich also aus **6+2*-4**. Damit ergibt sich ein SCL von **-2**. Die E-Mail würde NoSpamProxy Protection passieren.

Schon bei diesem kleinen Beispiel deutet sich an, welche Möglichkeiten der modulare Aufbau der Regeln bietet und wie wichtig die Filtergewichtung mit Multiplikatoren sein kann. SCL-Berechnungen werden im Kapitel [Berechnung des Spam Confidence Levels](#) detailliert beschrieben.

Ein weiteres aufschlussreiches Beispiel ist der folgende Fall:

Eine E-Mail kommt von einem System, das auf einer Sperrliste (RBL) steht. Die meisten Filterprodukte würden eine solche Verbindung ohne nähere Analyse kategorisch ablehnen. Mit NoSpamProxy Protection jedoch können Sie diese Entscheidung relativieren. Wenn die E-Mail z. B. eine Antwort darstellt, dann kann der Level-of-Trust-Filter die Bewertung überstimmen. Ergebnis: Die E-Mail von diesem Absender wird nicht geblockt, sondern, wie erwünscht, zugestellt.

E-Mails von einem anderen unbekannten Absender, der diesen unsicheren Server missbraucht, können aber nicht passieren.

Konfiguration der Regeln

Die Regeln, wie E-Mails bearbeitet werden sollen, werden im Knoten **Regeln** gepflegt ([Bild 91](#)).

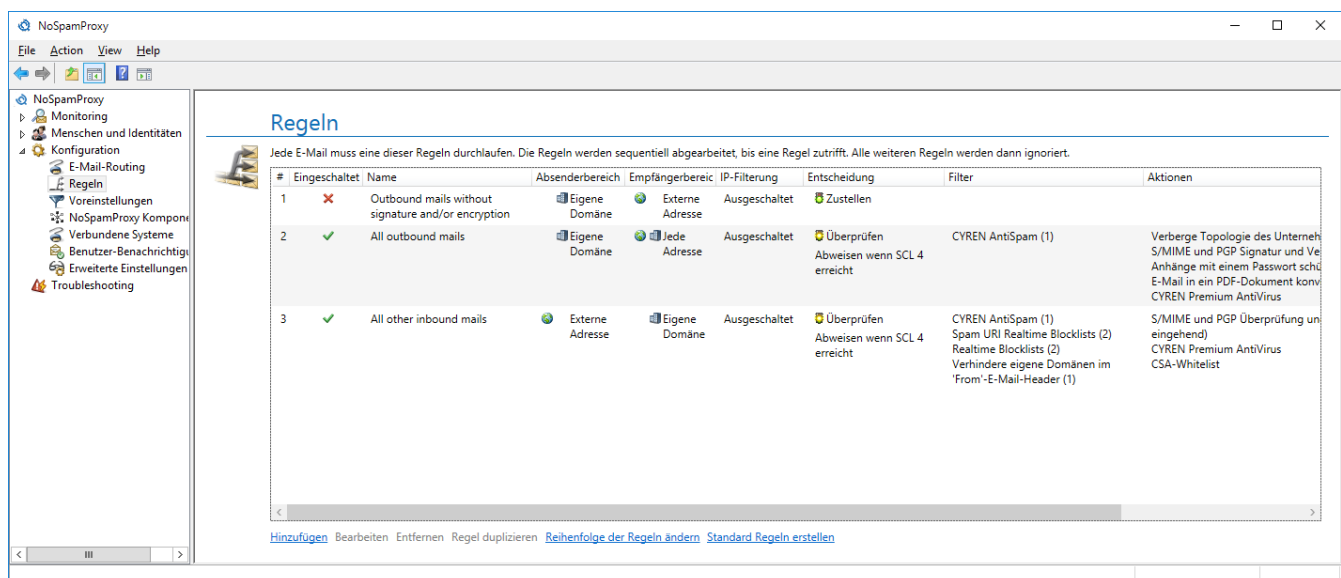


Bild 91: Die Übersicht über alle Regeln, die die Verarbeitung der E-Mails bestimmen

Bei einer Neuinstallation von NoSpamProxy ist die Auflistung der Regeln leer. In diesem Fall können Sie die Standard Regeln erzeugen lassen, in dem Sie den Link **Standard Regeln erstellen** nutzen ([Bild 92](#)). Die Funktion für die Erzeugung von Standard Regeln steht Ihnen auch später zur Verfügung, falls Sie Ihre eigenen Regeln mit den Standard Regeln ergänzen oder ersetzen möchten. Beim Ergänzen werden

die Standard Regeln hinter die bestehenden Regeln angefügt und können danach in der Reihenfolge verändert werden, siehe [Reihenfolge der Regeln ändern](#).

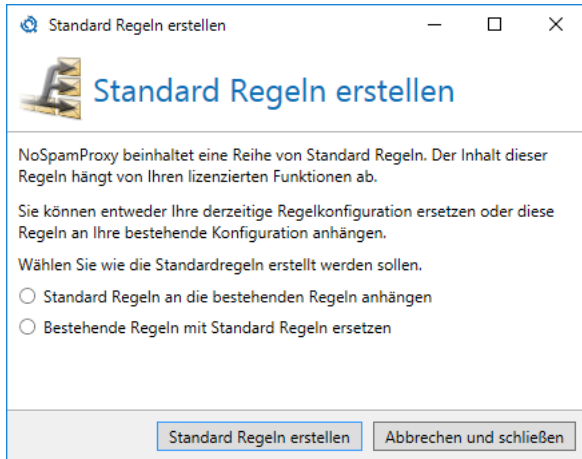


Bild 92: Erstellen der Standard Regeln

Neue Regel erstellen

Eine Regel besitzt folgende Einstellungen: **Allgemein**, **Richtung**, **Absender**, **Empfänger**, **Filter**, **Aktionen** und **Richtlinienvorstoß**. Welche Regel für eine E-Mail zur Anwendung kommt, wird durch die Einstellungen der Reiter **Richtung**, **Absender** und **Empfänger** festgelegt. Die anderen Reiter legen fest, wie die E-Mails verarbeitet werden.

Der erste Reiter ([Bild 93](#)) umfasst wichtige Parameter mit denen Sie grundlegende Eigenschaften festlegen.

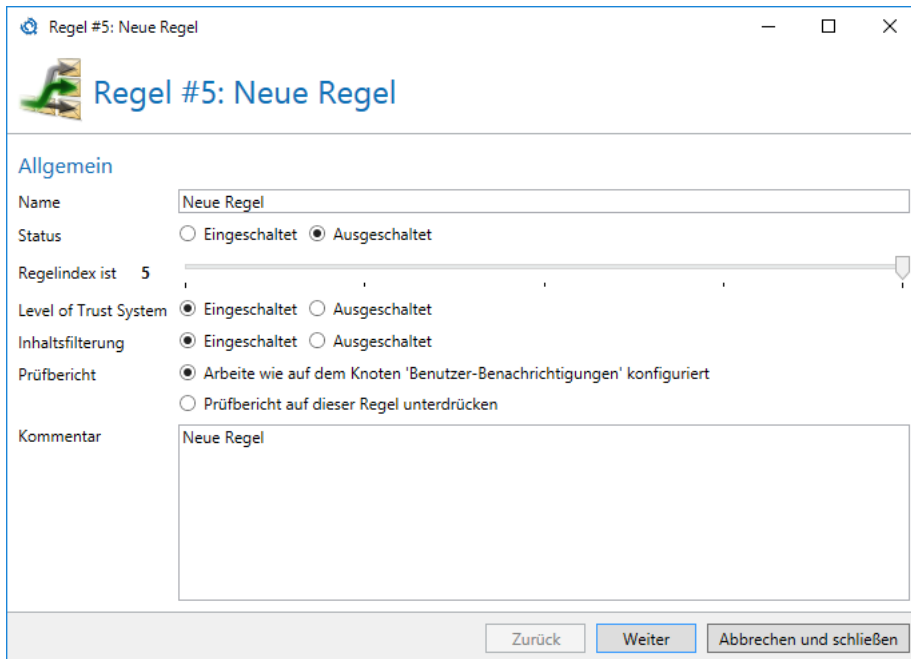


Bild 93: Allgemeine Einstellungen der Regel

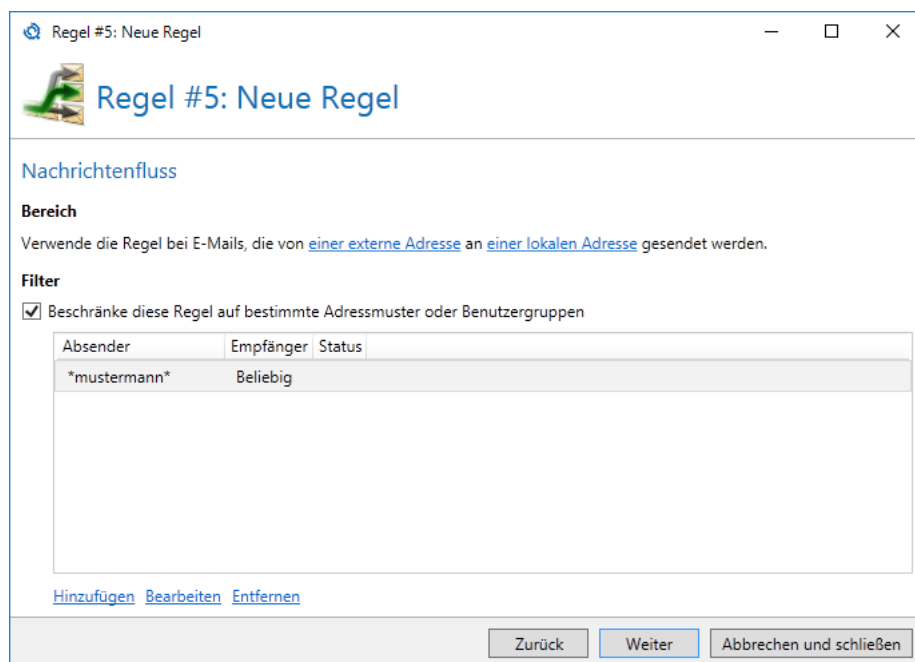
Zunächst geben Sie einen eindeutigen Namen für die Regel an, damit Sie in der Regelzusammenfassung nicht den Überblick verlieren. Unter **Aktiv** können Sie angeben, ob die Regel aktiviert oder deaktiviert ist. Mit dem **Index** der Regel geben Sie die Rangfolge der entsprechenden Regel ein.

Mit der Option **Level-of-Trust-System** können Sie das [Level-of-Trust-System](#) auf der Regel ein- oder abschalten.

Mit der Option **Inhaltsfilterung** können Sie die Überprüfung von Anhängen durch die [Inhaltsfilter](#) ein- oder abschalten.

Unter **Anmerkungen** können Sie eine Anmerkung zu der Regel festhalten, um die Identifizierung der Regel zu erleichtern. Die Anmerkungen haben keine Auswirkung auf Definition oder Funktion einer Regel. Sie dienen nur der Dokumentation.

Im Reiter **Nachrichtenfluss** schränken Sie die Regel auf bestimmte Absender und Empfänger ein ([Bild 94](#)).



Regel #5: Neue Regel

Regel #5: Neue Regel

Nachrichtenfluss

Bereich
Verwende die Regel bei E-Mails, die von [einer externen Adresse](#) an [einer lokalen Adresse](#) gesendet werden.

Filter
☒ Beschränke diese Regel auf bestimmte Adressmuster oder Benutzergruppen

Absender	Empfänger	Status
mustermann	Beliebig	

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Zurück Weiter Abbrechen und schließen

Bild 94: Geben Sie an, für welche Adressen diese Regel gelten soll.

Unter **Bereich** wählen Sie zunächst aus, für welche Absender und Empfänger diese Regel gelten soll. Des Weiteren können Sie die Regeln noch weiter einschränken, indem Sie einen oder mehrere **Filtereinträge** hinzufügen. Hier können Sie wahlweise Adressmuster oder Benutzergruppen verwenden ([Bild 95](#)).



Um Gruppen aus einem Benutzerverzeichnis zu erhalten, müssen Sie einen automatischen Benutzerimport von LDAP oder Active Directory Benutzern auf dem Knoten 'Domänen und Benutzer' konfigurieren. Gruppen sind verfügbar, nachdem die erste Synchronisation durchgeführt wurde.

Einschränkung

Absender

- ☒ Ein beliebiger Absender
- ☐ Der Absender entspricht dem unten angegebenen Eintrag. Platzhalter (* und ?) können benutzt werden.
- ☐ Der Sender ist Mitglied der unten angegebenen Benutzergruppe .

Absender

Gruppe

Empfänger

- ☒ Ein beliebiger Empfänger
- ☐ Der Empfänger entspricht dem unten angegebenen Eintrag. Platzhalter (* und ?) können benutzt werden.
- ☐ Der Empfänger ist Mitglied der unten angegebenen Benutzergruppe .

Empfänger

Gruppe

Bild 95: Konfigurieren eines Filtereintrags innerhalb einer Regel

Im Reiter **IP-Filterung** ([Bild 96](#)) können Sie die Regel auf bestimmte einliefernde Server einschränken.

Regel #5: Neue Regel

IP-Filterung

☐ Schränke diese Regel auf E-Mail ein, die von bestimmten Adressen gesendet werden

IP-Adresse oder Subnetz

Serveradresse

Entfernen

Bild 96: Definieren Sie die Gültigkeit der Regel in Bezug auf den einliefernden Server

Im Reiter **Filter** aktivieren Sie die gewünschten Filter für eine Regel ([Bild 97](#)). Die Filter wiederum können Sie unterschiedlich mit Multiplikatoren gewichten und so ihre Wirkung erhöhen oder verringern.

The screenshot shows a window titled 'Regel #4: Neue Regel' with a standard Windows title bar. Inside, the 'Filter' tab is selected. The text reads: 'Wenn eine E-Mail die Bedingungen von 'Nachrichtenfluss' und 'IP-Filterung' erfüllt, wird die unten angegebene Entscheidung angewandt.' Below this are three radio buttons: 'Annehmen der E-Mail' (selected), 'Abweisen der E-Mail', and 'Überprüfen der E-Mail mit den unten angegebenen Filtern'. A slider is positioned below the third option, with the label 'Abweisen falls der SCL-Wert 0 oder höher beträgt'. Below the slider is a section titled 'Aktive Filter' containing a table with columns 'Multiplikator', 'Name', and 'Status'. The table is currently empty. At the bottom of the table are three buttons: 'Hinzufügen', 'Bearbeiten', and 'Entfernen'. At the very bottom of the dialog are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Bild 97: Legen Sie die Filtereinstellungen der Regel fest

Stellen Sie die **Filtereinstellung** auf **Abweisen**, um alle E-Mails, die von dieser Regel verarbeitet werden, ungeprüft abzuweisen. Wählen Sie **Zustellen**, um alle E-Mails dieser Regel ungeprüft zuzustellen. Mit **Überprüfen** wird das Spam Confidence Level (SCL) jeder E-Mail überprüft und beim Erreichen des eingestellten Wertes als Spam abgewiesen. Ein SCL-Wert von "1" bedeutet, dass E-Mails bei geringen Spam Anzeichen bereits abgewiesen werden. Ein SCL-Wert von "10" weist nur E-Mails mit extrem hohen Spam Anzeichen ab.

Nur wenn Sie die Filtermethode **Überprüfen** ausgewählt haben, können Sie diejenigen Filter auswählen, die Sie einsetzen möchten. Hierzu dient der Bereich **Aktive Filter**. Um einen oder mehrere Filter für eine Regel zu aktivieren, klicken Sie auf den Link **Filter hinzufügen**. Es öffnet sich ein Dialog, in dem Sie aus den verfügbaren Filtern den gewünschten Filter auswählen können ([Bild 98](#)). Je nach Filter öffnet sich nochmal ein filterspezifischer Konfigurationsdialog, in dem Sie die Filterkonfiguration vornehmen. Links neben den Filternamen finden Sie jeweils einen Regler, mit dem Sie den Multiplikator einstellen können. Der Wert "5" bedeutet, dass der Filter fünfmal stärker gewichtet wird als ein Filter mit dem Wert "1".

Einige Filter sind nicht für den in der Regel gewählten Absender funktionsfähig. Dort wird in der Spalte **Status** der Text **Kann nicht auf Regeln für lokale (bzw. externe) Absender angewandt werden** angezeigt. Solche Filter können nicht hinzugefügt werden; eine Regel mit ungültigen Filtern wird zudem nicht abgespeichert.



Das Hinzufügen eines Filters zu einer Regel auf Grund der Richtung wird nur verhindert, falls er für diese Richtung keine Funktion zeigt. Diese Beschränkung stellt nicht immer den empfohlenen Einsatz dar. Das heißt, dass Filter, die für eine bestimmte Richtung gedacht sind, aber auch in der Gegenrichtung funktionieren, somit für beide Richtungen konfigurierbar sind. Die empfohlene Richtung steht dagegen teilweise im Namen des Filters.

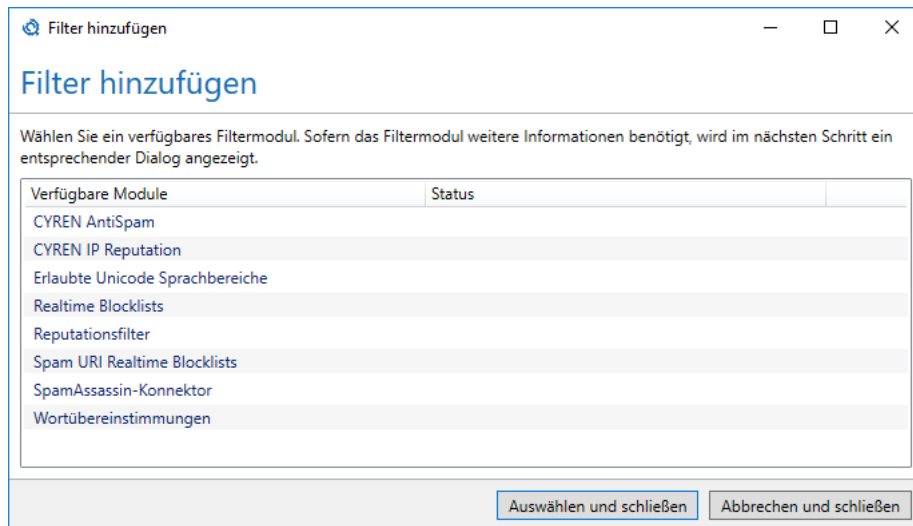


Bild 98: Fügen Sie einen verfügbaren Filter zu Ihrer Regel hinzu

Aktionen werden auf jeder geprüft oder ungeprüft zugestellten E-Mail ausgeführt. Sie können in diesem Reiter entscheiden, welche Aktionen in der Regel ausgeführt werden und wie diese Aktionen in der Regel konfiguriert werden. Aktionen werden immer ausgeführt, auch wenn die E-Mails nicht durch Filter überprüft werden.

Die in der Regel aktiven Aktionen werden in der Liste **Aktive Aktionen** aufgeführt ([Bild 99](#)).

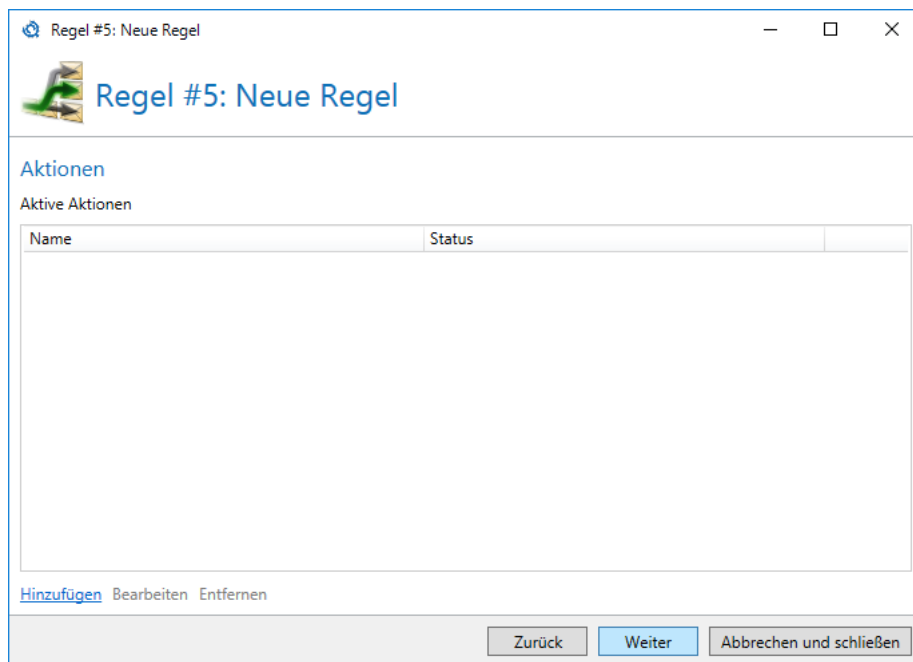


Bild 99: Die Aktionen einer E-Mail

Über den Link **Aktion hinzufügen** können Sie weitere Aktionen zur Regel hinzufügen. Je nach gewählter Aktion müssen Sie diese noch konfigurieren, bevor sie zur Liste der Aktionen hinzugefügt wird. ([Bild 100](#)). Einige Aktionen sind nicht für den in der Regel gewählten Absender funktionsfähig. Dort wird in der Spalte **Status** der Text **Lediglich lokale (bzw. externe) Absender werden unterstützt** angezeigt. Solche Aktionen können nicht hinzugefügt werden und eine Regel mit ungültigen Aktionen wird auch nicht abgespeichert.



Das Hinzufügen einer Aktion an eine Regel aufgrund des Absenders wird nur verhindert, falls sie für diese Richtung keine Funktion zeigt. Diese Beschränkung stellt nicht immer den empfohlenen Einsatz dar. Das heißt, dass Aktionen die für eine bestimmte Richtung gedacht sind, aber auch in der Gegenrichtung funktionieren, somit für beide Richtungen konfigurierbar sind. Die empfohlene Richtung steht dagegen teilweise im Namen der Aktion.

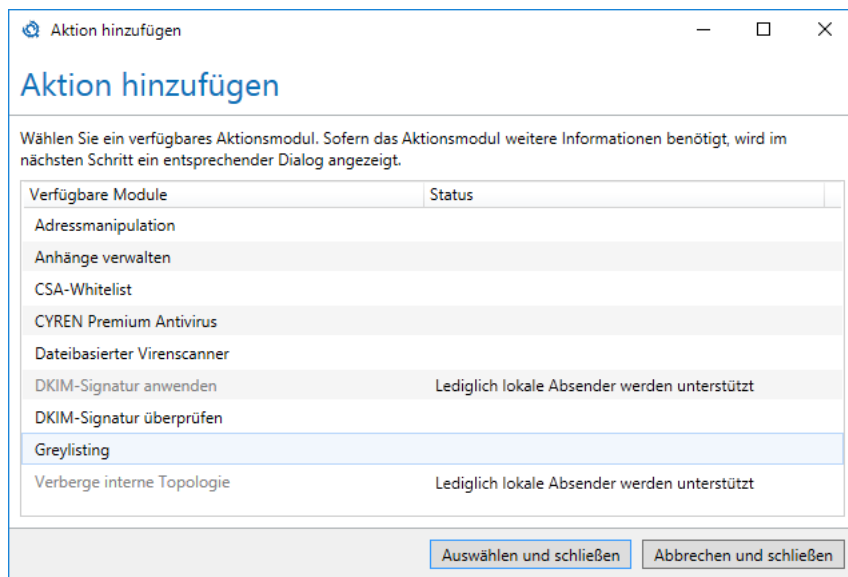


Bild 100: Aktionen aus dieser Liste können einer Regel hinzugefügt werden

Auf dem nächsten Reiter können Sie Einstellungen zum **Richtlinienverstoß** konfigurieren. Falls eine E-Mail die von Ihnen eingestellten Richtlinien für den Versand oder Empfang nicht erfüllt, wird das hier konfigurierte Verhalten verwendet. Richtlinienverstöße entstehen z.B. wenn eine E-Mail nicht verschlüsselt werden konnte oder weil ungültige Anhänge in E-Mails gefunden wurden.

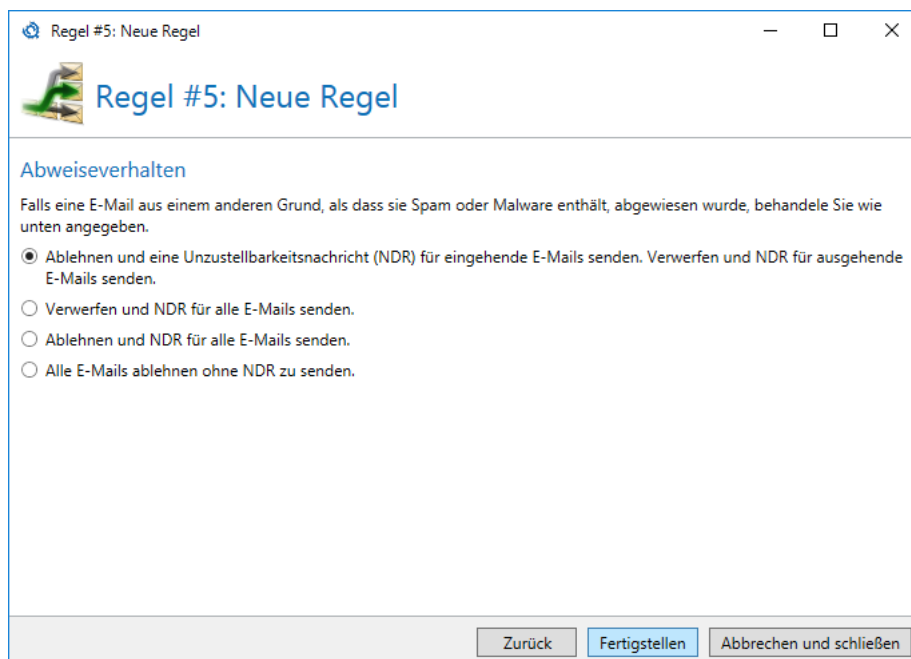


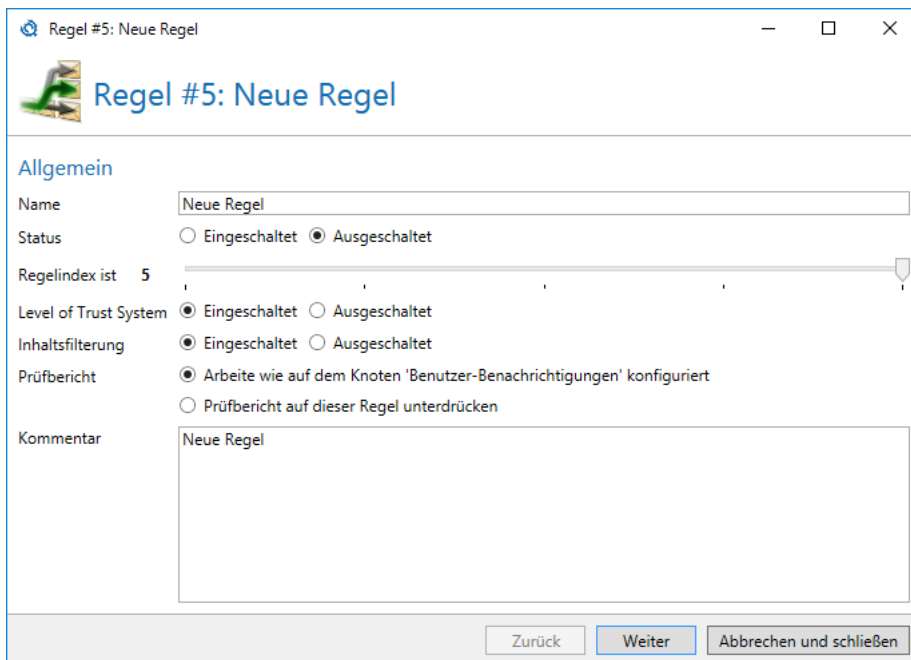
Bild 101: Verhalten bei Richtlinienverstoß

Ihnen stehen folgende Optionen zur Verfügung. **Ablehnen** einer E-Mail bedeutet, dass der empfangende Server die Annahme verweigert (SMTP-Meldung 5xx). Dadurch muss der einliefernde Server eine Unzustellbarkeitsnachricht (NDR) generieren. **Verwerfen** bedeutet eine positive Quittierung des empfangenden Servers an den einliefernden Server (SMTP-Meldung 200) aber ohne weitere Verarbeitung der empfangenen E-Mail. Da die E-Mail direkt nach der Annahme gelöscht wird, wird NoSpamProxy eine Unzustellbarkeitsnachricht generieren und an den einliefernden Server zurücksenden.

Reihenfolge der Regeln ändern

Nach Beendigung des Regel-Editors erscheint die neue Regel in der Regelliste. Die Position in der Liste entspricht dem Index, den Sie im Reiter **Allgemein** des Regel-Editors festgelegt haben.

Um diese Position einer Regel zu ändern, öffnen Sie die Konfiguration der Regel und stellen Sie die neue Position über die Einstellung **Regel-Index** ein.



Regel #5: Neue Regel

Allgemein

Name: Neue Regel

Status: ☐ Eingeschaltet ☒ Ausgeschaltet

Regelindex ist: 5

Level of Trust System: ☒ Eingeschaltet ☐ Ausgeschaltet

Inhaltsfilterung: ☒ Eingeschaltet ☐ Ausgeschaltet

Prüfbericht: ☒ Arbeite wie auf dem Knoten 'Benutzer-Benachrichtigungen' konfiguriert
☐ Prüfbericht auf dieser Regel unterdrücken

Kommentar: Neue Regel

Zurück Weiter Abbrechen und schließen

Bild 102: Über den Schieberegler für den "Regelindex" können Sie die Position der Regel verändern

Alternativ können Sie unter der Liste mit den Regeln auf **Regel Reihenfolge ändern** klicken ([Bild 103](#)).

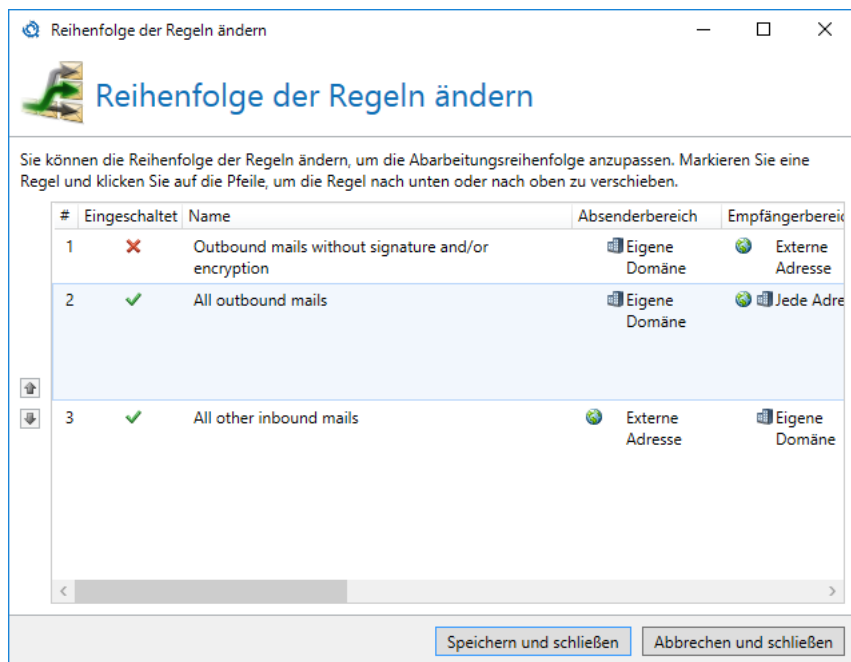


Bild 103: Hier kann die Reihenfolge aller Regeln zugleich verändert werden

Filter in NoSpamProxy

Filter bewerten E-Mails und beeinflussen dadurch den Spam Confidence Level (SCL) der E-Mails. Dadurch kann die Entscheidung getroffen werden, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis einen bestimmten SCL Wert übersteigt.

Cyren IP Reputation

Gültig für folgende Absender: **Extern**.

Standard SCL-Wert bei einfachem Multiplikator ist **3** für eine "schlechte" Reputation und **1** für einen "unbekannten Absender".

Dieser Filter überprüft über den Cyren-Dienst die Reputation der absendenden IP-Adresse, um die Trefferrate von NoSpamProxy weiter zu erhöhen. Das Greylisting wird übersprungen, wenn Cyren für die IP-Adresse die Reputation als "Gut" meldet. Bei einer "schlechten" Reputation oder einem unbekannten Absender werden die oben angegebenen SCL-Punkte vergeben. Der Filter selber verfügt über keine weiteren Einstellungsmöglichkeiten. Lediglich über die Gewichtung mit Multiplikatoren kann der Administrator weiteren Einfluss auf das Filterergebnis ausüben.

Cyren AntiSpam

Gültig für folgende Absender: **Extern** und **Lokal**.

Standard SCL-Wert bei einfachem Multiplikator ist **4**.

Der "Cyren AntiSpam"-Filter erstellt anhand festgelegter Kriterien einen Fingerabdruck der zu prüfenden E-Mail und vergleicht ihn mit den bekannten Fingerabdrücken des Cyren Detection Center im Internet. Ist dieser bekannt, stuft Cyren die E-Mail als Spam-E-Mail ein. Der "Cyren AntiSpam"-Filter wird daraufhin 4 SCL Punkte vergeben. Der Filter selber verfügt über keine weiteren Einstellungsmöglichkeiten. Lediglich über die Gewichtung mit Multiplikatoren kann der Administrator weiteren Einfluss auf das Filterergebnis ausüben.



Der Cyren-Dienst unterstützt Malwarescans bis zu einer Dateigröße von 50MB. Archive, zum Beispiel ZIP-Dateien, werden wenn möglich ausgepackt und die Dateien einzeln gescannt. Die Grenze von 50MB gilt in Archiven für die Größe der entpackten Dateien.

Erlaubte Unicode Sprachbereiche

Gültig für folgende Absender: **Extern** und **Lokal**.

Standard SCL-Wert bei einfachem Multiplikator ist **4**.

Spam-E-Mails kommen teilweise aus Sprachräumen, mit denen man üblicherweise keine Kommunikation unterhält. So kann zum Beispiel Spam eintreffen, der chinesische Schriftzeichen enthält. Dieser Filter kann E-Mails abblocken, in dem er alle enthaltenen Zeichensätze analysiert und die E-Mail nur passieren lässt, wenn alle enthalten Zeichensätze von Ihnen explizit erlaubt wurden.

Fügen Sie den Filter **Erlaubte Unicode Sprachbereiche** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 104](#)).

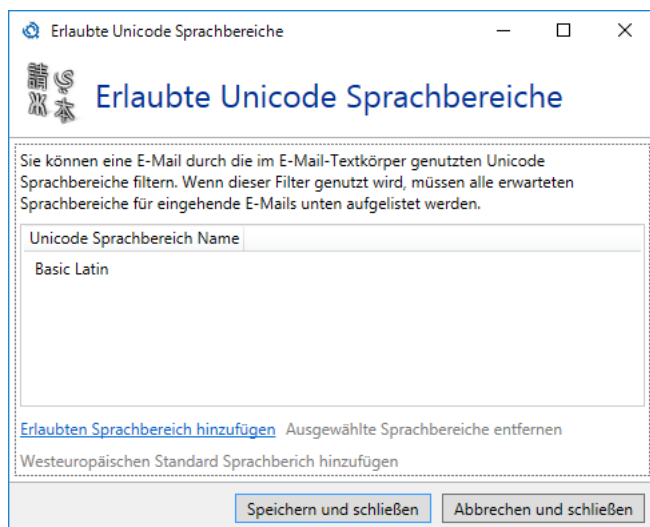


Bild 104: Die Liste der erlaubten Unicode Sprachbereiche

Fügen Sie nun alle Sprachbereiche, die in eintreffenden E-Mails verwendet werden können, zu den erlaubten Sprachbereichen hinzu. Wählen Sie dazu **Erlaubten Sprachbereich hinzufügen**. Es erscheint der Dialog mit allen noch nicht erlaubten Sprachbereichen ([Bild 105](#)).

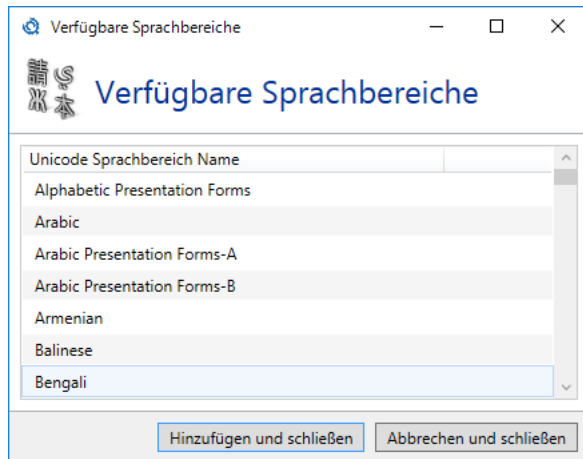


Bild 105: Die Liste der verfügbaren Unicode Sprachbereiche

Falls Sie nur mit Westeuropa oder Amerika kommunizieren, reicht üblicherweise der Sprachbereich für Westeuropäische Sprachen. Diesen können Sie über **Westeuropäischen Standard Sprachbereich hinzufügen** in die Liste einfügen, falls er sich noch nicht in der Liste der erlaubten Sprachen befindet.

Realtime Blocklists

Gültig für folgende Absender: **Extern**.

Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Listen. Pro Treffer werden die in der Liste eingestellten SCL-Punkte vergeben.

Der Filter "Realtime Blocklists" prüft, ob ein Adresseintrag in Realtime-Blocklists vorliegt. Sie können mehrere verschiedene Blocklists auswählen. Da auch die besten Listen False Positives aufweisen können, sollten Sie stets mehrere Listen heranziehen. Da jeder Treffer als Maluspunkt gewertet wird, wird das Risiko für eine Mail minimiert, anhand einer einzelnen Sperrliste gleich durch ein "False positive" blockiert zu werden.

Fügen Sie den Filter **Realtime Blocklists** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 106](#)).

Beim Filter **Realtime Blocklists** können Sie einstellen, welche Blocklists herangezogen werden sollen. Genau wie beim Filter **Wortübereinstimmungen**, werden die einzelnen Listen global im Menü **Allgemein Filtereinstellungen** vorkonfiguriert und müssen im Filter lediglich ausgewählt werden.

Über den Link **Mit Standardlisten ersetzen** können Sie die aktuell ausgewählten Listen durch die von Net at Work empfohlenen Listen ersetzen.

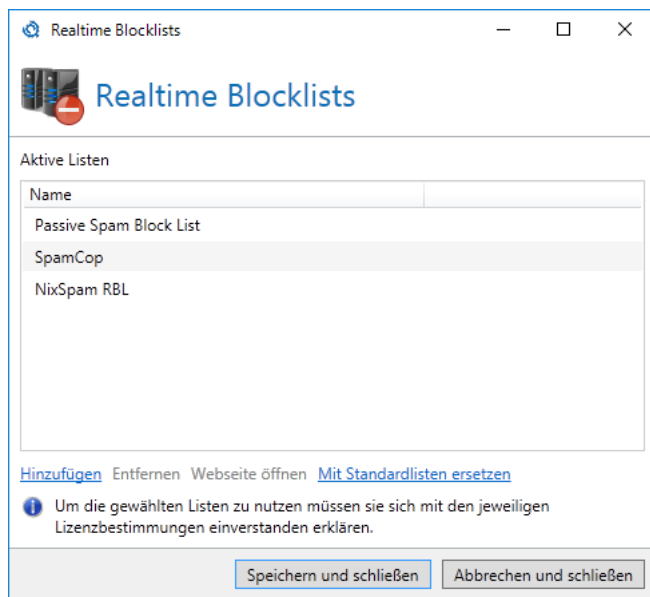


Bild 106: Fügen Sie alle Blocklists hinzu, die URIs in E-Mails überprüfen sollen

Klicken Sie auf **Hinzufügen**, um die Blocklists auszuwählen, die NoSpamProxy Protection bei der Filterung abfragen soll. Es öffnet sich der Dialog **Blocklist hinzufügen** (Bild 107). Wählen Sie hier die gewünschte(n) Blocklist(s) aus und klicken anschließend auf **Hinzufügen**. In der Übersicht der Realtime Blocklists tauchen die zuvor ausgewählten Listen auf.

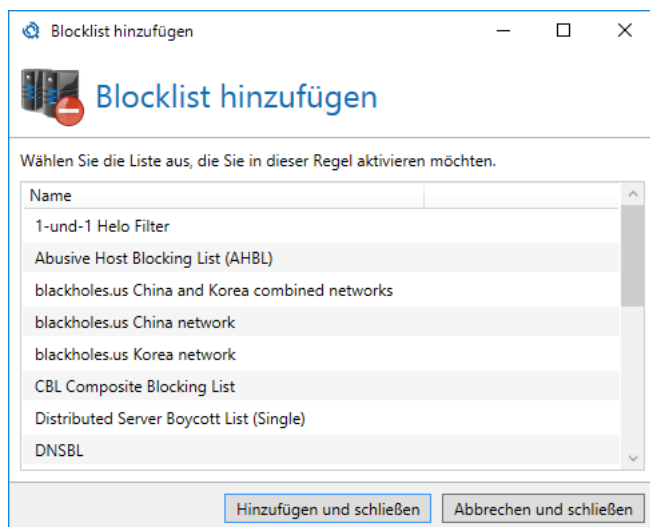


Bild 107: Sie können aus allen definierten Blocklists auswählen

Um eine oder mehrere Listen zu entfernen, markieren Sie die zu löschenden Einträge und klicken auf **Markierte Einträge entfernen**.

Beachten Sie, dass die entfernten Listen nur aus der gerade editierten Regel entfernt werden. In den globalen Regeleinstellungen tauchen die Listen nach wie vor auf.

Damit die DNS-Abfragen korrekt funktionieren, müssen Sie die DNS-Einstellungen des Betriebssystems geeignet konfigurieren. Der Server muss externe Domänen auflösen können. Es kann sinnvoll sein, einen eigenen DNS-Server als Forwarder zu installieren.

Spam URI Realtime Blocklists

Gültig für folgende Absender: **Extern** und **Lokal**.

Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Listen. Pro Treffer einer Liste werden **2** SCL-Punkte vergeben.

Spam URI Realtime Blocklists verwalten Listen mit verdächtigen Spam-URLs. Über das Internet ist es möglich zu überprüfen, ob gegebenenfalls eine URL in dieser Liste vorhanden ist oder nicht.

Der "Spam URI Realtime Blocklists Filter" isoliert aus den Links in einer Mail die Domäne und prüft, ob ein entsprechender Eintrag in diesen Listen vorliegt. Des Weiteren sucht er auch nach Adressen, die mit "www." anfangen und nicht als Link in der Mail auftauchen.

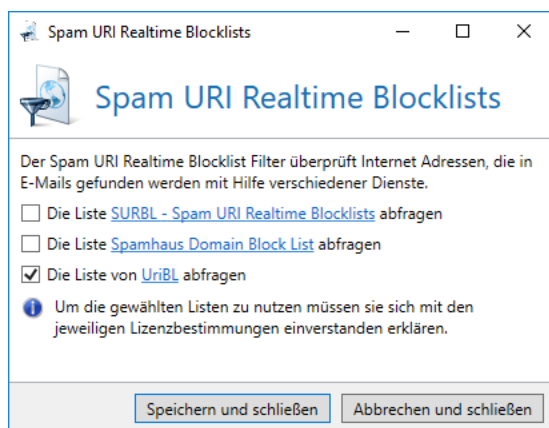


Bild 108: Konfigurieren Sie den Spam URI Realtime Blocklists Filter

Sie können mehrere verschiedene Blocklists auswählen ([Bild 108](#)).

Wie beim Realtime Blocklist Filter müssen DNS-Abfragen korrekt funktionieren. Der Server muss den angegebenen Dienst auflösen können. Es kann sinnvoll sein, einen eigenen DNS-Server als Forwarder zu installieren.

SpamAssassin Konnektor

Gültig für folgende Absender: **Extern** und **Lokal**.

Standard SCL-Wert bei einfachem Multiplikator ist abhängig vom **Rückgabewert** des SpamAssassin Daemon.

SpamAssassin ist ein kostenfreier Spamfilter, welcher verschiedene vordefinierte Tests beinhaltet, um Nachrichten zu klassifizieren. Viele dieser Tests, wie z. B. RBL, führt NoSpamProxy Protection selbst schon sehr viel früher und effektiver aus. Dennoch kann es interessant sein, die sonstigen Regeln dieses Filters zu integrieren.

SpamAssassin bewertet eine Nachricht und schreibt das Ergebnis in den Header der Nachricht. Er besteht aus Server (SpamD) und Client (SpamC). Der Filter von NoSpamProxy Protection agiert als SpamAssassin Client (SpamC) und funktioniert nur in Verbindung mit einem SpamAssassin Daemon (SpamD).

Sie können den SpamAssassin Daemon auf einem System Ihrer Wahl installieren. Dies kann ein UNIX oder Windows-System sein. Auch der Betrieb direkt auf dem gleichen Server wie NoSpamProxy ist möglich.

Fügen Sie den Filter **SpamAssassin Konnektor** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 109](#)).

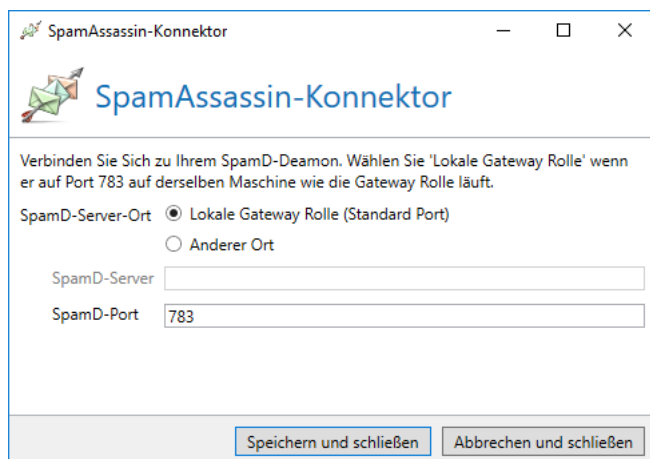


Bild 109: Definieren Sie die Verbindung zum SpamD Server

Beim SpamAssassin Konnektor können Sie die IP-Adresse bzw. den Full Qualified Domain Name (FQDN) des SpamD-Servers einstellen. Der Standard-Port des SpamD-Servers ist "783" und kann verändert werden, wenn Ihr SpamD auf einem anderen Port Verbindungen annimmt.

Mit der Einstellung **SpamD Servername** können Sie zunächst festlegen, ob sich der SpamD Server auf derselben Maschine befindet oder auf einer entfernten Maschine.

Unter **SpamD Server** können Sie die IP-Adresse bzw. den DNS-Namen des SpamD-Servers angeben. Unter **SpamD Port** können Sie die Port-Nummer des SpamD-Servers angeben. Standardmäßig nimmt der SpamD-Server auf der Port-Nummer "783" die Verbindungen an.



Achten Sie darauf, dass NoSpamProxy das angefragte System auch erreichen kann. Oftmals sind Portfilter, IP-Routing und Firewalls zu konfigurieren.

Reputationsfilter

Gültig für folgende Absender: **Extern**.

Dieser Filter führt verschiedene Tests auf dem E-Mail-Envelope und dem Inhalt der E-Mail durch ([Bild 110](#)). Durch einige der Tests wird auch DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), sowie darauf aufbauend DMARC (Domain-based Message Authentication, Reporting, and Conformance) analysiert ([Bild 111](#)). Jedem Test können individuelle SCL-Punkte gegeben werden, wodurch Sie die Bewertungen an die Anforderungen Ihres Unternehmens anpassen können.

Reputationsfilter

Reputationsfilter

Tests auf dem E-Mail-Envelope

E-Mail-Envelope-Tests werden auf der Absender-IP-Adresse und der 'MAIL FROM'-Adresse durchgeführt.

[Aktivieren](#) oder [deaktivieren](#) aller E-Mail-Envelope-Tests.

- ☒ Die IP-Adresse lässt sich nicht zu einem Hostnamen auflösen
2 SCL-Punkte
- ☒ Der Hostname, der mit der IP-Adresse verknüpft ist, beinhaltet die IP-Adresse in Textform
2 SCL-Punkte
- ☒ Der Hostname der mit der IP-Adresse verbunden ist, lässt sich nicht zu der IP-Adresse zurück auflösen
2 SCL-Punkte
- ☒ 'MAIL FROM'-Domäne lässt sich nicht zu einer IP-Adresse auflösen
2 SCL-Punkte

Zurück Weiter Abbrechen und schließen

Bild 110: Test auf dem E-Mail-Envelope

Reputationsfilter

Reputationsfilter

Tests auf dem E-Mail-Body

E-Mail-Body-Tests werden auf den Daten der Envelope und der eigentlichen E-Mail durchgeführt.

[Aktivieren](#) oder [deaktivieren](#) aller E-Mail-Body-Tests.

- ☒ SPF-Check schlägt in Abwesenheit von DMARC fehl
2 SCL-Punkte
- ☒ DKIM schlägt in Abwesenheit von DMARC fehl
2 SCL-Punkte
- ☒ DMARC Überprüfung schlägt fehl
2 SCL-Punkte für Quarantäne-Ergebnis
- ☒ Unstimmigkeit zwischen der 'MAIL FROM'- und 'Header-From'-Domäne in Abwesenheit von DMARC
4 SCL-Punkte für Abweisen-Ergebnis
- ☒ 'Header-From' ist eine lokale Adresse
4 SCL-Punkte

Zurück Fertigstellen Abbrechen und schließen

Bild 111: Test auf dem E-Mail-Body

Wortübereinstimmungen

Gültig für folgende Absender: **Extern** und **Lokal**.

Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Wortgruppen. Pro Treffer werden die in der Wortgruppe eingestellten SCL-Punkte vergeben.

Mit diesem Filter können Sie vorher definierte Wörter und Ausdrücke sowohl in der Betreffzeile als auch dem E-Mail-Body erkennen und sie mit positiven oder negativen SCL-Punkten bewerten. Jedes Auftauchen, oder je nach Einstellung auch Fehlen, eines solchen Ausdrucks in einer E-Mail wird mit den im Filter eingestellten Punkten bewertet.

Falls ein oder mehrere Worte aus den konfigurierten Wortgruppen in der E-Mail gefunden wird, kann optional noch eine E-Mail mit einer Benachrichtigung an eine lokale E-Mail-Adresse versandt werden. Diese E-Mail beinhaltet den Absender der E-Mail, den Empfänger, Betreff, sowie die gefundenen Worte.



Die in diesem Filter zur Verfügung stehenden Wortgruppen werden zuvor unter dem Knoten [Voreinstellungen](#) definiert.

Fügen Sie den Filter **Wortübereinstimmungen** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 112](#)).

Wortübereinstimmungen

Fügen Sie eine oder mehrere der bereits definierten Wortgruppen aus dem Bereich 'Wortübereinstimmungen' des Knoten 'Voreinstellungen' ein.

Aktive Wortgruppen

Wortgruppe
Common notation for medical products
Common notation of porn words

[Hinzufügen](#) [Entfernen](#)

Falls ein Übereinstimmung gefunden wird, kann eine E-Mail an eine lokale Adresse versandt werden.

☐ **Sende eine Benachrichtigung**

Adresse

[Speichern und schließen](#) [Abbrechen und schließen](#)

Bild 112: Fügen Sie Ihre definierten Wortgruppen in den Filter der Wortübereinstimmungen ein

Nun haben Sie die Möglichkeit über den Link **Wortgruppe hinzufügen** zuvor erstellte Wortgruppen aufzunehmen. Standardmäßig sind bereits einige Wortgruppen vorkonfiguriert. Wählen Sie die gewünschte(n) Wortgruppe(n) aus und klicken Sie auf **Hinzufügen**. In der Übersicht des Dialogs für die Wortübereinstimmungen sehen Sie nun die ausgewählten Wortgruppen.

Aktionen in NoSpamProxy

Aktionen können E-Mails verändern

Eine Aktion erhält Informationen über das Filter-Ergebnis und kann daraufhin weitergehende Aufgaben ausführen. Im Gegensatz zu den Filtern können Aktionen die E-Mails verändern; zum Beispiel Anhänge aussortieren. Zudem können Aktionen Filter-Ergebnisse überstimmen. Beispiele hierfür sind Virens Scanner und eine Greylisting Aktion.

Um eine Aktion zu aktivieren, müssen Sie in der Regel, die die Aktion enthalten soll, die Karteikarte **Aktionen** wählen. Dann klicken Sie auf **Hinzufügen**. Es erscheint der Dialog **Aktion hinzufügen**, in dem Sie die hinzuzufügende Aktion auswählen und dann auf **Auswählen und schließen** klicken. Nun

wird die Aktion hinzugefügt; falls sie konfiguriert werden muss, wird die Konfiguration der Aktion geöffnet und die Aktion danach zu Ihrer Regel hinzugefügt.

Adressmanipulation

Gültig für folgende Absender: **Extern** und **Lokal**.

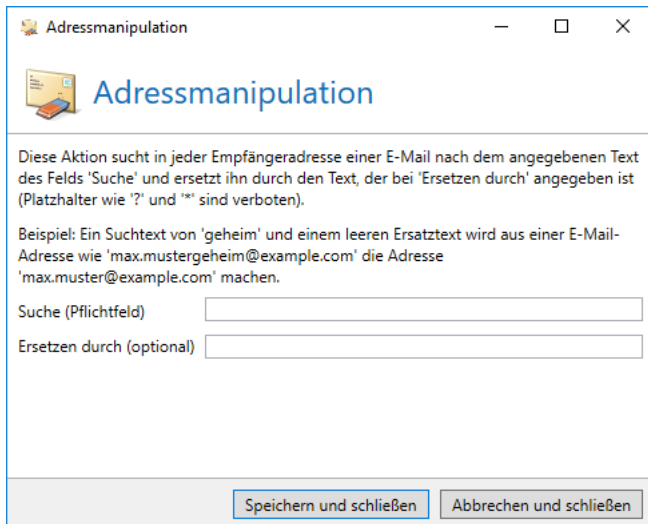
Diese Aktion eröffnet Ihnen die Möglichkeit, die Zieladresse beim Empfang einer E-Mail zu verändern. So können Sie z. B. nach einem Namenswechsel der Firma, alle E-Mails, die an die alte Adresse adressiert sind, an die neue Adresse umschreiben lassen.

Ein zweiter Anwendungsfall ist die Definition einer "Geheimadresse". So können Sie zum Beispiel festlegen, dass alle E-Mails mit einem Zusatz *geheim* im Adressfeld, als erwünscht bewertet und ohne Prüfung zugestellt werden. Eine Regel könnte wie folgt aussehen:

Pos.	Von	An	Entscheidung	Aktion
1	*@*	*geheim@example.com	Pass	Adressmanipulation

Die Adressmanipulation entfernt das "Code"-Wort und leitet diese E-Mail an Ihre korrekte E-Mail-Adresse weiter. Das "Code"-Wort in der Adresse können Sie natürlich selbst festlegen und bei Bedarf wieder ändern.

Fügen Sie die Aktion **Adressmanipulation** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 113](#)).



Adressmanipulation

Adressmanipulation

Diese Aktion sucht in jeder Empfängeradresse einer E-Mail nach dem angegebenen Text des Felds 'Suche' und ersetzt ihn durch den Text, der bei 'Ersetzen durch' angegeben ist (Platzhalter wie '?' und '*' sind verboten).

Beispiel: Ein Suchtext von 'geheim' und einem leeren Ersatztext wird aus einer E-Mail-Adresse wie 'max.mustergeheim@example.com' die Adresse 'max.muster@example.com' machen.

Suche (Pflichtfeld)

Ersetzen durch (optional)

Bild 113: Konfigurieren Sie Ersetzungen auf den Empfängeradressen der E-Mails

Sie können angeben, welcher Teil einer "**Code**"-**Wort-Adresse** durch einen Teil der korrekten Adresse ersetzt werden soll.

In den **Allgemeinen Einstellungen** tragen Sie unter **Suche** den zu ersetzenden String aus der "Geheim"-Adresse ein, für die die Adressmanipulation aktiv werden soll.

Unter **Ersetzen durch** geben Sie ein, mit welchem Text der Text aus dem Feld **Suche** ersetzt werden soll.

So ist es beispielsweise sinnvoll, den String "topsecret" in der "Geheim"-Adresse "user1topsecret@example.com" durch einen leeren String für die korrekte Adresse "user1@example.com" zu ersetzen.

Cyren Premium AntiVirus

Gültig für folgende Absender: **Extern** und **Lokal**.

Ungeachtet der Filterergebnisse erstellt die "Cyren AntiVirus"-Aktion anhand festgelegter Kriterien einen Fingerabdruck der zu prüfenden E-Mail und vergleicht ihn mit den Fingerabdrücken des Cyren Detection Centers im Internet. Sollte der Abdruck bekannt sein, bedeutet das, dass Cyren die E-Mail als Virus-Mail einstuft. Zusätzlich wird die vollständige E-Mail mit lokal vorgehaltenen Pattern-Dateien auf alle bekannten Viren hin überprüft.



Der Cyren-Dienst unterstützt Malwarescans bis zu einer Dateigröße von 50MB. Archive, zum Beispiel ZIP-Dateien, werden wenn möglich ausgepackt und die Dateien einzeln gescannt. Die Grenze von 50MB gilt in Archiven für die Größe der entpackten Dateien.

CSA-Whitelist

Gültig für folgende Absender: **Extern**.

Viele Newsletter sind erwünscht, da ihre Inhalte mit Zustimmung des Empfängers ausgeliefert werden. Häufig kann der Empfang solcher Newsletter nicht sichergestellt werden, da kein Level-of-Trust-Eintrag erstellt wurde. Das manuelle Eintragen aller vertrauenswürdigen Newsletter-Versender als vertrauten [Partner](#) bedeutet hier einen zu großen Aufwand .

Diese Lücke schließt die CSA-Whitelist. Sie stellt eine Positiv-Liste dar, bei der ein Kontrollgremium die Rechtmäßigkeit der versendeten Newsletter überwacht. Dadurch können Newsletter von Versendern, die sich auf der CSA-Whitelist befinden, gefahrlos zugestellt werden.

Wenn sich der Absender einer empfangenen E-Mail in der CSA-Whitelist befindet, markiert die CSA-Whitelist Aktion die E-Mail als vertrauenswürdig. Dadurch werden alle Filter der angewandten Regeln übersprungen.

Fügen Sie die Aktion **CSA-Whitelist** an Ihre Regel an. Sie erscheint danach in der Aktionsübersicht der Regel.

Die Konfiguration der Aktion wird im Knoten [Verbundene Systeme](#) vorgenommen.

Dateibasierter Virenschanner

Gültig für folgende Absender: **Extern** und **Lokal**.

Viren sind, neben Spam, eine große Bedrohung und sollten ebenfalls so früh wie möglich aussortiert werden. Auch bei der Suche nach Viren können übereifrige Filter eine erwünschte E-Mail irrtümlich entfernen. Die meisten Produkte löschen solche E-Mails, ohne den Empfänger oder Absender zu informieren. Die Problematik ist hier vergleichbar mit einem Quarantäneverzeichnis einer herkömmlichen Lösung. NoSpamProxy Protection arbeitet anders.

Die Aktion "Dateibasierter Virenschanner" speichert Anhänge von durchkommenden E-Mails in ein bestimmtes Verzeichnis. Wenn Sie einen beliebigen On-Access-Virenschanner installiert haben, wird dieser Scanner einen lesenden Zugriff auf eventuell verseuchte Anhänge verweigern. NoSpamProxy Protection prüft sofort nach Ablage der Anhänge in das Verzeichnis, ob ein Zugriff möglich ist oder nicht. Anhänge, auf die zugegriffen werden kann, werden als virenfrei angesehen. NoSpamProxy Protection kann mit jedem beliebigen Virenschanner zusammen arbeiten, der in Echtzeit Dateizugriffe überwacht. Diese Scan-Methode ist auf sehr vielen Dateiservern bereits installiert, sehr performant und zuverlässig.

Auch Anhänge aus E-Mails im RTF-Format können von Virenschannern verarbeitet werden. Die Anhänge - die standardmäßig den Namen winmail.dat erhalten - werden überprüft und bei Bedarf einzeln geblockt. Beachten Sie, dass diese Art der Verarbeitung eine Veränderung der E-Mail darstellt.

Das Verzeichnis für die temporäre Speicherung von Dateien ist in aktuellen Installationen `%ProgramData%\Net at Work Mail Gateway\Temporary Files\Netatwork.NospamProxy.Addins.Core.Actions.FileVirusScanAction`. In älteren Installationen können die Dateien auch im Installationsverzeichnis von NoSpamProxy unter `"\AntiSpam Role\Temporary Files\Netatwork.NospamProxy.Addins.Core.Actions.FileVirusScanAction"` liegen.



Beim simultanen Betrieb von On-Access-Virenschannern und dem integrierten [CYREN Premium Antivirus](#) treten unter Umständen Probleme auf. Der Grund hierfür ist, dass der Virenschanner die von CYREN Premium Antivirus abgelegten, für dessen Betrieb benötigten Dateien möglicherweise als schädlich einstuft und löscht bzw. blockiert. Dadurch kann die Funktionalität von CYREN Premium Antivirus beeinträchtigt werden. Konfigurieren Sie Ihren Virenschanner deshalb so, dass die Verzeichnisse `C:\ProgramData\Net at Work Mail Gateway\CYREN` und `C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailQueues` sowie `C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailsOnHold` auf allen Systemen mit installierter Gateway Rolle oder Webportal vom Scan ausgeschlossen werden. Beachten Sie, dass es sich hierbei um versteckte Verzeichnisse handeln kann.

Sie können selbst einstellen, ob verseuchte Anhänge nur gelöscht werden oder ob die zugehörige E-Mail automatisch geblockt werden soll.



Falls eine E-Mail abgewiesen wird, wird der Absender darüber durch den einliefernden Server informiert. Über einen gelöschten Anhang wird weder der Absender noch der Empfänger informiert.

Fügen Sie die Aktion **Dateibasierter Virenschanner** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 114](#)).

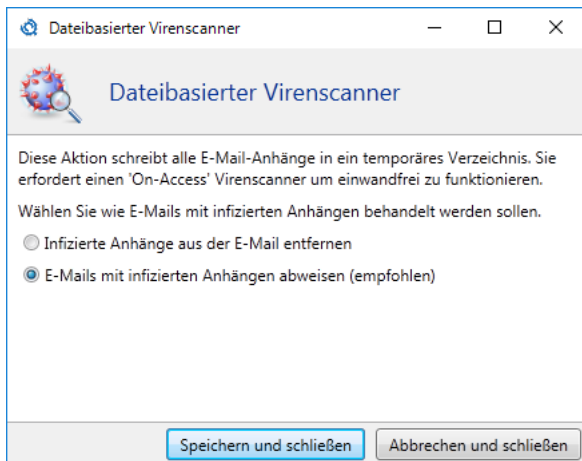


Bild 114: Konfigurieren Sie die Aktion für den dateibasierten Virenschanner

Wenn Sie diese Art von E-Mails ablehnen wird - wie bei einer erkannten Spam-E-Mail - der einliefernde E-Mail-Server eine Unzustellbarkeitsnachricht abschicken. Das Risiko einer Falscherkennung entfällt.

In der dateibasierten Virenschanner Aktion können Sie festlegen, wie mit verseuchten Anhängen und der zugehörigen E-Mail verfahren wird.

Wählen Sie aus, ob infizierte Anhänge aus der E-Mail entfernt werden sollen oder ob E-Mails mit infizierten Anhängen abgewiesen werden sollen. Die Aktion wird nun in der Übersicht der Aktionen in der Regel angezeigt.



Wie bei allen Virenschannern, werden auch hier kennwortgeschützte ZIP-Dateien nicht überprüft und ohne weitere Prüfung weitergegeben.

Greylisting

Gültig für folgende Absender: **Extern**.

Das Greylisting ist eine Vorsichtsmaßnahme gegen "verdächtige" E-Mails. Bleibt eine E-Mail knapp unter dem von Ihnen definierten Spam-Schwellenwert, würde diese E-Mail ohne Greylisting als ausreichend gut bewertet werden. Die Greylisting-Aktion lässt nun diese E-Mail nicht gleich durch,

sondern lehnt sie temporär ab. Der einliefernde E-Mail-Server erhält eine Fehlermeldung die ihn anweist, die E-Mail nach einiger Zeit erneut zu senden. Im zweiten Versuch wird die E-Mail dann zugestellt. Dabei kann eingestellt werden, ab wann der einliefernde Server einen zweiten Versuch starten darf.

Hinter dieser Aktion steht folgendes Prinzip: Ein Spammer scheut in der Regel die Mühe, eine zweite E-Mail zu senden. Ein normaler Absender hingegen wird nach einiger Zeit erneut die Zustellung versuchen. Bei dem zweiten Versuch wird nun diese Verbindung besser bewertet, so dass die E-Mail passieren kann.

Den Schwellenwert, ab wie vielen Malus-Punkten eine eigentlich passierende E-Mail als "verdächtig" eingestuft wird, können Sie individuell einstellen.

Fügen Sie die Aktion **Greylisting** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration ([Bild 115](#)).

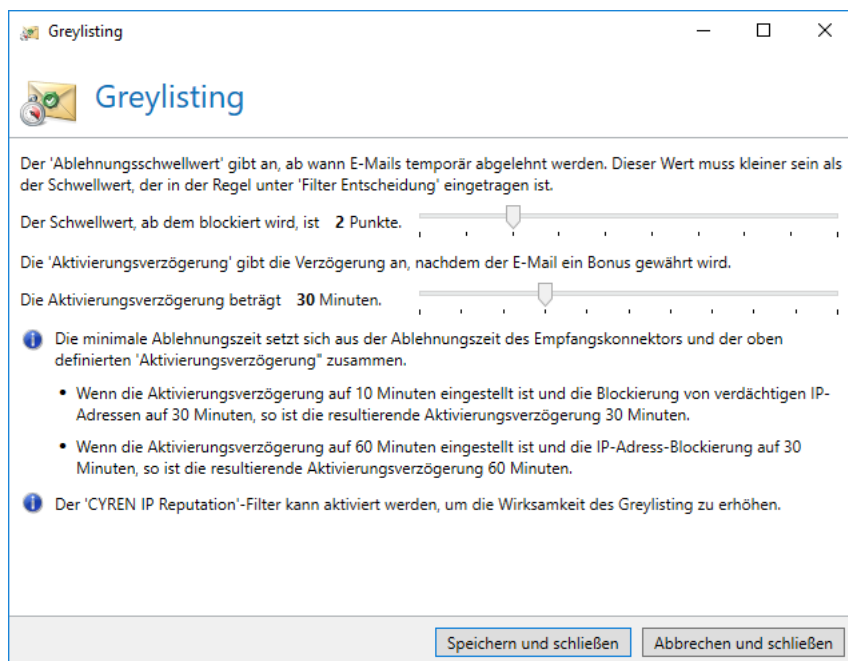


Bild 115: Konfigurieren Sie die Optionen des Greylisting

Sie können angeben, ab welchem Schwellenwert das Greylisting aktiv wird und die Verzögerungszeit einstellen, nach der der Level-of-Trust-Eintrag erfolgen soll.

Mit dem Schieberegler **Der Schwellenwert, ab dem blockiert wird** können Sie angeben, ab welchem Schwellenwert (SCL) E-Mails für das Greylisting zwischenzeitlich geblockt werden sollen. Dieser Greylisting-Schwellenwert muss niedriger sein, als der Spam-Schwellenwert, andernfalls würde das Greylisting nicht greifen.

Des Weiteren können Sie die **Aktivierungsverzögerung** ändern. Damit bestimmen Sie die Verzögerungszeit, nach der die E-Mail besser bewertet wird.



Das Greylisting wird übersprungen, wenn der Filter [Cyren IP Reputation](#) für die IP-Adresse die Reputation als "Gut" meldet.

Verberge interne Topologie

Gültig für folgende Absender: **Lokal**.

Die Aktion **Verberge interne Topologie** entfernt die "Received"-E-Mail-Header einer E-Mail von einem lokalem Absender. Durch diese Received-Einträge kann ansonsten ein Rückschluss auf die lokale Topologie erfolgen.

Automatische Antwort

Gültig für folgende Absender: **Extern** und **Lokal**.

Die Aktion **Automatische Antwort** sendet eine automatische Antwort an den Absender einer E-Mail ([Bild 116](#)). Der Text der E-Mail wird über eine Vorlage aus dem **Templates**-Ordner der Intranet Rolle erzeugt. Vom Setup wird eine Beispiel-Vorlage (**SampleAutoReply.cshtml**) in den Ordner kopiert. Von dieser Vorlage können Sie Kopien erstellen und diese auf Ihre Bedürfnisse anpassen.



Änderungen an Vorlagen werden innerhalb weniger Minuten von der Intranet Rolle zu allen Gateway Rollen repliziert. Die Rollen müssen dafür nicht neugestartet werden.

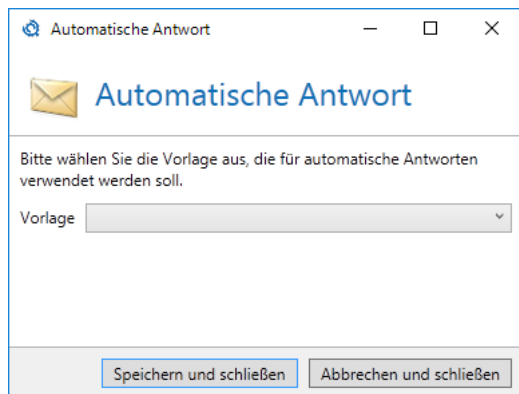


Bild 116: Automatische Antwort erstellen

Leite E-Mail um

Gültig für folgende Absender: **Extern** und **Lokal**.

Die Aktion bietet die Möglichkeit die Empfänger einer E-Mail zu ergänzen oder komplett zu ersetzen. E-Mails werden Abhängig von den Einstellungen entweder zusätzlich oder nur zu den in der Aktion hinterlegten Empfängern zugestellt ([Bild 117](#)).

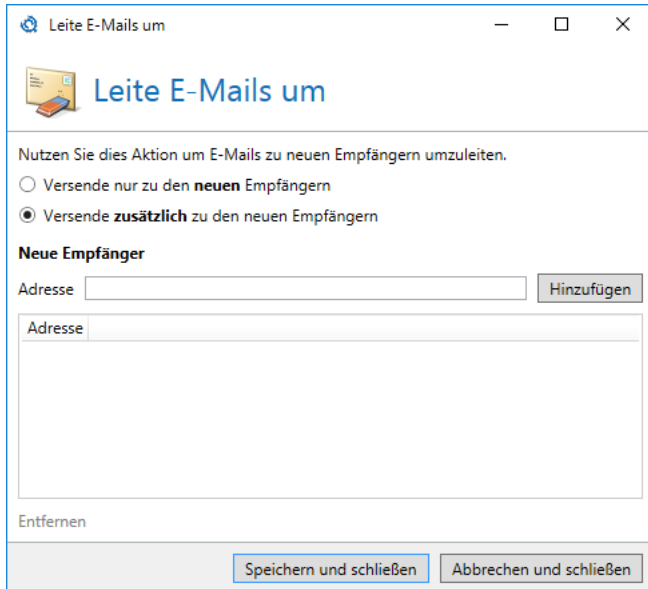


Bild 117: Konfiguration zur Umleitung von E-Mails

Es muss mindestens eine Empfängeradresse in der Liste hinterlegt werden, um die Aktion nutzen zu können.

DKIM-Signatur anwenden

Gültig für folgende Absender: **Lokal**.

Diese Aktion bringt eine DKIM-Signatur (DomainKeys Identified Mail) auf ausgehende E-Mails auf. Damit kann der Empfänger sicherstellen, dass die E-Mail auch wirklich von Ihrem Unternehmen gesendet wurde. Um die Signatur erstellen zu können, ist ein DKIM-Schlüssel erforderlich. Wie Sie einen solchen Schlüssel erstellen und veröffentlichen, erfahren Sie im Kapitel [DomainKeys Identified Mail](#).

Disclaimer anwenden




Für die Benutzung der Disclaimer-Funktion muss diese lizenziert sein.

Gültig für folgende Absender: **Lokal**.

Diese Aktion fügt in ausgehende Nachrichten einen Disclaimer an. Dazu werden die Disclaimer-Regeln und -Vorlagen ausgewertet und an die entsprechenden Stellen in der E-Mail angehängt. Im Kapitel [Disclaimer](#) erfahren Sie, wie Sie die Disclaimer konfigurieren können.

Berechnung des Spam Confidence Level

NoSpamProxy Protection weist alle E-Mails ab, deren Spam Confidence Level (SCL) über einem bestimmten Schwellwert liegt. Diesen Schwellwert legen Sie als Administrator in den einzelnen Regeln fest. Der folgende Absatz erläutert die Vorgehensweise von NoSpamProxy Protection bei der Berechnung des SCL. Zunächst wird an einem sehr einfachen Beispiel erläutert, wie die Filter ohne das Level-of-Trust-System arbeiten. Die folgende Filterkonfiguration ist dabei gegeben ([Bild 118](#)).

 E-Mail überprüfen
Abweisen wenn SCL ist größer 4

Realtime Blocklists (2)
Spam URI Realtime Blocklists (2)
Wortübereinstimmungen (1)

Bild 118: Die Beispielkonfiguration für die Berechnung des SCL Wertes

In diesem Beispiel sollen E-Mails überprüft und abgewiesen werden, sobald der SCL größer oder gleich 4 ist. Es sind drei Filter aktiviert: Realtime Blocklists, Spam URI Realtime Blocklists und die Wortübereinstimmungen. Der Filter Wortübereinstimmungen ist so konfiguriert, dass er nach den Wörtern Sex, Viagra, Cialis usw. suchen und pro Treffer zwei Strafpunkte vergeben soll. Die beiden Blocklistenfilter sollen pro Treffer zwei Punkte vergeben. Das Level-of-Trust-System ist ausgeschaltet.

Nun wird eine Mail verarbeitet, die acht verbotene Wörter und einen verbotenen Link enthält. Der Link ist auf einer Blacklist enthalten. Des Weiteren ist die einliefernde IP-Adresse auf zwei Blacklists vertreten. Hier zunächst das vorläufige Ergebnis der Filter:

Filter	SCL Bewertung des Filters
Realtime Blocklists	4 (Zwei Treffer X zwei Strafpunkte pro Treffer)
Spam URI Realtime Blocklists	2 (Ein Treffer X zwei Strafpunkte pro Treffer)
Wortübereinstimmungen	16 (Acht Treffer X zwei Strafpunkte pro Treffer)

Grundsätzlich ist es bei allen Filtern - auch dem Level-of-Trust-System - so, dass der ermittelte Wert immer auf 10 zurückgekürzt wird, wenn er größer als "10" ist. Bei negativen Werten die kleiner als "-10" sind, wird der Wert auf -10 angepasst. In unserem Beispiel wäre dann der Nettowert der Filter wie folgt:

Filter	SCL Bewertung des Filters
Realtime Blocklists	4
Spam URI Realtime Blocklists	2

Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)
-----------------------	---

Abschließend wird der Multiplikator der einzelnen Filter berücksichtigt. Die Filter Realtime Blocklists und Spam URI Realtime Blocklists haben den Multiplikator "2", die Wortübereinstimmungen haben den Multiplikator "1". Der Nettowert der Filter wird nun mit der jeweiligen Multiplikator multipliziert. Folgende Werte ergeben sich nun:

Filter	SCL Bewertung des Filters	Multiplikator	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Gesamt			22

Die E-Mail erhält also einen SCL von 22 und wird damit abgewiesen.

Im zweiten Beispiel wird die Filterkonfiguration aus dem ersten Beispiel lediglich um das Level-of-Trust-System erweitert. Es handelt sich des Weiteren um die gleiche E-Mail wie im vorigen Beispiel. Wir gehen aber davon aus, dass es sich hier um eine gewollte E-Mail handelt und es von der Absender- und Empfänger-Adresse bereits ein Adresspäarchen und einen Domänenbonus in der Datenbank gibt. Da der letzte Mailkontakt bereits vier Tage zurückliegt, ist der Adresspäarchen-Bonus mit 65 Bonuspunkten nicht mehr so hoch. Die Domäne hingegen steht mit statischen 100 Bonuspunkten in den Vertrauensstellungen. Bei den Bonuspunkten des Level-of-Trust-Systems in der Datenbank handelt es sich nicht direkt um den SCL Wert, sondern um die sogenannten Vertrauenspunkte. Diese werden nur innerhalb der Filter verwendet.

Das Level-of-Trust-System bewertet nun wie folgt:

Zunächst wird der größte Wert der einzelnen Level-of-Trust-Werte (Adress-, Domänen-, Betreff-, Messageld-Bonus, sowie die Punkte der DSN-Prüfung) genommen "100". Zur Berechnung des SCL wird diese Summe grundsätzlich durch den Wert "-10" dividiert und ergibt in diesem Beispiel einen SCL von -10 Punkten. Wie bei allen anderen Filtern auch, wird der ermittelte Wert auf 10 oder -10 beschnitten. Die Tabelle mit den Nettowerten aller Filter sieht nun wie folgt aus:

Filter	SCL Bewertung des Filters
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)
Level-of-Trust-System	-10

Den Multiplikator der einzelnen Filter können Sie in der jeweiligen Regel festlegen. Das Level-of-Trust-System hingegen ermittelt seinen Multiplikator selbstständig. Dazu werden die Multiplikatoren aller anderen Filter addiert und ergeben in diesem Beispiel den Wert "5". Die endgültige Berechnung des SCL mit dem Einfluss des Level-of-Trust-Systems sieht dann wie folgt aus:

Filter	SCL Bewertung des Filters	Multiplikator	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Level-of-Trust-System	-10	5 (=2+2+1)	-50
Gesamt			-28

Die E-Mail wäre in diesem Beispiel zugestellt worden, da der SCL kleiner als 4 ist.

Um das Beispiel zu verdeutlichen, wird der Filter "Cyren AntiSpam" mit dem Multiplikator "3" ebenfalls konfiguriert. Dieser Filter vergibt bei einem Treffer immer 4 Punkte und dieser Wert ist auch nicht konfigurierbar. ([Bild 119](#))

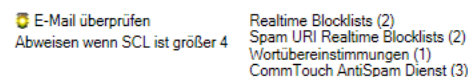


Bild 119: Zur Berechnung der SCL wurde der "Cyren AntiSpam" Filter hinzugefügt

Der "Cyren AntiSpam" Filter bewertet die E-Mail ebenfalls schlecht. Das Endergebnis der SCL Berechnung sieht dann wie folgt aus:

Filter	SCL Bewertung des Filters	Multiplikator	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Cyren AntiSpam	4	3	12
Level-of-Trust-System	-10	8 (=2+2+1+3)	-80
Gesamt			-46

Der Multiplikator des Level-of-Trust-Systems hat sich durch den zusätzlichen Filter automatisch angepasst und kann sich dadurch noch entscheidender durchsetzen. Es wird damit gewährleistet, dass gewollte Kommunikation auch immer den Empfänger erreicht - unabhängig vom Inhalt der E-Mail.

Voreinstellungen

Dieser Bereich beinhaltet globale Einstellungen, die in anderen Bereichen der Konfiguration (zum Beispiel Regeln, Partner oder Unternehmensbenutzer) benutzt werden können ([Bild 120](#)).

Farbschema

Die folgenden Einstellungen werden im Web Portal und in E-Mails für Benachrichtigungen verwendet.

Die Schriftart ist **Calibri, Verdana, Arial** mit einer Größe von **16px**.

Die Farben sind **#C01B1B** für die Akzentfarbe, **#d2d6d9** für Rahmen, **#F8F8F8** für den Hintergrund des Inhalts und **#ffffff** für den Hintergrund des Logos.

Das Logo ist **links** ausgerichtet, es wird das unten stehende Bild verwendet.

noSpam proxy

[Bearbeiten](#)

Wortübereinstimmungen

Globale Wortgruppen

Name	Bereich	Suchkriterium	Format	Punkte pro Treffer
Common notation for medical products	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common notation of commercial words	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common notation of porn words	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common spam words (german)	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Realtime Blocklists

Globale Blocklists

Name	Typ	URL
Bonded Sender	DNS	query.bondedsender.org
CRI Composite Blocking List	DNS	chlabuseat.org

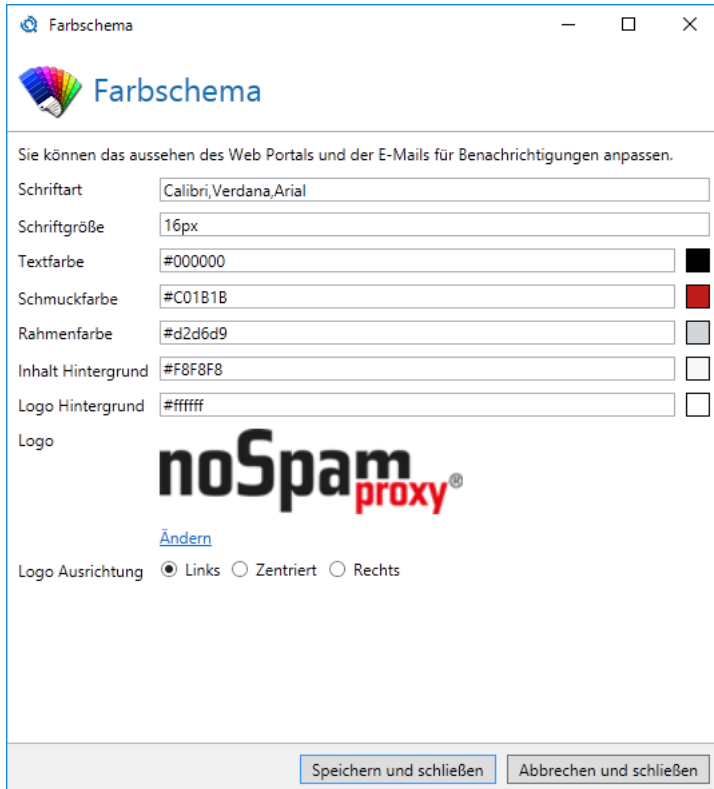
Bild 120: Voreinstellungen



Die Änderung von Einstellungen in diesem Bereich wirkt sich auch auf bestehende Regeln, Partner oder Unternehmensbenutzer aus. Die Einstellungen gelten immer für alle Konfigurationen, in denen sie referenziert werden.

Farbschema

Über das Farbschema können Sie das Aussehen der von NoSpamProxy generierten E-Mails sowie das des Web Portals an Ihre Bedürfnisse anpassen ([Bild 121](#))





Farbschema


Sie können das Aussehen des Web Portals und der E-Mails für Benachrichtigungen anpassen.


Schriftart:


Schriftgröße:

Textfarbe: 


Schmuckfarbe: 

Rahmenfarbe: 

Inhalt Hintergrund: 

Logo Hintergrund: 

Logo



[Ändern](#)

Logo Ausrichtung: ☒ Links ☐ Zentriert ☐ Rechts

Bild 121: Dialog für das Ändern des Farbschemas.

Im Normalfall werden Sie nur die Akzentfarbe und das Logo an Ihre Corporate Identity anpassen müssen.

Das Farbschema wird auf folgende Element angewendet:

- Das Web Portal
- Alle von NoSpamProxy erzeugten E-Mail-Benachrichtigungen
- Den Ersatz-Anhang für Dateien, die über Large Files verschickt werden.

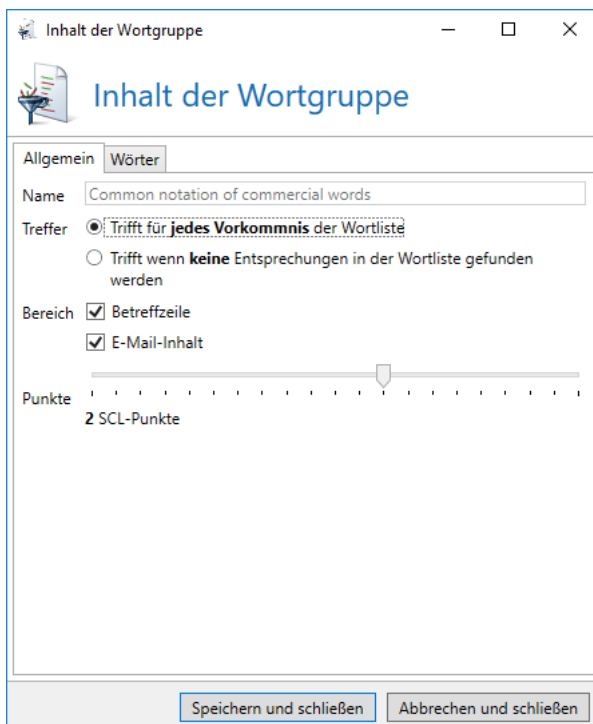
Wortübereinstimmungen

Im Abschnitt **Wortübereinstimmungen** haben Sie die Möglichkeit, Listen mit Ausdrücken zu pflegen, für die Sie entweder Bonus- oder Malus Punkte vergeben möchten. Die Ausdrücke werden in einzelnen Wortgruppen zusammengefasst, die Sie dann später in den einzelnen Regeln verwenden können. Pro

Wortgruppe legen Sie fest, ob für die Begriffe dann Bonus- oder Malus Punkte vergeben werden sollen. So haben Sie die Möglichkeit, Gruppen mit gewollten und ungewollten Ausdrücken zu erstellen.

Neue Wortgruppe hinzufügen

Auf der Seite **Allgemein** definieren Sie, wie die Treffer der Wortgruppe gewertet werden und wo sie gesucht werden ([Bild 122](#)). Zusätzlich können Sie noch einstellen, ob Sie Punkte für jedes Vorkommen eines Wortes verteilen möchten, oder ob Sie nur Punkte verteilen, wenn keins der Wörter in Inhalt oder dem Betreff zu finden ist.



The screenshot shows a window titled 'Inhalt der Wortgruppe' with a tabbed interface. The 'Allgemein' tab is active. It contains the following fields and options:

- Name:** A text box containing 'Common notation of commercial words'.
- Treffer:** Two radio buttons. The first is selected and labeled 'Trifft für jedes Vorkommnis der Wortliste'. The second is labeled 'Trifft wenn keine Entsprechungen in der Wortliste gefunden werden'.
- Bereich:** Two checked checkboxes: 'Betreffzeile' and 'E-Mail-Inhalt'.
- Punkte:** A horizontal slider bar with a handle in the middle. Below it, the text '2 SCL-Punkte' is displayed.
- Buttons:** At the bottom, there are two buttons: 'Speichern und schließen' and 'Abbrechen und schließen'.

Bild 122: Einstellungen zur Bewertung und des Suchbereichs

Die Seite **Wörter** definiert die Art der Suchwörter und die Suchwörter selbst. Die Suche unterscheidet nicht zwischen Groß- und Kleinschreibung, so dass die Groß- und Kleinschreibung bei der Eingabe der Wörter vernachlässigt werden kann. Bei der einfachen Suche und der Suche mit Platzhaltern steht zusätzlich noch die Option **Auch ähnliche Wörter finden** zu Verfügung ([Bild 123](#)). Die suche nach ähnliche Wörtern lässt NoSpamProxy beim Beispiel "Viagra" auch Wörter wie "V1agr@", "Vlagra", "V1@gra" oder "V-I-A-G-R-A" finden.

Die Option **Platzhalter** bedeutet, dass Sie die Möglichkeit haben, mit Platzhaltern ('*' und '?') zu arbeiten, so dass Sie auch zum Beispiel auch "Cialis*" eingeben können, um nach allen Begriffen zu suchen, in denen das Wort "Cialis" am Anfang steht.



Die Suchart **Einfach** ist empfehlenswert, da hiermit eine gegenüber den anderen Arten vielfach höhere Suchleistung erreicht wird.

Inhalt der Wortgruppe

Inhalt der Wortgruppe

Allgemein Wörter

Art

☐ Einfach (*schnell*, empfohlen)

☒ Platzhalter (langsamer, '?' und '*' erlaubt)

☐ Regulärer Ausdruck (langsamer, mit Vorsicht verwenden)

Neues Wort

Wort

e-mail marketing

eliminate your debt

refinance

mortgage

Entfernen

☒ Auch ähnliche Wörter finden

Bild 123: Definition der Wortgruppe



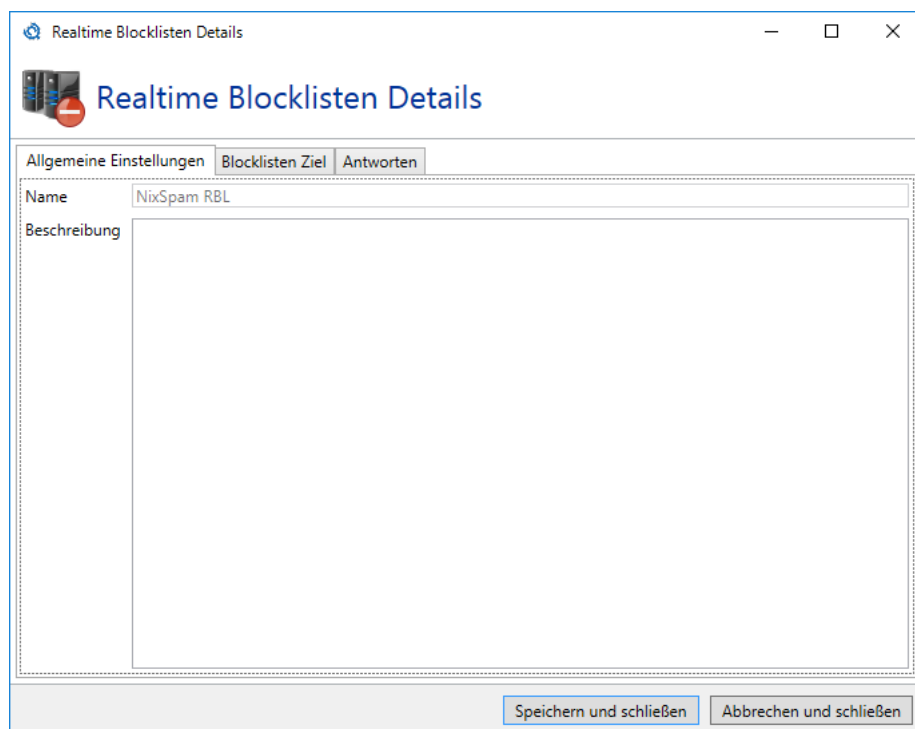
Wenn Sie Änderungen an den Wortgruppen vornehmen, wirken sich diese auf alle Regeln aus, die den Filter "Wortübereinstimmungen" verwenden und die entsprechende Wortgruppe konfiguriert haben.

Realtime Blocklists

Realtime Blocklists (RBL) verwalten Listen mit verdächtigen Spam-IP-Adressen. Über das Internet ist es nun möglich zu überprüfen, ob gegebenenfalls eine IP-Adresse in der RBL-Liste vorhanden ist oder nicht. Diese Blocklists werden im Abschnitt **Realtime Blocklists** gepflegt und können in den Regeln dann später einzeln ausgewählt werden.

Neue Blocklist hinzufügen

Unter **Allgemeine Einstellungen** ([Bild 124](#)) geben Sie im Feld **Name** zunächst den Namen der neuen RBL-Liste an. Im Feld **Beschreibung** können Sie persönliche Anmerkungen machen. Beide Einträge sind nur beschreibende Details und für die Funktion der Liste nicht relevant.



Realtime Blocklisten Details

Realtime Blocklisten Details

Allgemeine Einstellungen | **Blocklisten Ziel** | Antworten

Name: NixSpam RBL

Beschreibung:

Speichern und schließen | Abbrechen und schließen

Bild 124: Geben Sie den Namen und eine Beschreibung der Blocklist ein

Auf der Registerkarte **Blocklist-Ziel** geben Sie an, ob es sich um eine RBL-Liste handelt, die per DNS oder HTTP angesprochen wird. Im Feld **Adresse** wird dann entweder die IP-Adresse oder der Servername des abzufragenden Servers eingetragen.

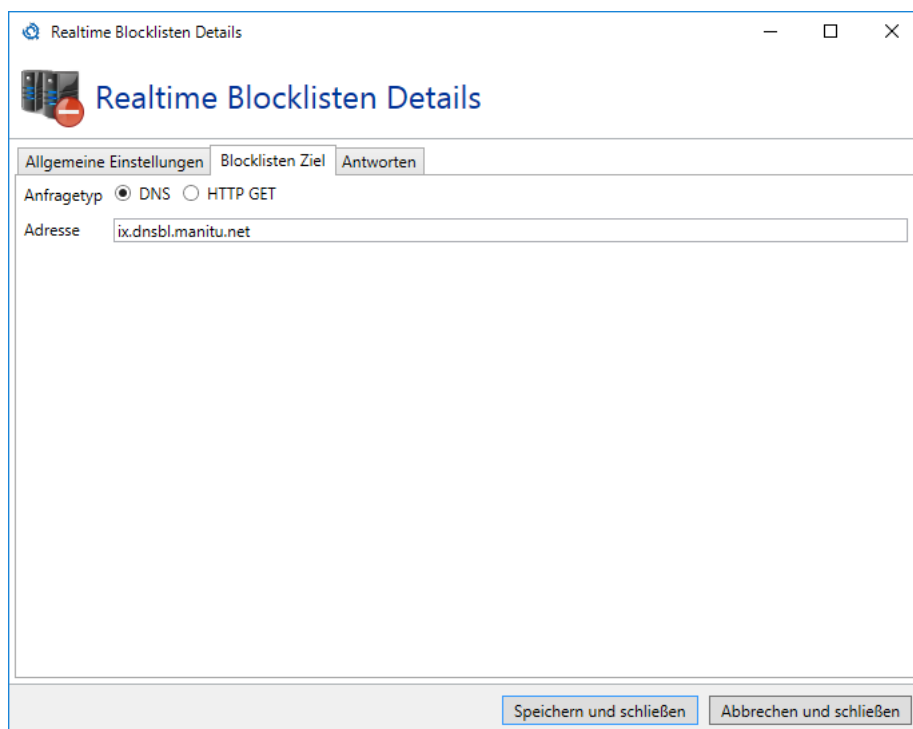


Bild 125: Der Dialog für die Definition einer Blocklist-Antwort

Auf der Registerkarte **Antworten** definiert man die möglichen Antworten des angefragten Servers und deren Bedeutung ([Bild 126](#)).

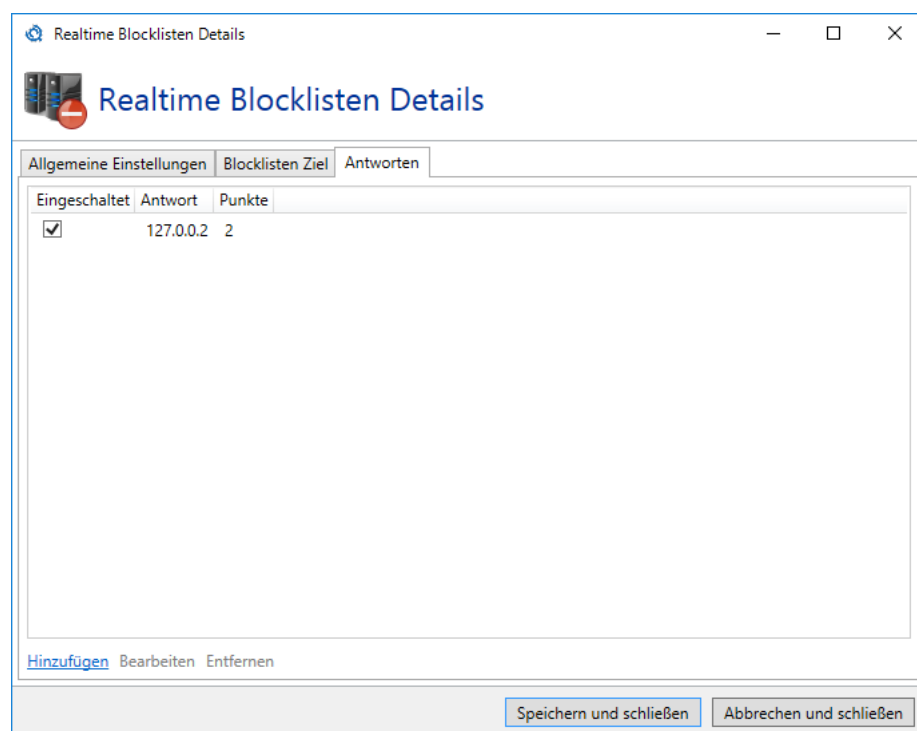


Bild 126: Alle zu erwartenden Antworten der Blocklist und deren Bewertung in SCL Punkten

Sie können neue Antworten im Dialog **Antwort Details** ([Bild 127](#)) hinzufügen. Legen Sie dort für die Antwort fest, wie viele SCL-Punkte aus ihr resultieren. Fügen Sie außerdem einen beschreibenden Fehlertext hinzu. Ein negativer Wert entspricht Bonuspunkten, ein positiver Wert entspricht Maluspunkten. Der Text der Antwort taucht gegebenenfalls im Unzustellbarkeitsbericht auf, wenn der erstellende Server dies unterstützt. So weiß der Versender der abgewiesenen E-Mail, auf welcher Blacklist er aus welchem Grund steht. Die Antwort kann auch deaktiviert werden.

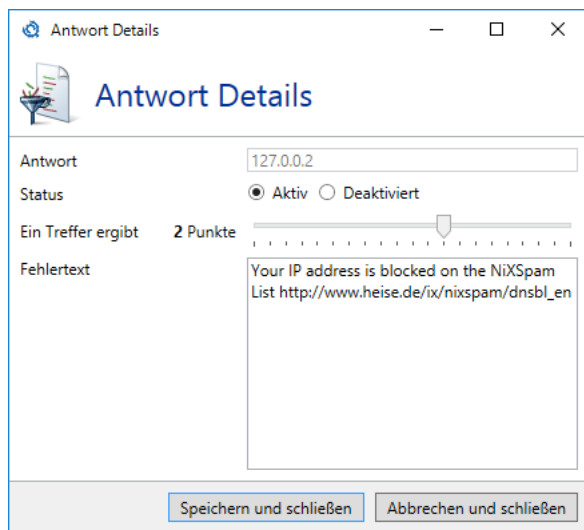


Bild 127: Eine Antwort der Liste

Inhaltsfilter



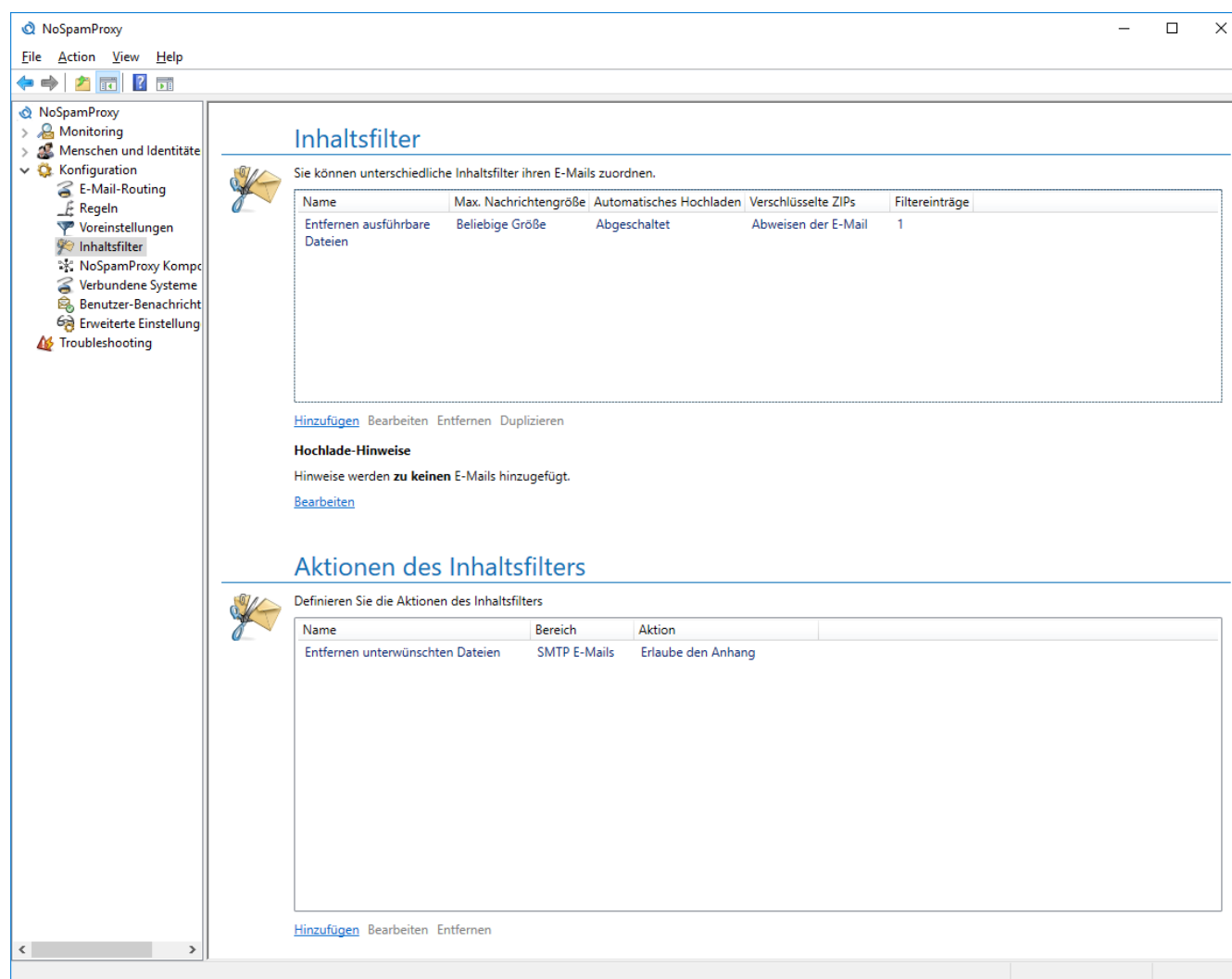
Dieser Bereich ist verfügbar, falls NoSpamProxy Large Files oder NoSpamProxy Protection lizenziert ist. Einzelne Funktionen innerhalb des Bereichs sind abhängig von Ihrer Lizenz.

Die Liste der Inhaltsfilter dient zum Erlauben, Blockieren und Umleiten von Anhängen, die einem der dort definierten Filtern entsprechen ([Bild 128](#)). Diese Liste dient der zentralen Verwaltung der Inhaltsfilter, damit Sie sowohl in den [Partnern](#), wie auch den [Unternehmensbenutzern](#) verwendet werden kann. Ein Inhaltsfilter kann im Partner Knoten in den **Standardeinstellungen für Partner**, in einem **Domäneneintrag** eines Partners sowie einer Partner E-Mail-Adresse zugeordnet werden. Die Einstellungen auf einer E-Mail-Adresse haben dabei Vorrang vor den Einstellungen auf einer Domäne und die Einstellungen auf einer Domäne haben Vorrang vor den Standardeinstellungen für Partner.



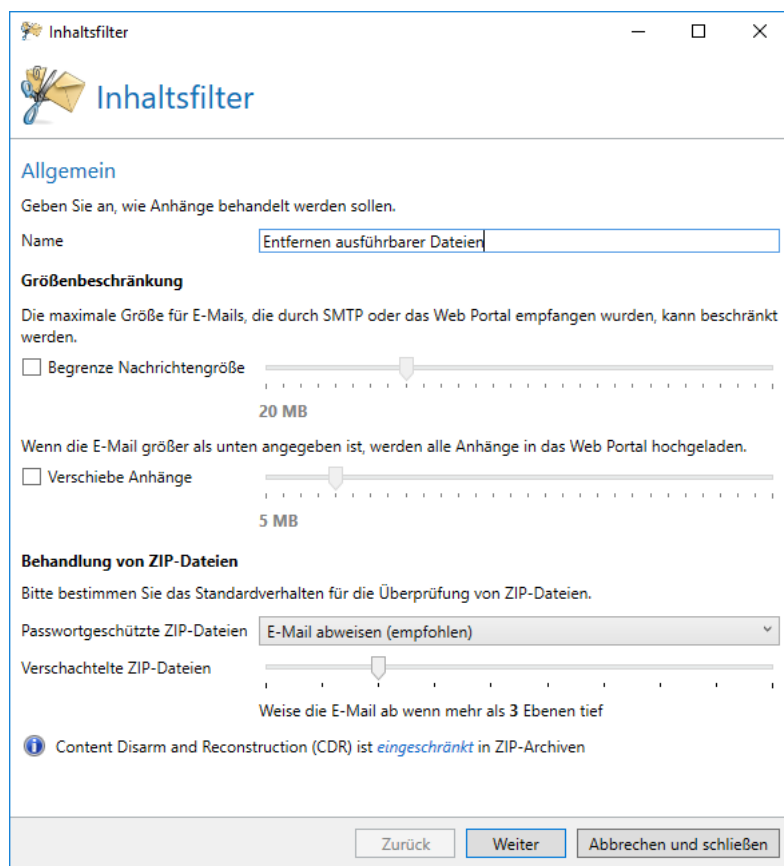
Sie können die Inhaltsfilter zusätzlich zu den Einstellungen auf den **Unternehmensbenutzern** und **Partnern** auch in den [Regeln](#), im Abschnitt **Allgemein**, ein- oder ausschalten.

In der Liste der Inhaltsfilter besteht jeder Filter aus mehreren Einträgen, in denen jeweils **Bedingungen** wie Dateiname, Typ oder Größe für die E-Mail-Anhänge definiert sind, sowie die dann auszuführenden [Aktionen](#), wie Sperren, Zulassen, Hochladen der Anhänge oder Abweisen der E-Mail. Die Aktionen werden zuvor in einer eigenen Liste konfiguriert und können dadurch in mehreren Inhaltsfiltereinträgen wiederverwendet werden.

**Bild 128: Die Übersicht der Inhaltsfilter**

Inhaltsfilter

Legen Sie für einen Inhaltsfilter einen eindeutigen und sprechenden Namen fest. Außerdem können Sie die Größen für E-Mails und Anhänge beschränken. E-Mails, deren Größe die maximal erlaubte überschreitet, werden abgewiesen. Bei der Analyse von ZIP-Dateien können Sie festlegen, wie damit umgegangen wird, falls die Dateien passwortgeschützt sind und wie viele Ebenen von ineinander geschachtelten Dateien analysiert werden sollen. Die Beschränkung dient dazu, sehr hoch bis unendlich geschachtelte ZIP-Dateien auszusortieren ([Bild 129](#)).



Inhaltsfilter

Allgemein

Geben Sie an, wie Anhänge behandelt werden sollen.

Name:

Größenbeschränkung

Die maximale Größe für E-Mails, die durch SMTP oder das Web Portal empfangen wurden, kann beschränkt werden.

☐ Begrenze Nachrichtengröße: 20 MB

Wenn die E-Mail größer als unten angegeben ist, werden alle Anhänge in das Web Portal hochgeladen.

☐ Verschiebe Anhänge: 5 MB

Behandlung von ZIP-Dateien

Bitte bestimmen Sie das Standardverhalten für die Überprüfung von ZIP-Dateien.

Passwortgeschützte ZIP-Dateien:

Verschachtelte ZIP-Dateien:

Content Disarm and Reconstruction (CDR) ist eingeschränkt in ZIP-Archiven

Bild 129: Allgemeine Einstellungen eines Inhaltsfilters

Ein Inhaltsfilter kann mehrere Einträge enthalten, um für einen Benutzer alle notwendigen Aktionen auf unterschiedlichen Dateianhängen konfigurieren zu können ([Bild 130](#)). Die Einträge werden von oben nach unten abgearbeitet und können mit den Pfeilen am linken Rand der Liste umsortiert werden. Trifft kein Filtereintrag eines gewählten Inhaltsfilters auf einen Anhang zu, wird dieser normal zugestellt.



Bild 130: Die Liste der Inhaltsfiltereinträgen

Ein Eintrag eines Inhaltsfilters kann Bedingungen enthalten, nach denen Anhänge ausgewählt werden ([Bild 131](#)). Hier stehen Ihnen mehrere Auswahlkriterien zur Verfügung, die auch kombiniert werden können ([Bild 132](#)). Falls der Eintrag auf alle Anhänge zutreffen soll, können Sie eine Bedingung mit den Standardeinstellungen hinzufügen. Sie können für die unterschiedliche Einstufung einer E-Mail bzw. der unterschiedlichen E-Mail-Richtung jeweils andere Aktionen definieren. Für E-Mails aus dem Web Portal können Sie auch das Verhalten der konfigurierten Aktion für ein- bzw. ausgehende SMTP-E-Mails auswählen, dann werden die Anhänge analog zu der gewählten SMTP-Aktion verarbeitet, ohne dass Sie eine eigene Web Portal Aktion konfigurieren müssen.

Inhaltsfilter

Die unten stehende Aktion wird angewandt wenn eine dieser Bedingungen erfüllt ist.

Name: Ausführbare Dateien

Bedingung

Dateityp	Dateiname	Min Größe	Max Größe	Bereich
Ausführbare Dateien	Beliebig	Beliebig	Beliebig	Überall

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

Aktion

Unterschiedliche Aktionen können, abhängig von der Einstufung der E-Mail, angewandt werden.

Nicht vertrauenswürdige oder ausgehende E-Mails: Entfernen unterwünschten Dateien

Vertrauenswürdige E-Mails: Entfernen unterwünschten Dateien

Web Portal E-Mails: -- Nutze die Aktion für nicht vertraute oder ausgehende E-Mails --

[Speichern und schließen](#) [Abbrechen und schließen](#)

Bild 131: Ein Inhaltsfiltereintrag

Eine **Bedingung** beschreibt die Dateien, die von dem Inhaltsfilter bearbeitet werden. Sie können hier nach verschiedenen Eigenschaften der Anhänge filtern. Der Abschnitt **Bereich** legt fest ob auch Dateien innerhalb von ZIP-Dateien analysiert werden. Dadurch können alle Analysefunktionen des Inhaltsfilter auch auf die ZIP-Dateien angewendet werden.

Bedingung

Beschreiben Sie welche Dateien Sie finden wollen.

☒ Dateityp [Ausführbare Dateien](#)

☐ Dateiname

Nutzen Sie '?' und '*' als Platzhalter. Trennen Sie mehrere Einträge mit ','

☐ Minimale Größe

5 MB

☐ Maximale Größe

20 MB

Bereich

☒ Überall anwenden

☐ Nur auf Dateien **innerhalb** von ZIP-Dateien anwenden

☐ Nur auf Dateien **außerhalb** von ZIP-Dateien anwenden

Speichern und schließen Abbrechen und schließen

Bild 132: Eine Bedingung für die Auswahl von Anhängen

Der **Dateityp** in einer Bedingung bietet Ihnen sogar die Möglichkeit, nach dem tatsächlichen Inhalt von Anhängen zu filtern, damit auch Anhänge mit umbenannten Dateiendungen sicher gefunden und bearbeitet werden können ([Bild 133](#)).

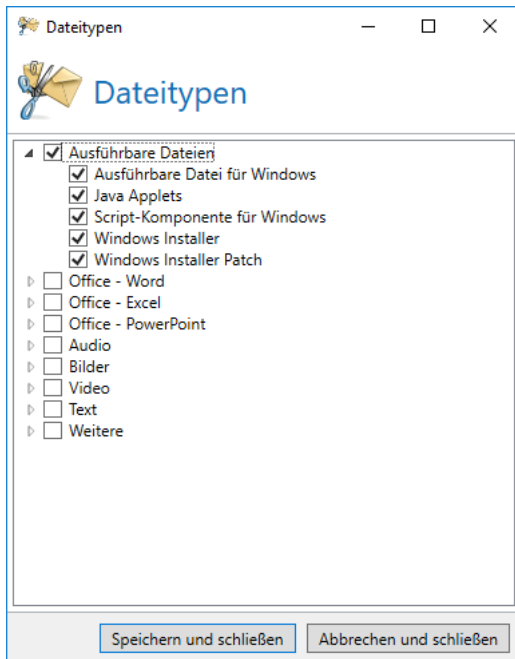
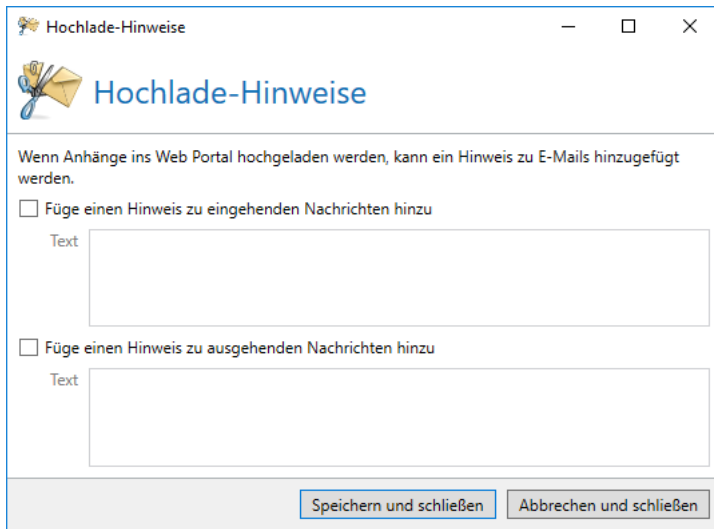


Bild 133: Der Dialog für die Auswahl von Dateitypen

Weitere Informationen zur Filterung von RTF-Dateien finden Sie im Anhang unter [Verarbeitung von RTF-Dateien bei der Inhaltsfilterung](#).

Hinweise zum Hochladen

Manche Benutzer bemerken nicht sofort, wenn ein Anhang von einer E-Mail entfernt und in das Web Portal hochgeladen wurde. Vergessen diese dann, die Datei herunterzuladen, ist die Datei irgendwann nicht mehr verfügbar. Um dies zu vermeiden, können Sie ein- und ausgehenden Nachrichten einen Text beifügen, mit dem Sie die Empfänger auf den Umstand hinweisen können, dass Anhänge ins Web Portal verschoben werden können ([Bild 134](#)).



Hochlade-Hinweise

Hochlade-Hinweise

Wenn Anhänge ins Web Portal hochgeladen werden, kann ein Hinweis zu E-Mails hinzugefügt werden.

☐ Füge einen Hinweis zu eingehenden Nachrichten hinzu

Text

☐ Füge einen Hinweis zu ausgehenden Nachrichten hinzu

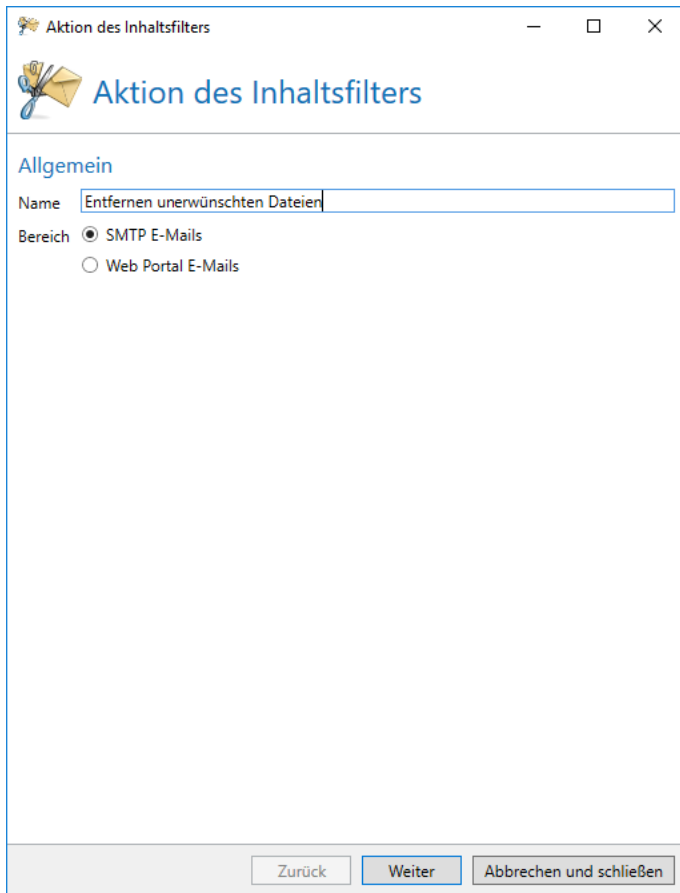
Text

Speichern und schließen Abbrechen und schließen

Bild 134: Der Text für Hinweise über hochgeladene Anhänge

Aktionen des Inhaltsfilters

Die Aktionen für den Inhaltsfilter werden zentral konfiguriert und mit sprechenden Namen belegt, damit man die selben Konfigurationen in mehreren Inhaltsfiltereinträgen nutzen kann, ohne diese doppelt erstellen zu müssen. Bei einem neuen Inhaltsfilter muss zuerst der Typ angegeben werden, da sich die Möglichkeiten für die Bearbeitung von Anhängen auf E-Mails für das Web Portal und bei SMTP-E-Mails unterscheiden ([Bild 135](#)).



Aktion des Inhaltsfilters

Aktion des Inhaltsfilters

Allgemein

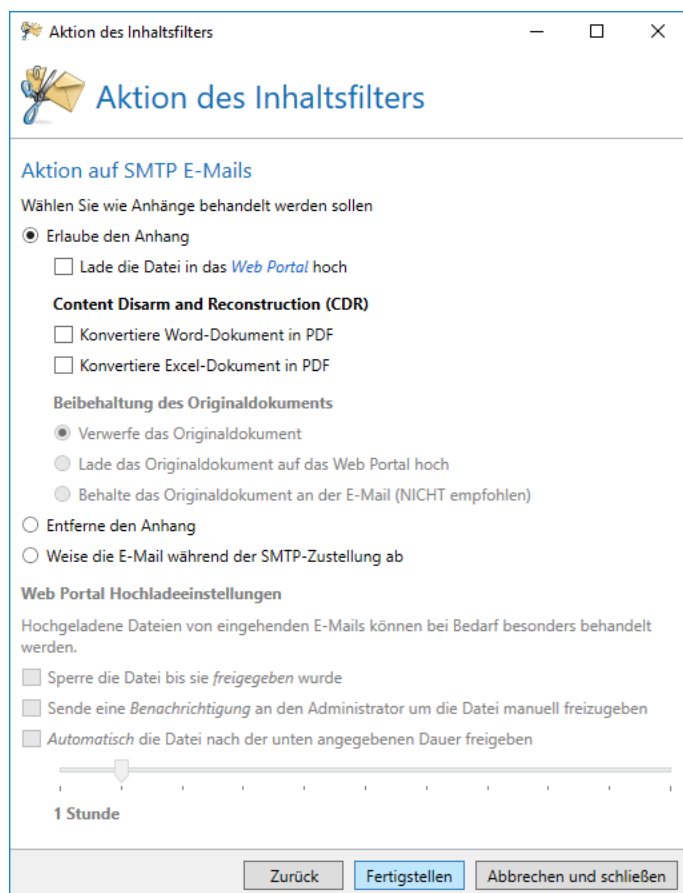
Name:

Bereich: ☒ SMTP E-Mails ☐ Web Portal E-Mails

Zurück Weiter Abbrechen und schließen

Bild 135: Der Typ der Aktion

Bei SMTP-E-Mails wählen Sie erst einmal das grundsätzliche Verhalten, wie **Erlaube den Anhang**, **Entferne den Anhang** und **Weise die E-Mail während der SMTP-Zustellung ab** aus. Beim Erlauben von Anhängen stehen Ihnen hier die Optionen für das Hochladen von Anhängen auf das Web Portal, konvertieren von Word- und Excel-Dokumenten in PDF, sowie das Verfahren mit dem Originaldokument nach einer Konvertierung in PDF zur Verfügung ([Bild 136](#)). Wenn Ihre Auswahl in diesem Dialog das Web Portal für Large Files nutzt, können Sie die Behandlung des Anhangs in den Large Files im Abschnitt **Web Portal Hochladeeinstellungen** gesondert einstellen.



The screenshot shows a window titled 'Aktion des Inhaltsfilters' with a standard Windows title bar. Inside, there's a sub-header 'Aktion auf SMTP E-Mails'. Below this, a text prompt asks to choose how attachments should be handled. Three radio buttons are present: 'Erlaube den Anhang' (selected), 'Entferne den Anhang', and 'Weise die E-Mail während der SMTP-Zustellung ab'. Under 'Erlaube den Anhang', there's a checkbox for 'Lade die Datei in das Web Portal hoch'. A section titled 'Content Disarm and Reconstruction (CDR)' contains two checkboxes for converting Word and Excel documents to PDF. Another section, 'Beibehaltung des Originaldokuments', has three radio buttons: 'Verwerfe das Originaldokument' (selected), 'Lade das Originaldokument auf das Web Portal hoch', and 'Behalte das Originaldokument an der E-Mail (NICHT empfohlen)'. The 'Web Portal Hochladeeinstellungen' section includes three checkboxes for file handling and a slider for automatic release duration, currently set to '1 Stunde'. At the bottom are three buttons: 'Zurück', 'Fertigstellen', and 'Abbrechen und schließen'.

Aktion des Inhaltsfilters

Aktion auf SMTP E-Mails

Wählen Sie wie Anhänge behandelt werden sollen

☒ Erlaube den Anhang

☐ Lade die Datei in das *Web Portal* hoch

Content Disarm and Reconstruction (CDR)

☐ Konvertiere Word-Dokument in PDF

☐ Konvertiere Excel-Dokument in PDF

Beibehaltung des Originaldokuments

☒ Verwerfe das Originaldokument

☐ Lade das Originaldokument auf das Web Portal hoch

☐ Behalte das Originaldokument an der E-Mail (NICHT empfohlen)

☐ Entferne den Anhang

☐ Weise die E-Mail während der SMTP-Zustellung ab

Web Portal Hochladeeinstellungen

Hochgeladene Dateien von eingehenden E-Mails können bei Bedarf besonders behandelt werden.

☐ Sperre die Datei bis sie freigegeben wurde

☐ Sende eine *Benachrichtigung* an den Administrator um die Datei manuell freizugeben

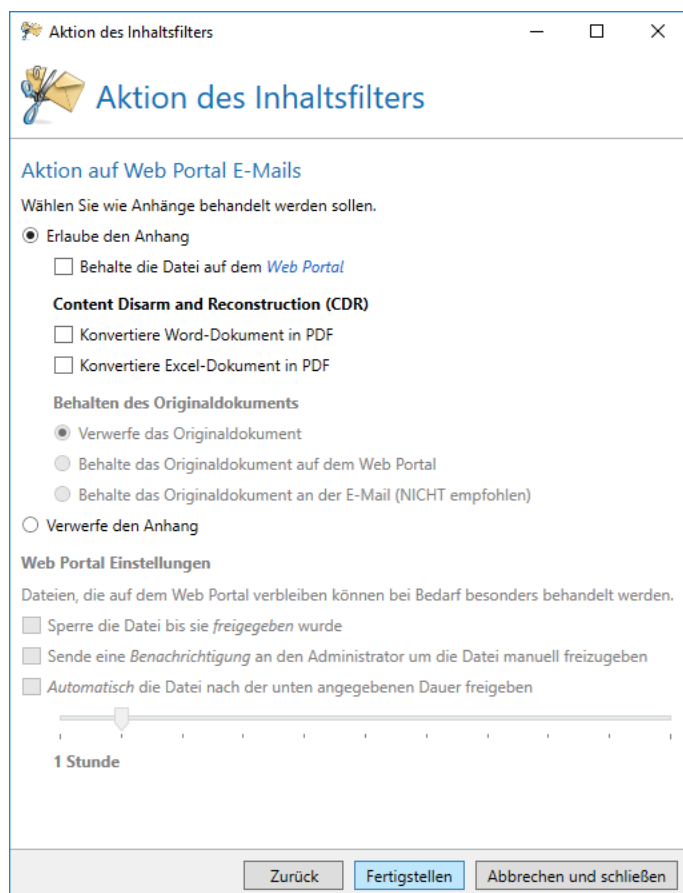
☐ Automatisch die Datei nach der unten angegebenen Dauer freigegeben

1 Stunde

Zurück Fertigstellen Abbrechen und schließen

Bild 136: Aktionen auf SMTP-E-Mails

Die **Aktion auf Web Portal E-Mails** wird analog zu einer **Aktion auf SMTP-E-Mails** konfiguriert. ([Bild 137](#))



Aktion des Inhaltsfilters

Aktion auf Web Portal E-Mails

Wählen Sie wie Anhänge behandelt werden sollen.

☒ Erlaube den Anhang

☐ Behalte die Datei auf dem [Web Portal](#)

Content Disarm and Reconstruction (CDR)

☐ Konvertiere Word-Dokument in PDF

☐ Konvertiere Excel-Dokument in PDF

Behalten des Originaldokuments

☒ Verwerfe das Originaldokument

☐ Behalte das Originaldokument auf dem Web Portal

☐ Behalte das Originaldokument an der E-Mail (NICHT empfohlen)

☐ Verwerfe den Anhang

Web Portal Einstellungen

Dateien, die auf dem Web Portal verbleiben können bei Bedarf besonders behandelt werden.

☐ Sperre die Datei bis sie freigegeben wurde

☐ Sende eine *Benachrichtigung* an den Administrator um die Datei manuell freizugeben

☐ Automatisch die Datei nach der unten angegebenen Dauer freigeben

1 Stunde

Zurück Fertigstellen Abbrechen und schließen

Bild 137: Aktion auf Web Portal E-Mails

NoSpamProxy Komponenten

Unter dem Menüpunkt **NoSpamProxy Komponenten** werden die Verbindungen zwischen den einzelnen Komponenten von NoSpamProxy konfiguriert ([Bild 138](#)).

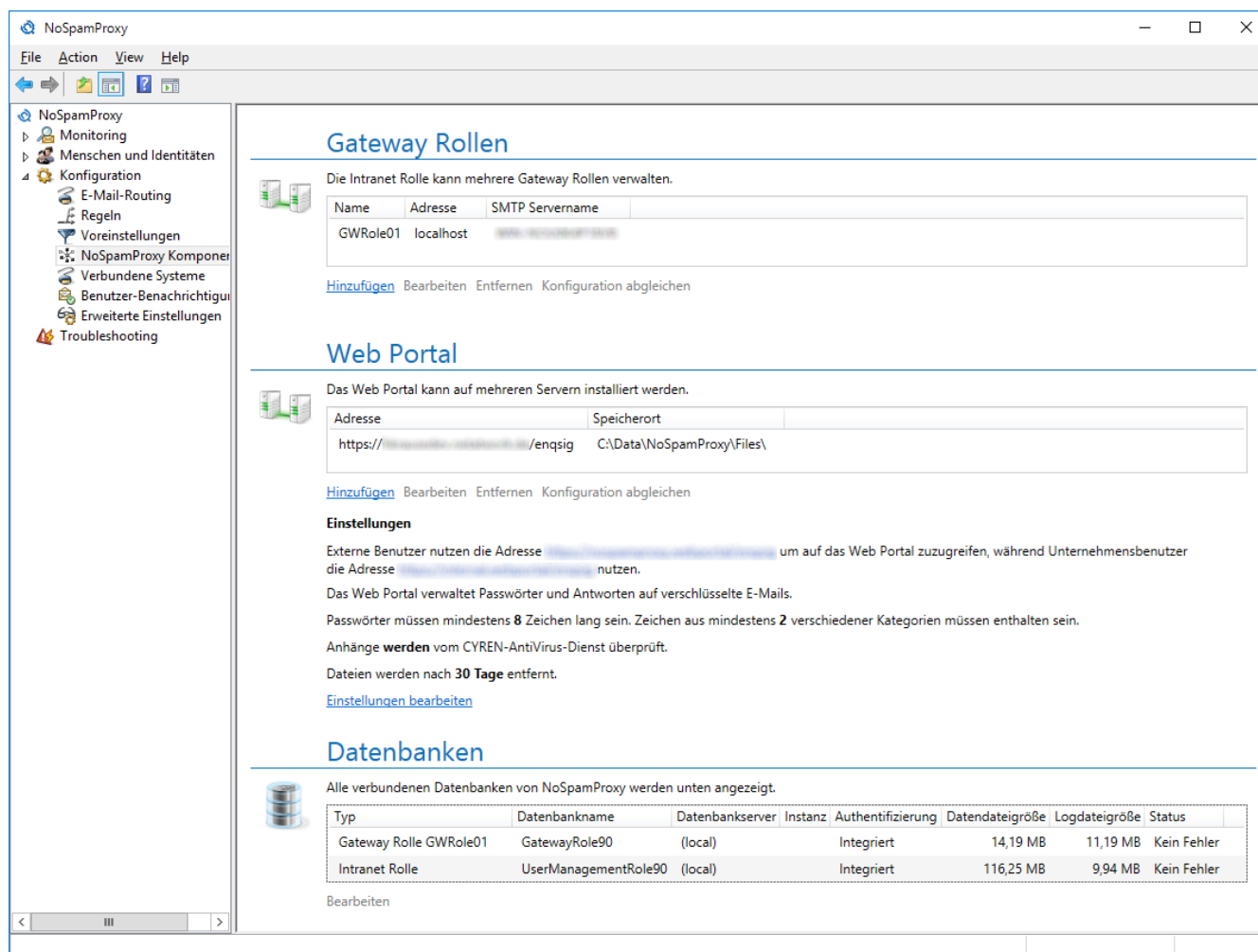


Bild 138: Die Verbindungen zu einzelnen Komponenten von NoSpamProxy

Gateway Rollen

Die Gateway Rolle kann entweder auf demselben Server wie die Intranet Rolle installiert werden oder aber auf einem anderen Server. Falls Sie mehr als eine Gateway Rolle betreiben, können Sie diese zusätzlich lizenzieren. Die Installation der ersten Gateway Rolle ist in jeder Lizenz bereits erlaubt. Sprechen Sie uns zum Thema Hochverfügbarkeit mit mehreren Gateway Rollen unter info@netatwork.de an.



Für Hochverfügbarkeit können Sie mehrere Rollen in Ihrem Unternehmen betreiben. Eine Übersicht steht in [Die Rollen von NoSpamProxy](#). Beispiele werden in [Funktionsweise und Einbindung in die Infrastruktur](#) erläutert.



Die Konfiguration wird von der Intranet Rolle zu allen verbundenen Gateway Rollen übertragen. Falls Sie in Ihrem Unternehmen eine DMZ betreiben, sollten Sie die Gateway Rollen dort, die Intranet Rolle aber im internen Netz installieren. In Ihrer Firewall brauchen Sie dann nur die Verbindung vom internen Netz zur DMZ für den TCP-Ports 6060 und den HTTPS-Port 6061 freischalten.

Es kann in Ausnahmefällen dazu kommen, dass die Konfiguration einer Gateway Rolle von der der Intranet Rolle abweicht. Für diesen Fall können Sie über die Schaltfläche **Konfiguration abgleichen** die Intranet Rolle dazu veranlassen, die Konfiguration mit den markierten Rollen zu synchronisieren.

Server-Identität

Bei einer Verbindung zu externen Servern stellt sich der Client mit dem HELO oder EHLO Kommando gefolgt vom Servernamen beim empfangenen Server vor. Ein mögliches Beispiel:

```
EHLO mail.netatwork.de
```

Einige Server überprüfen, ob dieser Name per DNS auflösbar ist. Die Auflösbarkeit dieses Namens ist in einer RFC vorgeschrieben. Sollte der Name nicht auflösbar sein, wird das von einigen anderen Mail Servern als Spam-Merkmal bewertet. Hier sollte der im Internet auflösbare FQDN eingetragen werden. Üblicherweise wird hier der MX der eigenen E-Mail-Domäne eingetragen.

Um die genannte Einstellung zu ändern, klicken Sie im Bereich **Server-Identität** auf **Ändern**. Es erscheint der Dialog zum Ändern der Identität ([Bild 139](#)).

Gateway Rolle

Gateway Rolle auf dem Server localhost

Name

Der SMTP Servername sollte mit Ihrem MX-Eintrag übereinstimmen.

SMTP Servername

[Finde die DNS-Einstellungen heraus](#)

Bild 139: Die Server-Identität sollte dem "MX" Eintrag in Ihrem DNS entsprechen

Im Feld **Name** geben Sie dann den zu verwendenden Namen an.

Sie können auch den DNS Namen für Ihre Domäne automatisch auflösen lassen. Dazu wird die primäre Domäne Ihrer Lizenz benutzt. Für die automatische Auflösung drücken Sie die Schaltfläche **Finde die DNS-Einstellungen heraus**. Es erscheint ein Dialog, der alle zur Verfügung stehenden DNS Identitäten für Ihre Domäne, nach der Priorität geordnet, auflistet.

Verbindung zu einer Gateway Rolle herstellen

Im Dialog für die Verbindung zu einer Gateway Rolle wählen Sie die Option **Die Rolle und die Gateway Rolle laufen beide auf demselben Server**, wenn Sie die zu verbindenden Rollen auf dem gleichen Server installiert haben. Ist die Gateway Rolle auf einem anderen Server installiert, wählen Sie zunächst die Option **Die Rolle und die Gateway Rolle laufen auf unterschiedlichen Servern...** Geben Sie dann unter **Servername** und **Port** den Namen der Gateway Rolle an, unter dem die aktuelle Rolle die Gateway Rolle erreichen kann. Wenn die Management Rolle sich zur Gateway Rolle mit denselben Daten verbinden kann, wählen Sie die Option **Die Management Konsole kann sich zur Gateway Rolle mit dem oben angegebenen Servernamen und Port verbinden**. Ansonsten wählen Sie **Die Management Konsole kann sich zur Gateway Rolle mit dem unten angegebenen Servernamen und Port verbinden** und geben Sie dann die Daten in das Feld **Servername** und **Port** ein. Standardmäßig ist der Port 6060.

Web Portal

Um das Web Portal verwenden zu können, müssen Sie zunächst eine Verbindung zwischen Intranet Rolle und Web Portal herstellen. Anschließend können Sie die einzelnen Features konfigurieren.



Für Hochverfügbarkeit können Sie mehrere Web Portale in Ihrem Unternehmen betreiben. Ein Übersicht steht in [Die Rollen von NoSpamProxy](#). Beispiele werden in [Funktionsweise und Einbindung in die Infrastruktur](#) erläutert.



Das Web Portal steht Ihnen nur zu Verfügung, wenn Sie die Large Files oder Encryption lizenziert haben.

Web Portal Verbindungen

Im Dialog für eine Verbindung zum Web Portal ([Bild 140](#)) geben Sie unter **Adresse** die HTTPS-Adresse des Web Portals, zum Beispiel: `https://portal.example.com/` oder `https://portal.example.com:1234/` für eine Verbindung über den Port '1234', unter dem die Intranet Rolle das Web Portal erreichen kann. Wenn die Management Rolle sich zur Gateway Rolle nicht mit denselben Daten verbinden kann, wählen Sie die Option **Die Management Konsole benötigt andere Verbindungsinformationen, um sich zum Web Portal zu verbinden, als die Intranet Rolle** und geben Sie die HTTPS-Adresse in das Feld **Adresse** ein, unter der die Management Konsole das Web Portal erreichen kann. Standardmäßig ist das der Port 443.

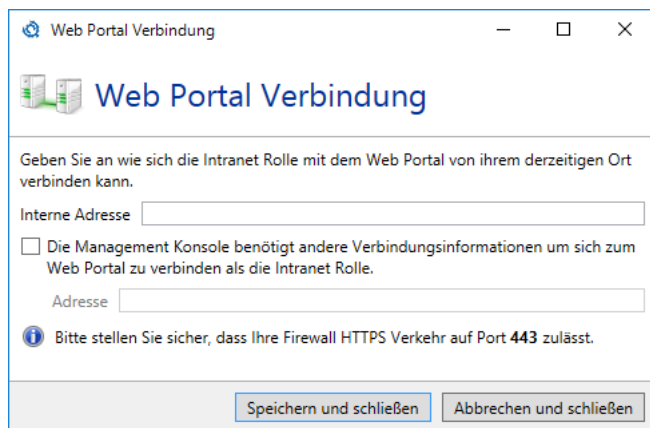


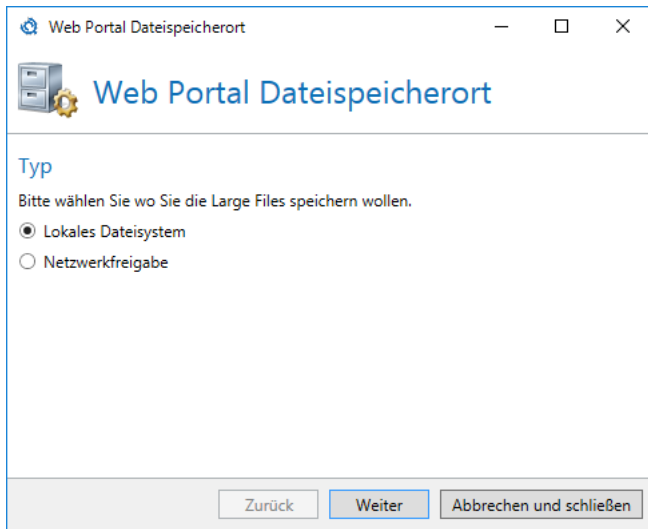
Bild 140: Die Einstellungen für eine Verbindung zu einem Web Portal



Es kann in Ausnahmefällen dazu kommen, dass die Konfiguration eines Web Portals von der der Intranet Rolle abweicht. Für diesen Fall können Sie über die Schaltfläche **Konfiguration abgleichen** die Intranet Rolle dazu veranlassen, die Konfiguration mit den markierten Web Portalen zu synchronisieren .

Sie können den Dateispeicherort der 'Large Files' nach der Einrichtung der Verbindung anpassen. Dabei stehen Ihnen die folgenden Orte zur Verfügung ([Bild 142](#)):

- **Lokales Dateisystem**
Geben Sie einen Pfad auf einem lokalen Speicher an, für den die im Dialog angegebenen Konten die entsprechenden Rechte haben.
- **Netzwerkfreigabe**
Geben Sie hier den Pfad zur Netzwerkfreigabe an. Wählen Sie, ob Sie auf die Freigabe durch das Computerkonto des Server zugreifen oder ob dafür ein bestimmtes Benutzerkonto zum Einsatz kommt ([Bild 141](#)).
- **Microsoft Azure BLOB Storage**
Durch die Angabe eines Azure Kontonamen und des dazugehörigen Kontoschlüssels werden alle Dateien im dazugehörigen Azure BLOB Storage gespeichert.



Web Portal Dateispeicherort

Web Portal Dateispeicherort

Typ

Bitte wählen Sie wo Sie die Large Files speichern wollen.

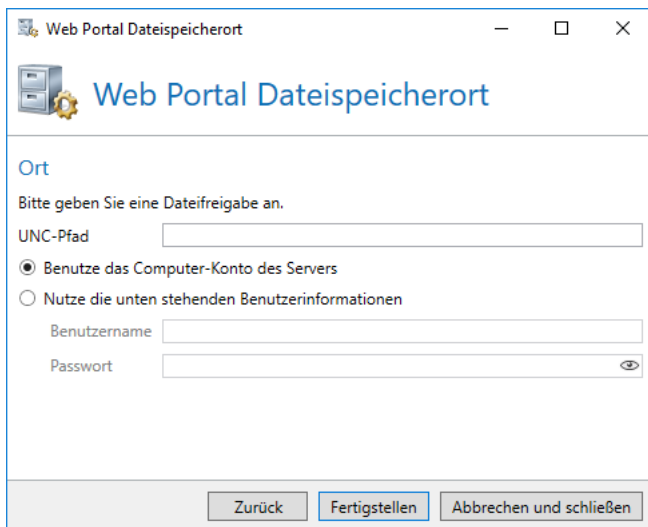
☒ Lokales Dateisystem

☐ Netzwerkfreigabe

Zurück Weiter Abbrechen und schließen

Bild 141: Speicherorte für die 'Large Files'

Je nach ausgewähltem Speicherort müssen Sie Speicherort und/oder Benutzerinformationen eingeben ([Bild 142](#)).



Web Portal Dateispeicherort

Web Portal Dateispeicherort

Ort

Bitte geben Sie eine Dateifreigabe an.

UNC-Pfad

☒ Benutze das Computer-Konto des Servers

☐ Nutze die unten stehenden Benutzerinformationen

Benutzername

Passwort

Zurück Fertigstellen Abbrechen und schließen

Bild 142: Die Verbindung zum Dateispeicherort des Web Portal am Beispiel der Netzwerkfreigabe

Web Portal - Einstellungen

Bei Benutzung des Web Portals wird in E-Mails ggf. ein Link auf dasselbe eingefügt. Der Link beinhaltet dabei die Adresse unter der das Web Portal aus dem Internet erreichbar ist ([Bild 143](#)). Falls Sie für den Zugriff aus dem Firmennetzwerk eine andere Adresse verwenden, können Sie diese in dem Feld **Interne Https-Adresse** eintragen.

Den Abschnitt **Sichere Web Mails** können Sie so konfigurieren, dass das Web Portal über die dort eingeblendete Adresse auch ohne Einladungslink verwendet werden kann. Bei dieser Verwendung kann ein externer Partner über das Web Portal eine E-Mail an Empfänger in Ihrem Unternehmen senden. Dazu muss er eine Absenderadresse und eine gültige Empfängeradresse eines in NoSpamProxy hinterlegten Unternehmensbenutzers eintragen. Falls in NoSpamProxy keine Unternehmensbenutzer hinterlegt sind, wird bei der Empfängeradresse mindestens die Domäne daraufhin validiert, ob sie in der Liste der eigenen Domänen vorhanden ist.

The screenshot shows a window titled 'Web Portal Einstellungen' with a standard Windows title bar. Inside, there's a sub-header 'Web Portal Einstellungen' with a small icon. Below it are three tabs: 'Allgemein' (selected), 'PDF Mail', and 'Large Files'. A text line states: 'Die Adresse des Web Portals wird bei externen E-Mail-Empfängern genutzt.' Under the heading 'Adressen des Portals', there are two text input fields. The first is labeled 'Externe HTTPS-Adresse' and contains 'https://.../enQsig'. Below it is a checked checkbox labeled 'Benutze eine andere Adresse für Zugriffe von innerhalb Ihres Unternehmens'. The second text input field is labeled 'Interne HTTPS-Adresse' and also contains 'https://.../enQsig'. Under the heading 'Sichere Web Mails', there is an unchecked checkbox labeled 'Erlaube sichere Web Mails ohne Einladungslink'. Below this checkbox is a note: 'Die Adresse https://webportal.mailgateway.test/enQsig/mail/new kann durch Ihre Partner genutzt werden.' At the bottom of the dialog are two buttons: 'Speichern und schließen' and 'Abbrechen und schließen'.

Bild 143: Allgemeine Einstellungen

Wenn Sie Large Files aktivieren, müssen Sie auf der nächsten Seite noch einige weitere Einstellungen vornehmen ([Bild 144](#)). Um die Kommunikation zwischen dem Outlook Add-In und dem Web Portal abzusichern, ist ein **gemeinsames Passwort** ("Shared Secret") notwendig. Geben Sie ein Kennwort ein, das mindestens 12 Zeichen lang ist.

Die vom Web Portal gespeicherten 'Large Files'-Dateien sind vollständig verschlüsselt. Dabei steht der Entschlüsselungsschlüssel nur dem Empfänger zur Verfügung, dadurch haben Administratoren des Servers keinen Zugriff auf die Dateien. Wenn Sie Dateien, die auf die Genehmigung warten, vor der Genehmigung überprüfen wollen, müssen Sie das über die Option **Erlaube Mitgliedern der 'Monitoring Administrators'-Gruppe Dateien, die auf Genehmigung warten, herunterzuladen und zu untersuchen** explizit erlauben. Nachdem die Datei im Knoten 'Large Files' genehmigt wurde, ist kein weiterer Zugriff durch die 'Monitoring Administrators'-Gruppe möglich.

Mit NoSpamProxy Protection können alle 'Large Files'-Dateien mit dem **Cyren-AntiVirus-Dienst** überprüft werden.

Die 'Large Files'-Dateien werden nach Ablauf der **Aufbewahrungsdauer** vom Web Portal entfernt und stehen dann nicht mehr zum Herunterladen zur Verfügung.

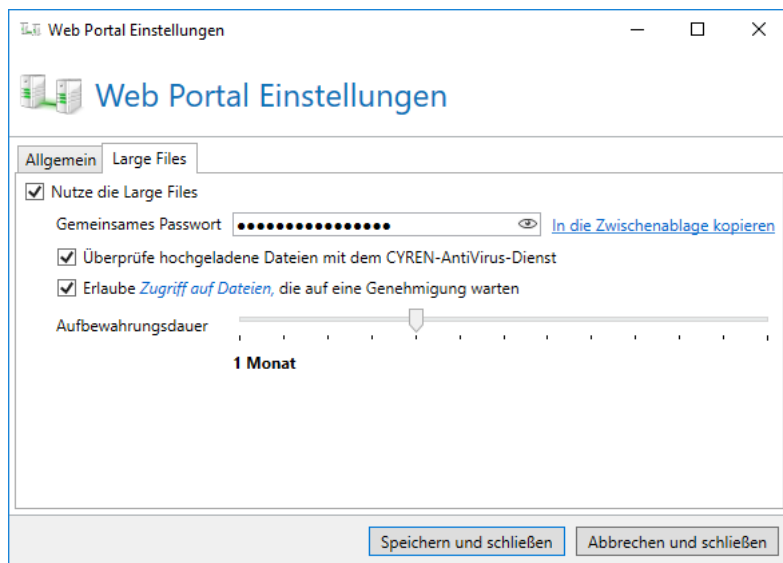


Bild 144: Einstellungen für Large Files

Datenbanken

Im Bereich der **Datenbankkonfiguration** können Sie die Verbindung zur Datenbank der entsprechenden Rolle ändern. Die Datenbank wird während des Setups eingerichtet. Änderungen müssen nur im Falle eines Umzugs der Datenbank auf einen anderen SQL-Server vorgenommen werden. In einem solchen Fall sollten Sie die bestehende Datenbank auf dem bisherigen SQL Server sichern und diese Sicherung auf dem neuen Datenbank Server einspielen. Stellen Sie nun die Verbindung auf den neuen Datenbank Server mit **Datenbankkonfiguration ändern** um ([Bild 145](#)).



Jede Datenbank der Rollen ist eigenständig und darf nicht zwischen den Rollen geteilt werden. Das heißt, dass Sie bei zwei Gateway Rollen auch zwei Datenbanken erstellen. Diese dürfen sich sowohl einen Server als auch eine Instanz teilen, sind ansonsten aber voneinander unabhängig. Unabhängige Datenbanken erhöhen die Stabilität von NoSpamProxy und erleichtern administrative Aufgaben, wie Upgrades oder Datenbankumzüge.

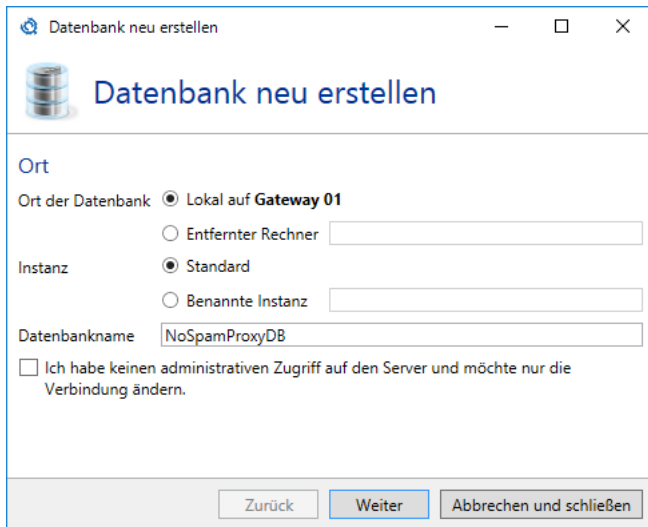


Bild 145: Die Verbindung zur Datenbank der entsprechenden Rolle

Mit der Einstellung **Ort der Datenbank** bestimmen Sie, auf welchem Server sich die Datenbank befindet. Wenn sich die Datenbank auf demselben Server wie die Gateway Rolle befindet, wählen Sie **Lokaler Server**. Ist die Datenbank auf einem anderen Server eingerichtet, wählen Sie zunächst die Option **Entfernter Rechner** und geben dann im Eingabefeld entweder die IP-Adresse oder den voll qualifizierten Domännennamen (FQDN) des Servers ein, auf dem sich die Datenbank befindet.

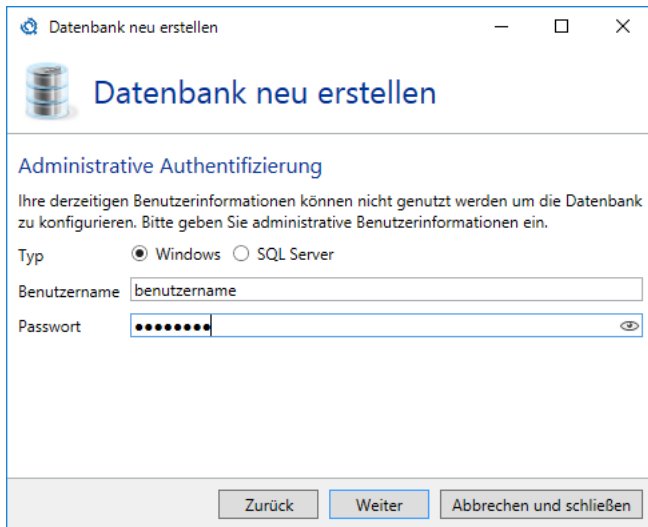
Ob es sich bei der Instanz, in der die Datenbank der Gateway Rolle liegt, um die Standardinstanz des SQL-Servers oder um eine benannte Instanz handelt, geben Sie mit **Datenbank Instanz** an. Wenn es sich um die Standardinstanz des SQL-Servers handelt, wählen Sie die Option **Standard**. Anderenfalls klicken Sie auf **Benannte Instanz** und tragen anschließend im Eingabefeld den Namen der entsprechenden Instanz ein.

In dem Feld **Datenbankname** bzw. den Feldern, wenn mehrere Datenbanken für die Rolle benötigt werden, tragen Sie den Namen der entsprechenden Datenbank ein. Die folgenden Datenbanknamen werden standardmäßig verwendet.

- **Gateway Rolle**
NoSpamProxyDb
- **Intranet Rolle**
NoSpamProxyAddressSynchronization

Wenn Sie lediglich die Verbindungsparameter ändern möchten, markieren Sie das entsprechende Feld im unteren Bereich des Dialogs.

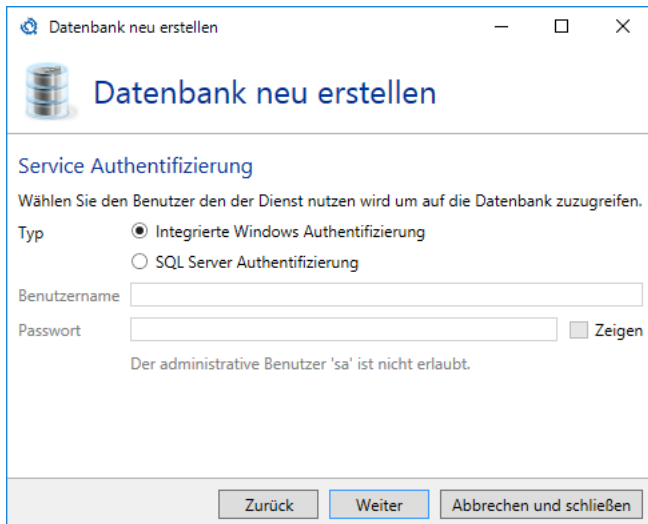
Die Einstellung **Administrative Authentifizierung** ([Bild 146](#)) legt fest, mit welchem Benutzerkonto Änderungen an der gewählten Datenbank durchgeführt werden sollen. Wählen Sie die Einstellung **Windows**, wenn Sie ein Windows-Benutzerkonto verwenden möchten. Andernfalls wählen Sie die Option **SQL Server** und tragen anschließend in den Feldern **Benutzername** und **Passwort** die entsprechenden Anmeldedaten ein.



The screenshot shows a Windows dialog box titled 'Datenbank neu erstellen' (Create New Database). The main heading is 'Datenbank neu erstellen'. Below it, the section is 'Administrative Authentifizierung' (Administrative Authentication). The text says: 'Ihre derzeitigen Benutzerinformationen können nicht genutzt werden um die Datenbank zu konfigurieren. Bitte geben Sie administrative Benutzerinformationen ein.' (Your current user information cannot be used to configure the database. Please enter administrative user information). There are two radio buttons for 'Typ' (Type): 'Windows' (selected) and 'SQL Server'. Below are input fields for 'Benutzername' (Username) containing 'benutzername' and 'Passwort' (Password) with masked characters. At the bottom are three buttons: 'Zurück' (Back), 'Weiter' (Next), and 'Abbrechen und schließen' (Cancel and Close).

Bild 146: Die Verbindung zur Datenbank der entsprechenden Rolle

Die Einstellung **Service Authentifizierung** ([Bild 147](#)) legt fest, wie sich die Gateway Rolle beim SQL Server anmelden soll. Ist auf dem SQL-Server die SQL-Authentifizierung abgeschaltet, dann muss die integrierte Authentifizierung verwendet werden. Ansonsten können Sie hier zwischen Integrierter und SQL-Authentifizierung wählen. ([Bild 148](#)).



The screenshot shows the same 'Datenbank neu erstellen' dialog box, but the section is 'Service Authentifizierung' (Service Authentication). The text says: 'Wählen Sie den Benutzer den der Dienst nutzen wird um auf die Datenbank zuzugreifen.' (Select the user the service will use to access the database). There are two radio buttons for 'Typ' (Type): 'Integrierte Windows Authentifizierung' (selected) and 'SQL Server Authentifizierung'. Below are input fields for 'Benutzername' (Username) and 'Passwort' (Password). There is a 'Zeigen' (Show) checkbox next to the password field. Below the password field, it says: 'Der administrative Benutzer 'sa' ist nicht erlaubt.' (The administrative user 'sa' is not allowed). At the bottom are three buttons: 'Zurück' (Back), 'Weiter' (Next), and 'Abbrechen und schließen' (Cancel and Close).

Bild 147: Dienstanbindung an die Datenbank.

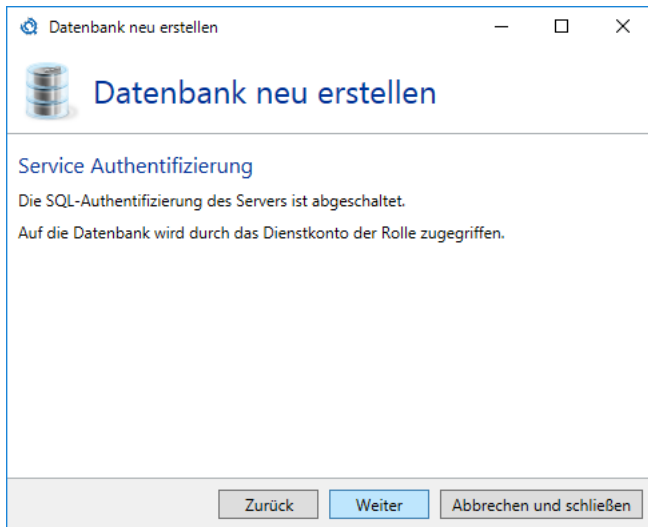


Bild 148: Keine SQL-Authentifizierung verfügbar.

Auf der Seite **Was soll getan werden** wählen Sie nun die gewünschte Aktion aus. Je nachdem, was NoSpamProxy für eine Datenbank gefunden hat, stehen hier andere Möglichkeiten zur Verfügung. Wählen Sie die gewünschte Aktion aus und klicken Sie auf **Fertigstellen** ([Bild 149](#)).

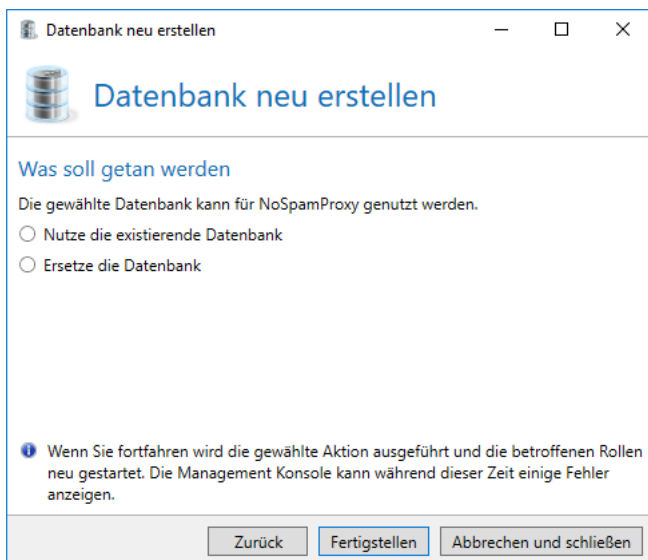


Bild 149: Wählen Sie ob die alte Datenbank gelöscht oder erhalten werden soll

Verbundene Systeme

Der Knoten **verbundenen Systeme** beinhaltet Verbindungen zu Drittanbieterprodukten, die mit NoSpamProxy interagieren.

DNS-Server

Beim Einsatz von DANE benötigen Sie einen DNS-Server der DNSSEC unterstützt. Da derzeit die in Windows-Server-Betriebssystemen mitgelieferten DNS-Server diese Funktion nicht unterstützen, können Sie hier eine Verbindung zu einem solchen Server einrichten ([Bild 150](#)).

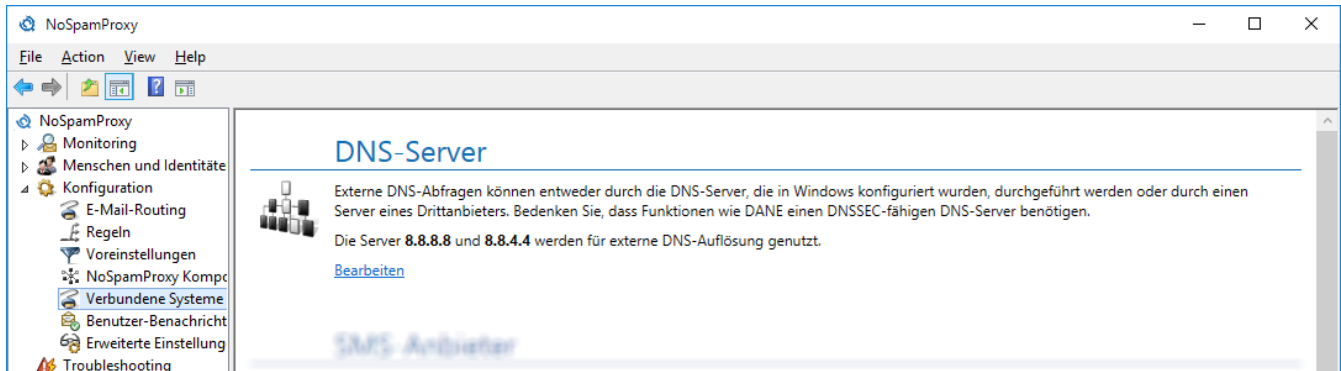


Bild 150: Anbindung an einen DNSSEC fähigen Server

Der Konfigurationsdialog bietet die Möglichkeit, IP-Adressen eines primären und sekundären Servers mit DNSSEC-Unterstützung einzutragen. Mit Hilfe von **Nutze Google** können Sie den öffentlich erreichbaren DNS-Server von Google in die Konfiguration eintragen lassen ([Bild 151](#)).

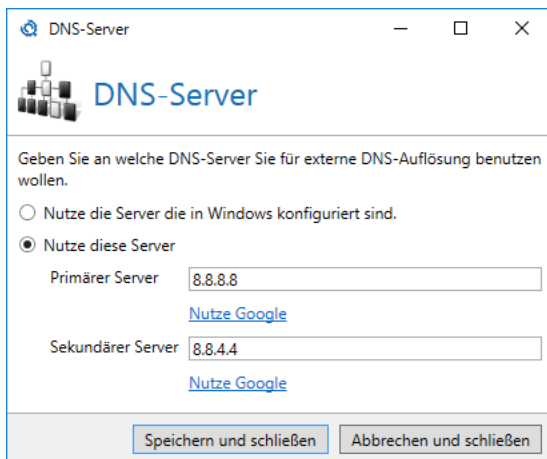


Bild 151: Konfiguration eines DNSSEC fähigen Server



DANE wird für die Überprüfung der Transportverschlüsselung bei der Zustellung von E-Mails zu Ihren Partnern verwendet. Diese konfigurieren Sie in den [Standardeinstellungen für Partner](#).

Archivschnittstelle

Über die Archivschnittstelle können E-Mails und qualifiziert signierte Dokumente an ein externes Archivsystem übergeben werden ([Bild 152](#)). Unterstützt werden derzeit das Dateisystem, ein Archivpostfach sowie d.velop d.3. Es können auch mehrere Archivsysteme parallel verwendet werden.

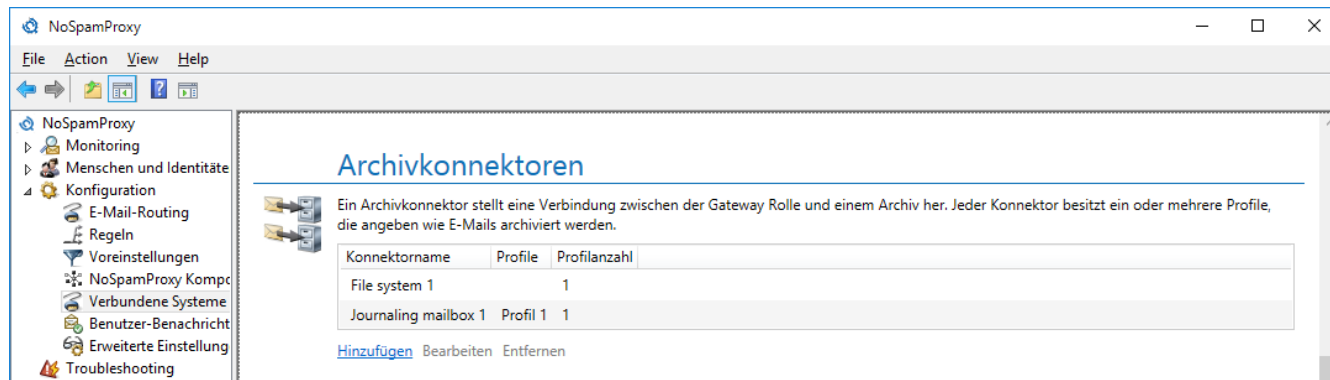
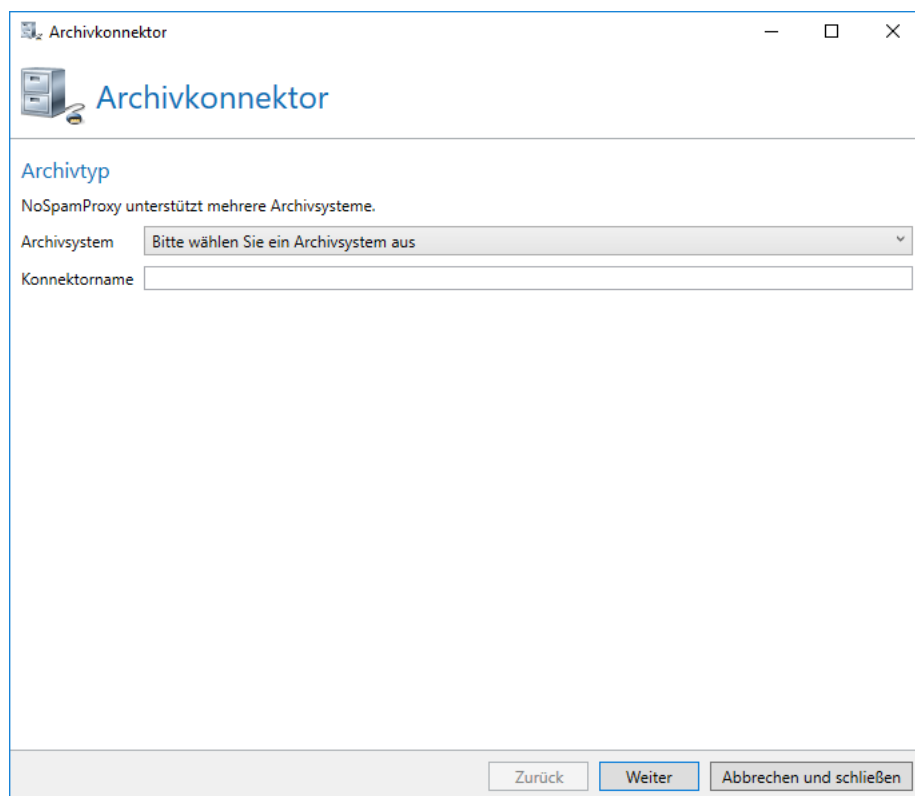


Bild 152: Die Liste der konfigurierten Archivschnittstellen

Die Konfiguration besteht aus zwei Teilen: den Archivkonnektoren und den Profilen. Konnektoren definieren die Schnittstelle zu einem externen Archivsystem, wie z.B. dem Dateisystem. Innerhalb eines Konnektors werden ein oder mehrere Profile erstellt. Darin können Eigenschaften wie z.B. der genaue Speicherort für E-Mails und Dokumente festgelegt werden. Außerdem wird hier ggf. eine Zuordnung von Metadaten von E-Mails auf Metadaten des Archivsystems durchgeführt.

Um einen neuen Konnektor zu erstellen, klicken Sie auf **Neuen Konnektor hinzufügen**. Hier wählen Sie zunächst den Konnektor-Typ aus und geben dem Konnektor einen neuen Namen ([Bild 153](#)).



The screenshot shows a Windows-style window titled "Archivkonnektor". Inside the window, there is a header section with a small icon of a server and the text "Archivkonnektor". Below this, the section "Archivtyp" is displayed. A note states: "NoSpamProxy unterstützt mehrere Archivsysteme." Below the note, there is a label "Archivsystem" followed by a dropdown menu with the text "Bitte wählen Sie ein Archivsystem aus". Below the dropdown, there is a label "Konnektorname" followed by a text input field. At the bottom of the window, there are three buttons: "Zurück", "Weiter", and "Abbrechen und schließen".

Bild 153: Allgemeine Einstellungen des Archivkonnektors

Die zu konfigurierenden Optionen im zweiten Schritt hängen davon ab, welches Archivsystem Sie im ersten Schritt gewählt haben.

Bei einer Ablage von E-Mails und Dokumenten im **Dateisystem**, ist nur ein Pfad anzugeben. E-Mails und Dokumente werden in Ordnern unterhalb dieses Pfades abgespeichert ([Bild 154](#)).

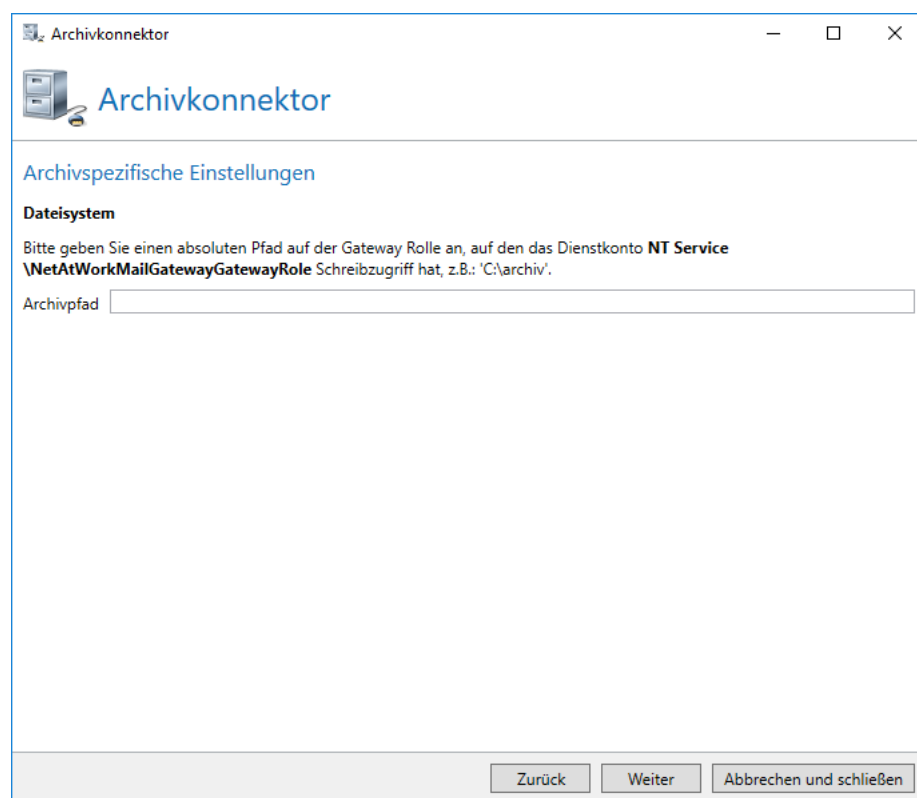


Bild 154: Eigenschaften für die Ablage im Dateisystem

Der Konnektor für das **Archivpostfach** besitzt keine weiteren Einstellungen auf dem Konnektor. Es werden direkt die Profile angezeigt.

Für einen Konnektor zu einem d.velop d.3 System ist lediglich ein Pfad anzugeben ([Bild 155](#)). E-Mails und Dokumente werden in dieses Verzeichnis geschrieben und von dort durch das d.velop d.3 System abgeholt.

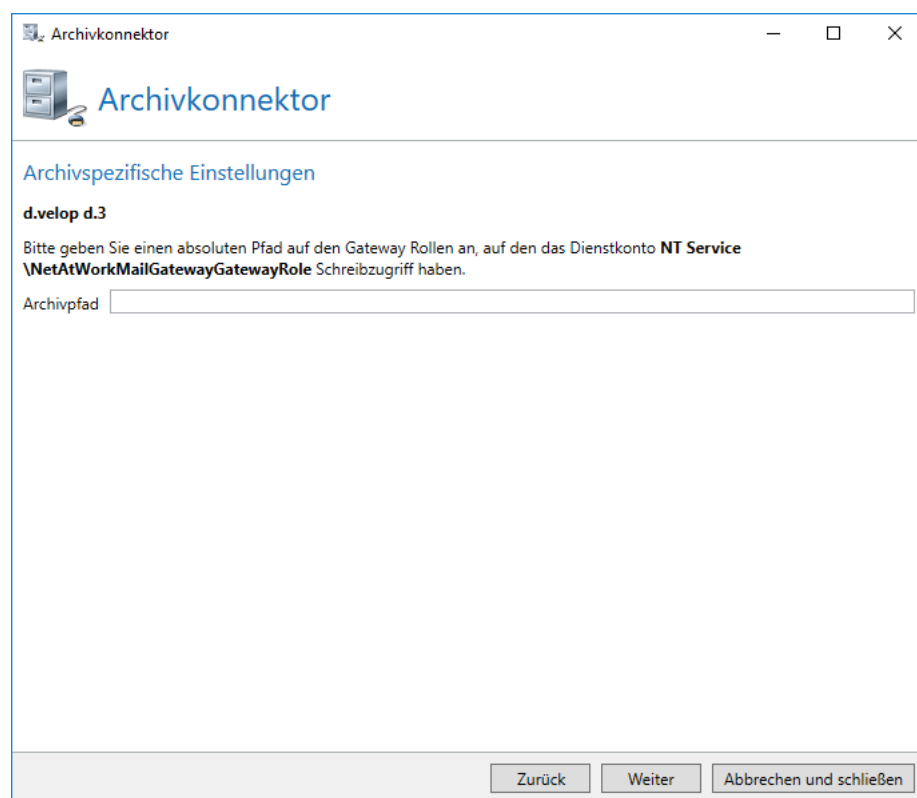
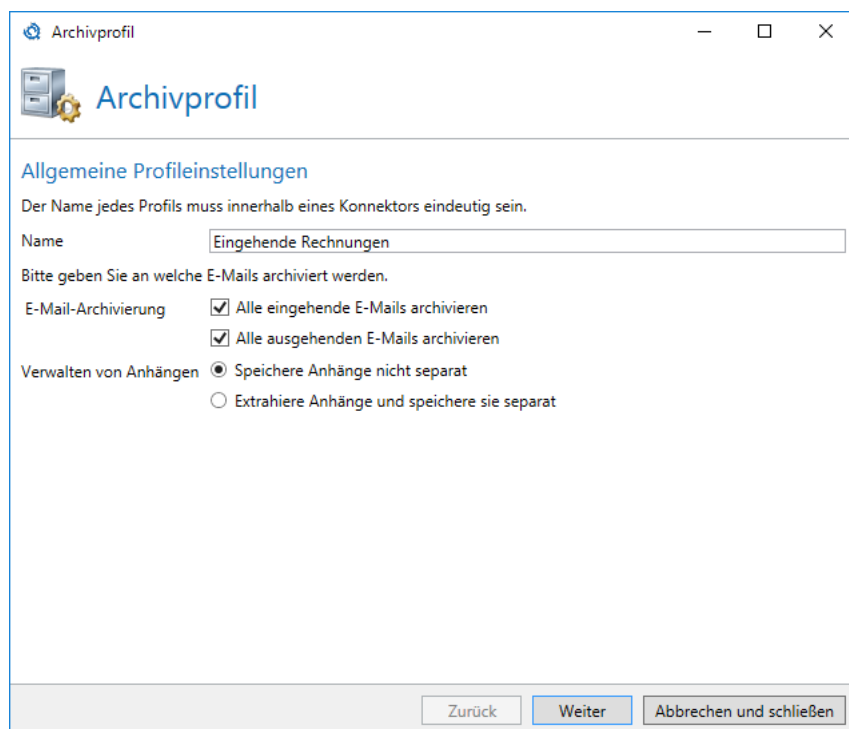


Bild 155: d.velop d.3-spezifische Eigenschaften

Auf der nächsten Seite können Sie Profile für diesen Konnektor anlegen. Profile ermöglichen es Ihnen zum Beispiel, E-Mails und Dokumente innerhalb eines Archivsystems auf verschiedene Ordner zu verteilen.

Einem neuen Profil müssen Sie zunächst einen Namen geben ([Bild 156](#)). Außerdem wählen Sie hier aus, welche E-Mails durch dieses Profil archiviert werden.



The screenshot shows a Windows-style window titled 'Archivprofil'. Inside, there's a header with a folder icon and the title 'Archivprofil'. Below this, the section 'Allgemeine Profileinstellungen' is displayed. A note states: 'Der Name jedes Profils muss innerhalb eines Konnektors eindeutig sein.' There is a text input field for 'Name' containing 'Eingehende Rechnungen'. Below this, a prompt says 'Bitte geben Sie an welche E-Mails archiviert werden.' Under 'E-Mail-Archivierung', there are two checked checkboxes: 'Alle eingehende E-Mails archivieren' and 'Alle ausgehenden E-Mails archivieren'. Under 'Verwalten von Anhängen', there are two radio buttons; 'Speichere Anhänge nicht separat' is selected, and 'Extrahiere Anhänge und speichere sie separat' is unselected. At the bottom, there are three buttons: 'Zurück', 'Weiter' (highlighted with a blue border), and 'Abbrechen und schließen'.

Archivprofil

Allgemeine Profileinstellungen

Der Name jedes Profils muss innerhalb eines Konnektors eindeutig sein.

Name

Bitte geben Sie an welche E-Mails archiviert werden.

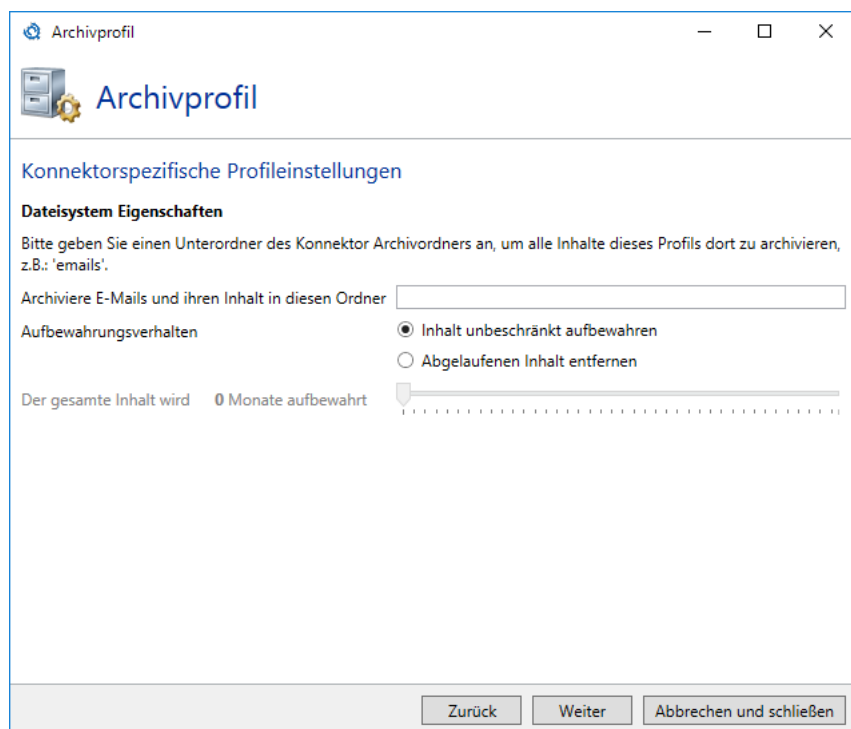
E-Mail-Archivierung ☒ Alle eingehende E-Mails archivieren
☒ Alle ausgehenden E-Mails archivieren

Verwalten von Anhängen ☒ Speichere Anhänge nicht separat
☐ Extrahiere Anhänge und speichere sie separat

Bild 156: Allgemeine Einstellungen des Profils

Der Inhalt der zweiten Seite hängt von dem gewählten Archivsystem ab.

Für die Speicherung im **Dateisystem** können Sie einen Unterordner für die E-Mails angeben, die durch dieses Profil gespeichert werden.



The screenshot shows a Windows-style window titled 'Archivprofil'. Inside, there's a header with a folder icon and the title 'Archivprofil'. Below this, the section 'Konnektorspezifische Profileinstellungen' is visible. Underneath, 'Dateisystem Eigenschaften' is highlighted. The text instructs the user to specify a subfolder for archiving. There is a text input field for 'Archiviere E-Mails und ihren Inhalt in diesen Ordner'. Below that, 'Aufbewahrungsverhalten' has two radio button options: 'Inhalt unbeschränkt aufbewahren' (selected) and 'Abgelaufenen Inhalt entfernen'. At the bottom left, it says 'Der gesamte Inhalt wird 0 Monate aufbewahrt' next to a slider control. At the bottom right, there are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

Archivprofil

Konnektorspezifische Profileinstellungen

Dateisystem Eigenschaften

Bitte geben Sie einen Unterordner des Konnektor Archivordners an, um alle Inhalte dieses Profils dort zu archivieren, z.B.: 'emails'.

Archiviere E-Mails und ihren Inhalt in diesen Ordner

Aufbewahrungsverhalten

☒ Inhalt unbeschränkt aufbewahren

☐ Abgelaufenen Inhalt entfernen

Der gesamte Inhalt wird 0 Monate aufbewahrt

Zurück Weiter Abbrechen und schließen

Bild 157: Eigenschaften für die Ablage im Dateisystem

Im Falle eines **Archivpostfachs** wird die E-Mail-Adresse des Zielpostfachs benötigt ([Bild 158](#)).

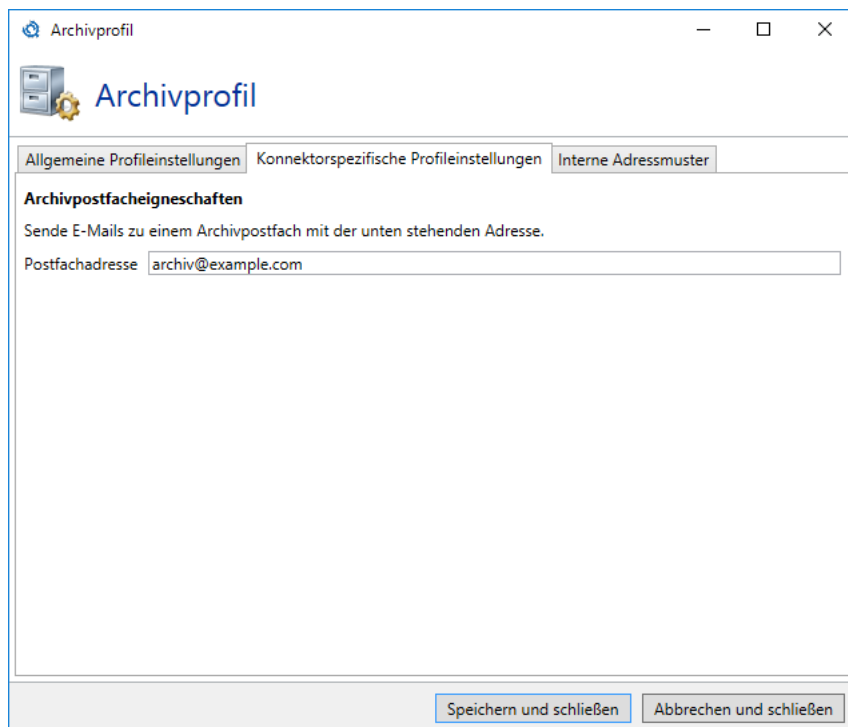


Bild 158: Eigenschaften für die Ablage in einem Archivpostfach

Bei einer Verbindung zu einem d.velop d.3 System ist keine weitere Konfiguration erforderlich. Der Dialog ist in diesem Fall leer ([Bild 159](#)).

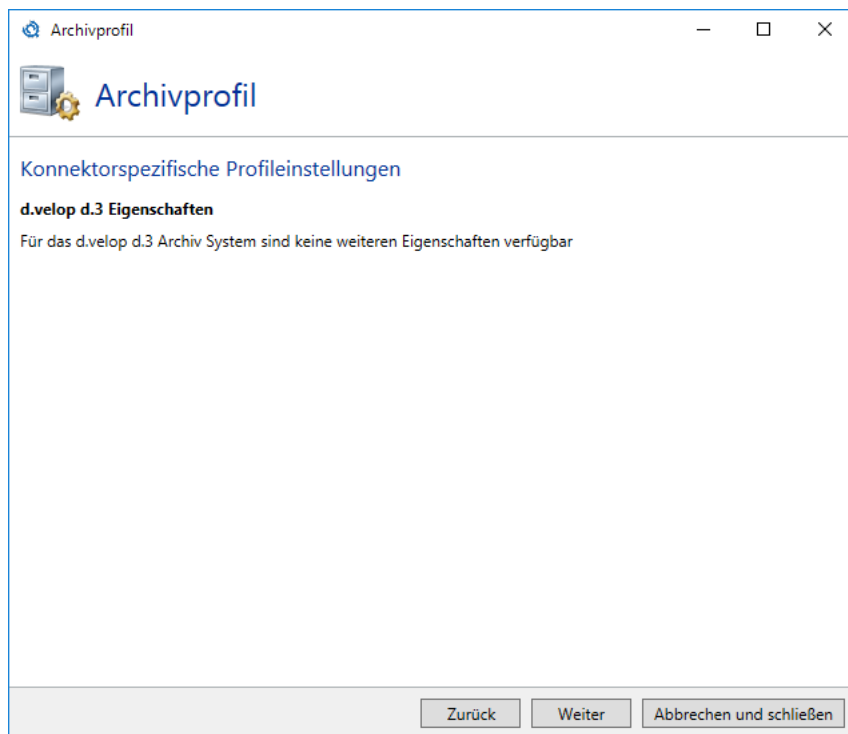


Bild 159: Eigenschaften für die Ablage in einem d.velop d.3 System

Im nächsten Schritt legen Sie fest, für welche lokalen E-Mailadressen dieses Profil zuständig ist. ([Bild 160](#)). Beim Versenden von E-Mails wird immer die Adresse des Absenders verwendet, um festzustellen, welche Profile für die Archivierung verwendet werden. Bei E-Mails an lokale Adressen werden die Adressen der Empfänger verwendet. Bei der Angabe der E-Mail-Adressen ([Bild 161](#)) können Sie auch Platzhalter ('*' und '?') verwenden, um mehrere Adressen anzugeben. Sollten bei einem Archivierungsvorgang mehrere Profile zu den hier angegebenen Daten passen, so wird die E-Mail mehrfach archiviert.

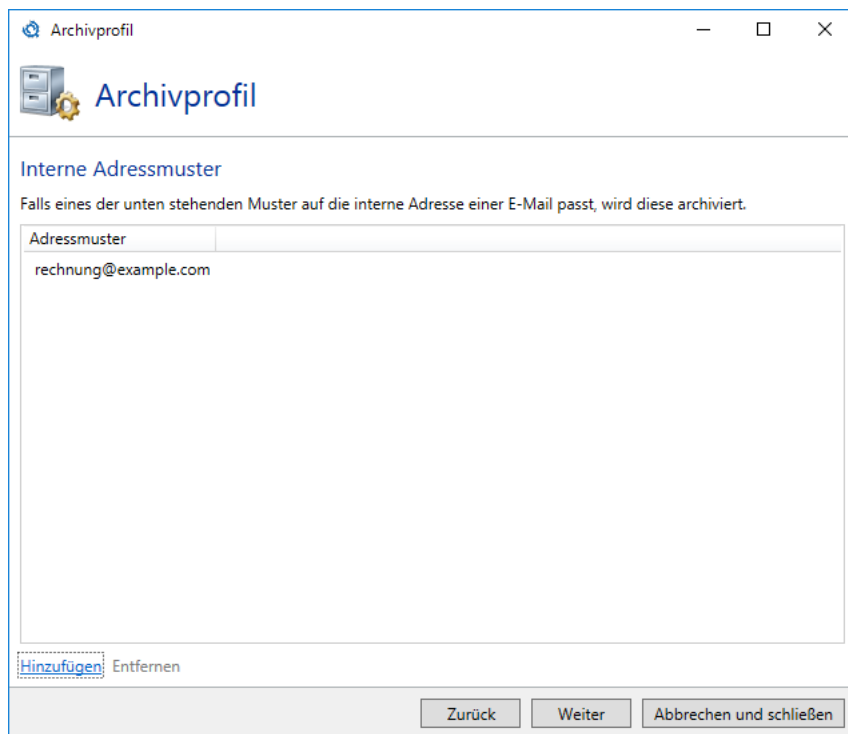


Bild 160: Zuordnung von Profilen zu internen E-Mail-Adressen

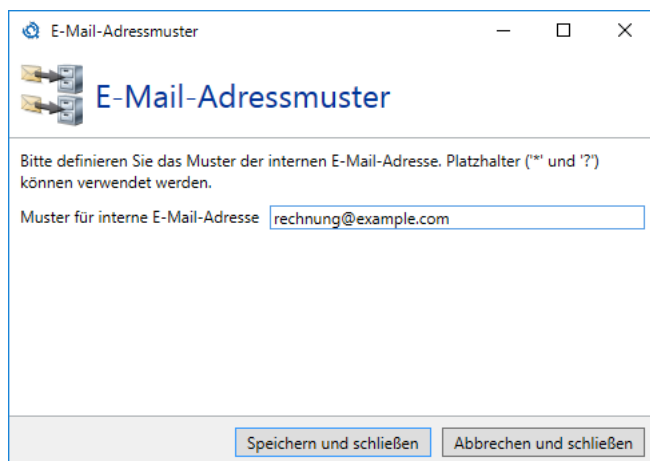


Bild 161: Neue Zuordnung erstellen

Im letzten Schritt definieren Sie in einem Profil, wie Metadaten einer E-Mail auf Metadaten im Archiv abgebildet werden. Metadaten umfassen unter anderem die Betreffzeile, Signatur- und Verschlüsselungsoptionen und andere E-Mail-Header. Um eine Verknüpfung der Werte zu erstellen, wählen Sie zunächst auf der linken Seite einen Wert aus. Wählen Sie danach aus der Liste rechts ein Feld aus dem Archiv aus. Je nach gewähltem Archivsystem kann die Liste der verfügbaren Felder sehr

lang sein. Über den Eigenschaftsfilter können Sie nach bestimmten Feldern suchen. Sobald Sie ein Feld in der Liste auswählen, wird die Zuordnung hergestellt ([Bild 162](#)).



Auf einem Profil für ein Archivpostfach werden keine Metadaten-Zuordnungen konfiguriert, da die E-Mail komplett an das Archivpostfach weitergeleitet wird, damit alle Metadaten in der E-Mail erhalten bleiben.

Eigenschaften der Gateway Rolle	Eigenschaften des Archivs
Bcc	Nicht gesetzt
Cc	Nicht gesetzt
connection-client-ip	Nicht gesetzt
connection-starttime	Nicht gesetzt
connection-type	Nicht gesetzt
Content-Disposition	Nicht gesetzt
Content-Id	Nicht gesetzt
Content-Location	Nicht gesetzt
Content-Transfer-Encoding	Nicht gesetzt
Content-Type	Nicht gesetzt
Date	Nicht gesetzt
Disposition-Notification-To	Nicht gesetzt
...	...

Eigenschaftsfilter:

Wählen Sie eine Archiv-Eigenschaft:

- 1
- 10
- 100
- 11
- 12
- 13
- 14
- 15
- 16

[Metadaten-Zuordnung entfernen](#)

Zurück Fertigstellen Abbrechen und schließen

Bild 162: Metadaten-Zuordnung

Nachdem Sie mindestens ein Profil erstellt haben, ist die Konfiguration des Konnektors abgeschlossen.

De-Mail-Anbieter

Hier können Sie die Verbindungen zum De-Mail-System hinterlegen ([Bild 163](#)).

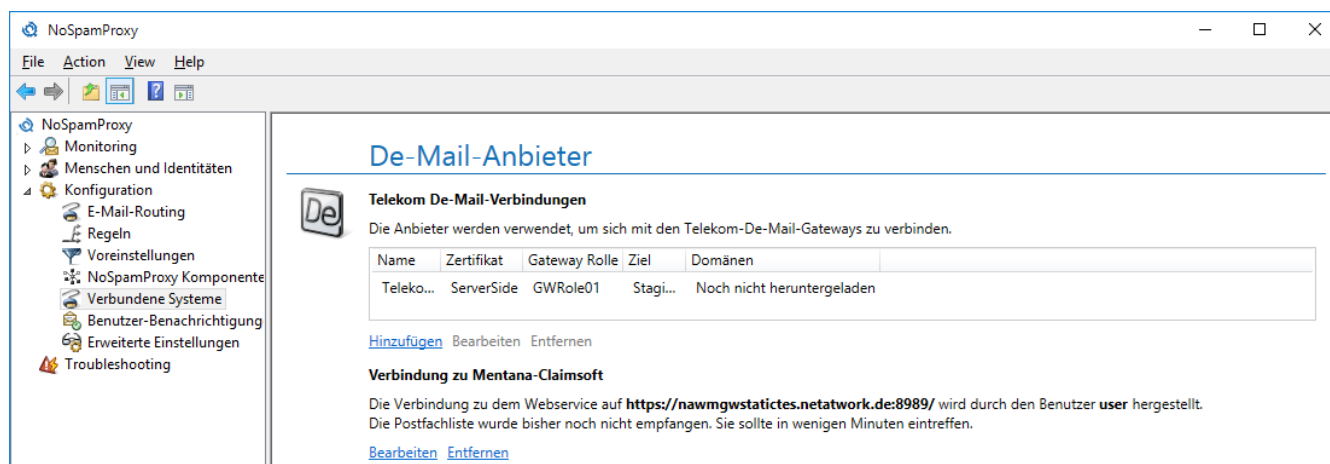


Bild 163: Die Liste der konfigurierten De-Mail-Verbindungen



Die in diesem Abschnitt eingegebenen Informationen sind sowohl für die De-Mail-Sendekonnektoren als auch die Empfangskonnektoren sofort verfügbar. Das heißt, dass Sie die Verbindung nur einmal konfigurieren müssen und sie Ihnen sofort in allen Konnektoren bereitsteht.

Telekom De-Mail-Verbindungen

Um Konnektoren für De-Mail über die Telekom zu erstellen, müssen zunächst die Verbindungen zum Diensteanbieter konfiguriert werden. ([Bild 164](#)).

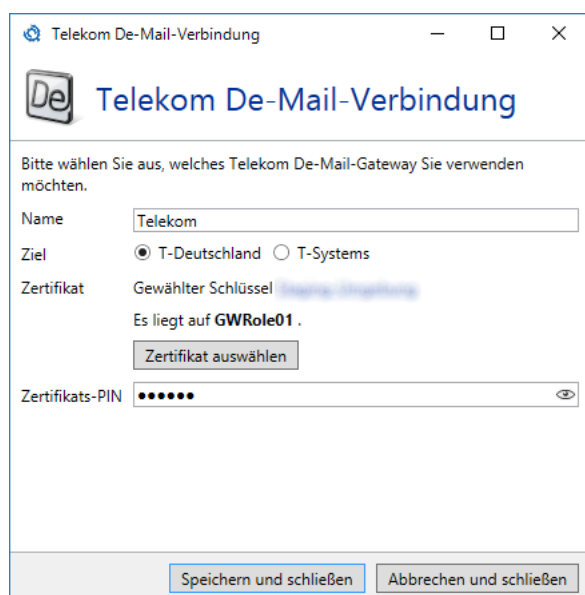


Bild 164: Konfigurieren Sie die Verbindung zum Telekom De-Mail-Anbieter

Neben dem Namen des Profils wählen Sie hier aus, ob Sie die Verbindung über T-Deutschland oder T-Systems herstellen möchten. Des Weiteren wählen Sie das Zertifikat aus, das für die Absicherung der Verbindung zum Diensteanbieter verwendet wird. Da das Zertifikat auf einer Smartcard gespeichert ist, müssen Sie auch noch die PIN für die Karte eingeben.



Durch die Auswahl des Zertifikats ergibt sich automatisch die Bindung des Profils an eine Gateway Rolle. Konnektoren, die das Profil verwenden, werden automatisch der Gateway Rolle zugeordnet, auf der das Zertifikat liegt.

Verbindung zu Mentana-Claimsoft

Für die De-Mail-Konnektoren von Mentana-Claimsoft muss eine Verbindung zu dem Webservice dieses Anbieters eingerichtet werden ([Bild 165](#)).

Verbindung zu Mentana-Claimsoft

De-Mail Verbindung zu Mentana-Claimsoft

Bitte geben Sie die Adresse Ihres Mentana-Claimsoft-Web-Services an.

Dienstadresse

Benutzerinformationen werden für die erfolgreicher Verbindung zum Webservice benötigt.

Benutzername

Passwort

Bild 165: Verbinden Sie sich zum Mentana-Claimsoft-Webservice

Geben Sie unter **Dienstadresse** die Adresse ein, unter der der Webservice erreicht werden kann. Geben Sie unter **Benutzername** und **Passwort** die Anmeldeinformationen für den erfolgreichen Zugriff auf den Dienst ein.



Die in diesem Dialog eingegebenen Informationen sind sowohl für den De-Mail-Sendekonnektor als auch den Empfangskonnektor sofort verfügbar. Das heißt, dass Sie die Verbindung nur einmal konfigurieren müssen und sie Ihnen sofort in allen Konnektoren bereitsteht.

CSA-Whitelist

Um die [CSA-Whitelist](#) Aktion zu verwenden, müssen Sie zuerst den Download der Liste konfigurieren ([Bild 166](#)). Wählen Sie dazu **Bearbeiten**. Es öffnet sich der Dialog für die Konfiguration ([Bild 167](#)).

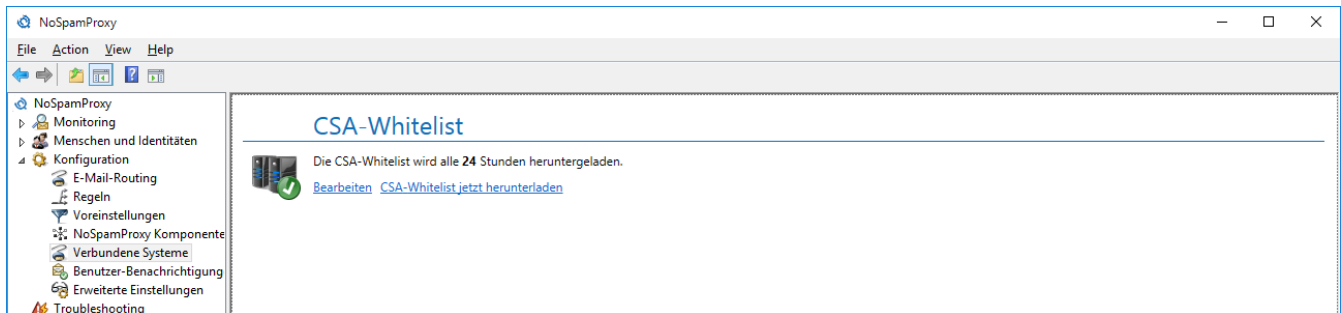


Bild 166: Verbindung zur CSA-Whitelist

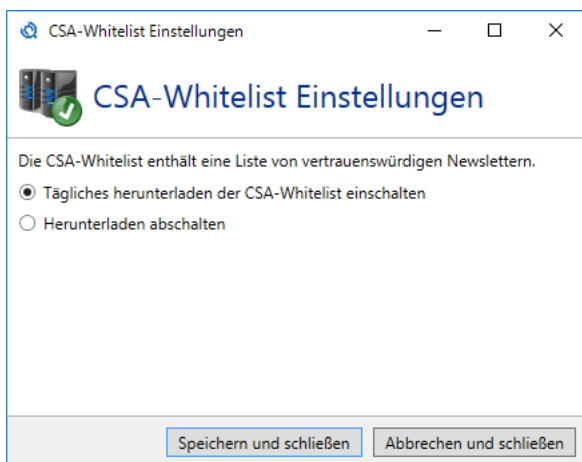


Bild 167: Konfigurieren Sie das Herunterladen der CSA-Whitelist

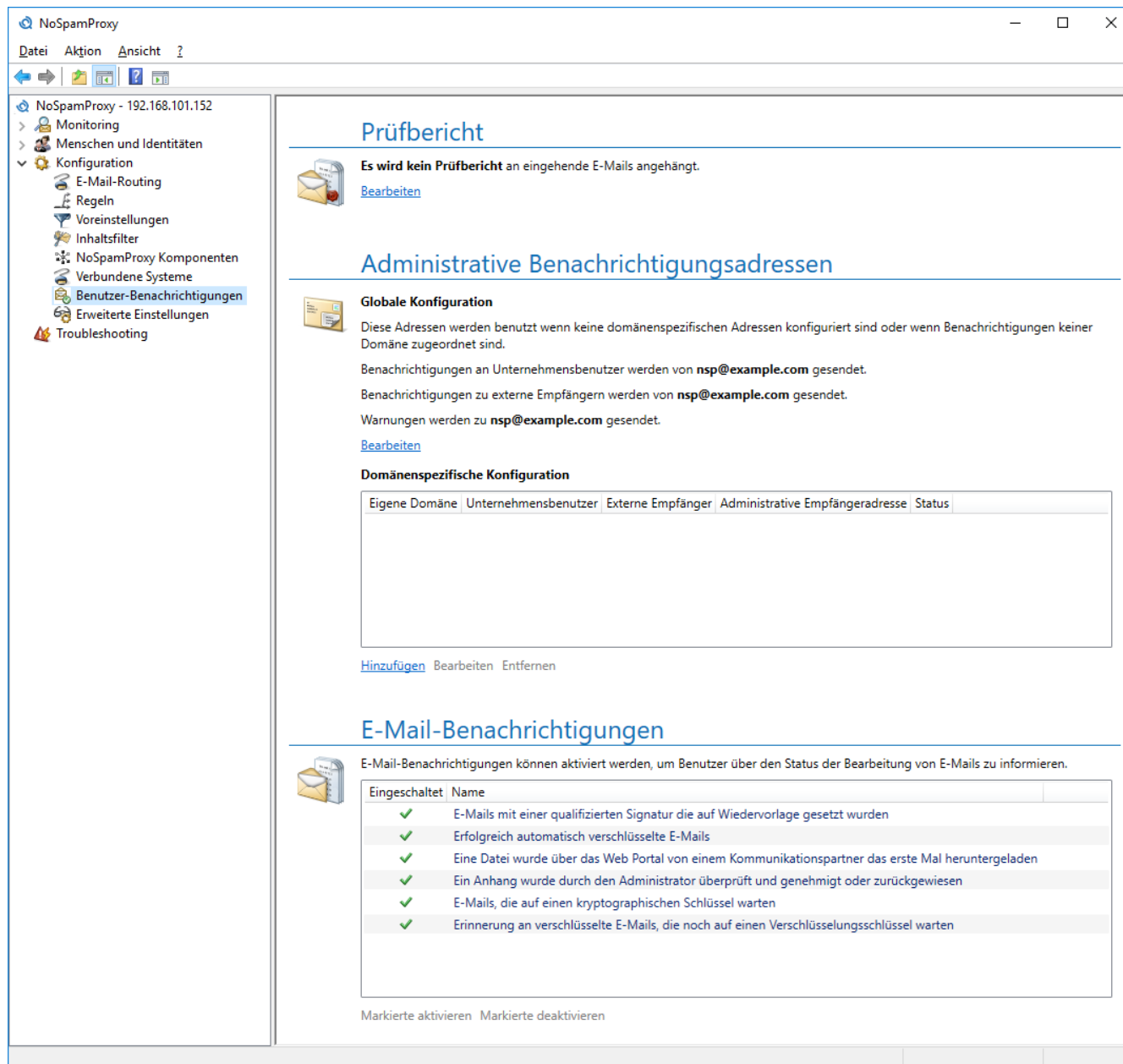
Wählen Sie **Tägliches herunterladen der CSA-Whitelist einschalten** wenn Sie die [CSA-Whitelist](#) Aktion verwenden wollen. Ansonsten können Sie **Herunterladen abschalten** wählen.



Die CSA-Whitelist wird von der Domäne `service.nospamproxy.de` heruntergeladen. Damit Ihr NoSpamProxy diese Liste laden kann, benötigt es den Zugriff auf diese Adresse. Bitte schalten Sie ggf. Ihre Firewall dafür frei.

Benutzer-Benachrichtigungen

Im Knoten Benutzer-Benachrichtigungen können Sie festlegen, welche Nachrichten NoSpamProxy automatisch an interne und externe Kontakte versendet. Außerdem können Sie festlegen, welche Absenderadressen verwendet werden ([Bild 168](#)).



Prüfbericht

Es wird kein Prüfbericht an eingehende E-Mails angehängt.
[Bearbeiten](#)

Administrative Benachrichtigungsadressen

Globale Konfiguration

Diese Adressen werden benutzt wenn keine domänenspezifischen Adressen konfiguriert sind oder wenn Benachrichtigungen keiner Domäne zugeordnet sind.

Benachrichtigungen an Unternehmensbenutzer werden von **nsp@example.com** gesendet.

Benachrichtigungen zu externe Empfängern werden von **nsp@example.com** gesendet.

Warnungen werden zu **nsp@example.com** gesendet.

[Bearbeiten](#)

Domänenspezifische Konfiguration

Eigene Domäne	Unternehmensbenutzer	Externe Empfänger	Administrative Empfängeradresse	Status
---------------	----------------------	-------------------	---------------------------------	--------

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)

E-Mail-Benachrichtigungen

E-Mail-Benachrichtigungen können aktiviert werden, um Benutzer über den Status der Bearbeitung von E-Mails zu informieren.

Eingeschaltet	Name
✓	E-Mails mit einer qualifizierten Signatur die auf Wiedervorlage gesetzt wurden
✓	Erfolgreich automatisch verschlüsselte E-Mails
✓	Eine Datei wurde über das Web Portal von einem Kommunikationspartner das erste Mal heruntergeladen
✓	Ein Anhang wurde durch den Administrator überprüft und genehmigt oder zurückgewiesen
✓	E-Mails, die auf einen kryptographischen Schlüssel warten
✓	Erinnerung an verschlüsselte E-Mails, die noch auf einen Verschlüsselungsschlüssel warten

[Markierte aktivieren](#) [Markierte deaktivieren](#)

Bild 168: Benutzerbenachrichtigungen

Administrative E-Mail-Adressen

In diesem Abschnitt werden Adressen für Benachrichtigungen von NoSpamProxy hinterlegt ([Bild 169](#)). NoSpamProxy benötigt für die von ihm zu sendenden E-Mail-Benachrichtigungen gültige Absenderadressen. Abhängig davon, ob der Empfänger ein Unternehmensbenutzer ist oder nicht, können unterschiedliche Absenderadressen genutzt werden. Für Benachrichtigungen über bestimmte Vorfälle wird eine Empfängeradresse für diese Benachrichtigungen benötigt. Tragen Sie die Adresse in das Feld **Empfängeradresse** ein.

Im Abschnitt **Globale Konfiguration** stellen Sie die Adressen für alle Domänen ein, die keinen eigenen Eintrag besitzen oder für Benachrichtigungen, die keiner Domäne zugeordnet sind.

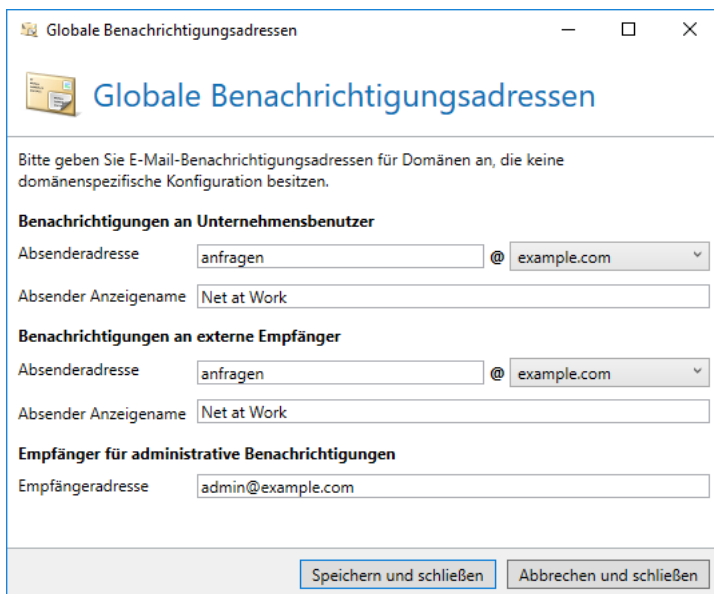


Bild 169: Die globalen Benachrichtigungsadressen

Falls eine Domäne eine von den globalen Einstellungen abweichende Konfiguration benötigt, können Sie diese in der Liste **Domänenspezifische Konfiguration** hinzufügen. Der Einstellungsdialog ist analog zur globalen Konfiguration. Zusätzlich müssen Sie noch eine Ihrer eigenen Domänen, für die diese Konfiguration gelten soll, auswählen.

Benutzer-Benachrichtigungen

Hier werden die konfigurierbaren Benachrichtigungen angezeigt. Sie können die einzelnen Benachrichtigungen markieren und aktivieren oder deaktivieren.

Erweiterte Einstellungen

Unter dem Knoten "Erweiterte Einstellungen" finden Sie Konfigurationsmöglichkeiten, die Sie in der Regel nicht anpassen müssen. ([Bild 170](#)).

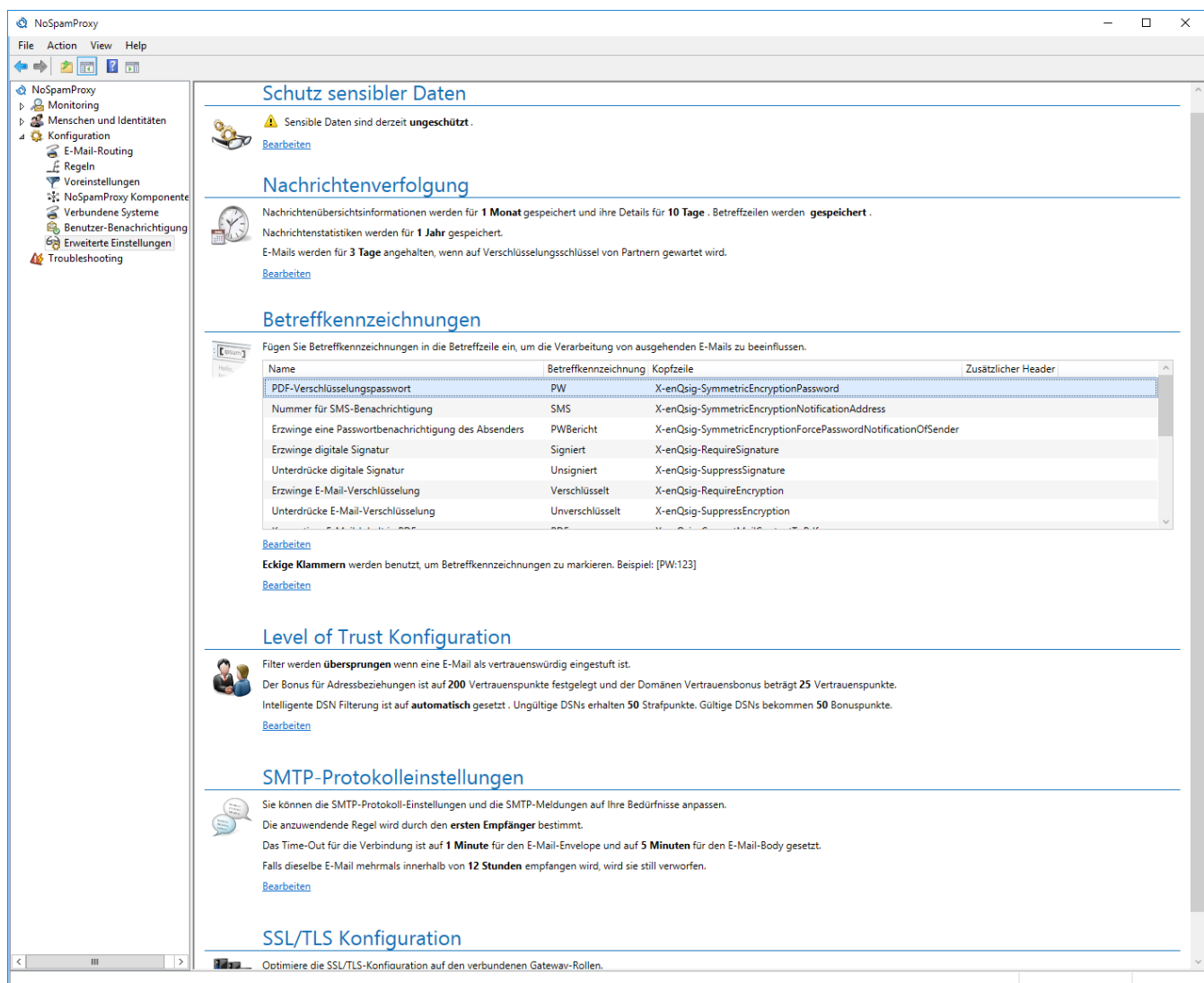


Bild 170: Die erweiterte Einstellungen von NoSpamProxy

Schutz sensibler Daten

Um sensible Daten wie beispielsweise kryptographische Schlüssel oder Authentifizierungsinformationen vor dem Zugriff durch Dritte zu schützen, müssen Sie diese Daten durch ein von Ihnen angegebenes Passwort verschlüsseln lassen ([Bild 171](#)). Sie können auch zu einem späteren Zeitpunkt das Passwort ändern; der Schutz der Daten kann aber nicht mehr rückgängig gemacht werden.



Sollten Sie das Passwort vergessen und die Konfiguration mit dem verschlüsselten Passwort gelöscht werden, gibt es keine weitere Möglichkeit auf die geschützten Daten zuzugreifen. Verwahren Sie deswegen immer eine Kopie des Passworts an sicherer Stelle.

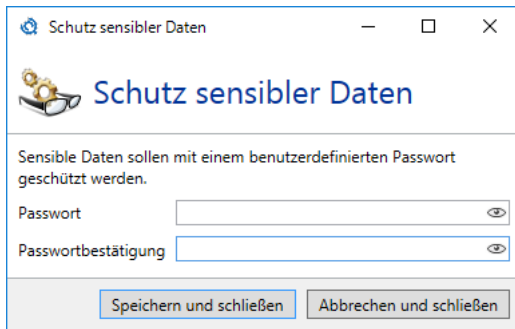


Bild 171: Das Passwort zum Schutz Ihrer Daten

Monitoring

NoSpamProxy kann jede Verbindung in der Nachrichtenverfolgung mitprotokollieren, damit Sie jederzeit kontrollieren können, was mit den einzelnen E-Mails geschehen ist. Diese Funktion kann über die Option **Monitoring** komplett deaktiviert werden. Falls diese Option aktiviert ist, können Sie zusätzlich entscheiden, ob die Betreffzeilen der E-Mails ebenfalls gespeichert werden sollen oder ob diese von der Nachrichtenverfolgung ausgeschlossen werden sollen. Standardmäßig sind beide Optionen aktiviert.



Bitte beachten Sie die in Ihrem Unternehmen bestehenden Datenschutzvorschriften bei der Konfiguration dieses Abschnittes.

Um die Datenbankgröße der Nachrichtenverfolgung und der Reports nicht unkontrolliert wachsen zu lassen, räumt die Intranet Rolle die Datenbank in einem regelmäßigen Intervall auf. Dabei werden alle Elemente, die ein vorgegebenes Alter überschritten haben, aus der Datenbank gelöscht ([Bild 172](#)).

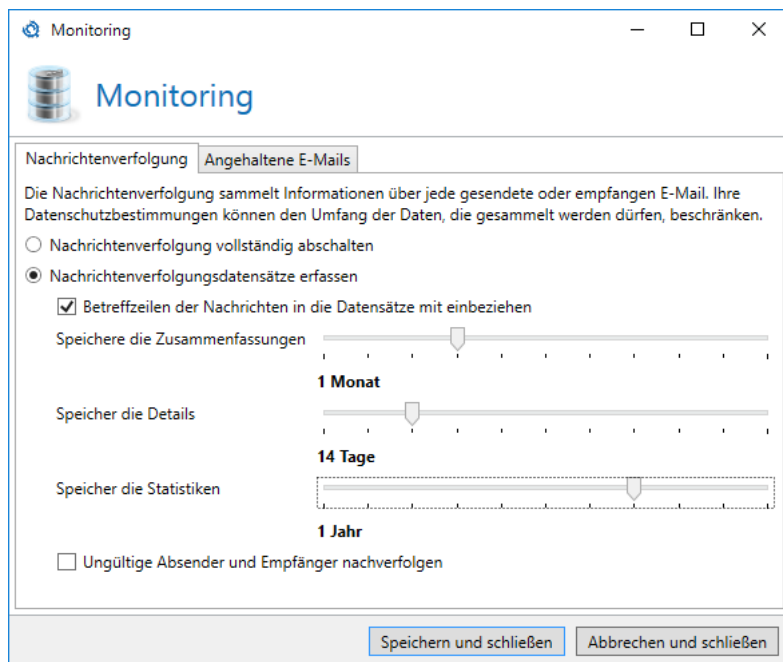


Bild 172: Anpassung der Aufbewahrungsfristen



Wenn alle Nachrichtenverfolgungsdatensätze und die statistischen Daten verworfen werden sollen, wählen Sie bitte die Option 'Nachrichtenverfolgung vollständig abschalten' unter dem Knoten 'Erweiterte Einstellungen' der Gateway Rolle. In diesem Fall werden absolut keine Daten gesammelt. Wenn Sie zum Beispiel nur die statistischen Daten aufzeichnen wollen, wählen Sie die Option **Nachrichtenverfolgungsdatensätze werden sofort gelöscht** um alle Nachrichtenverfolgungsdatensätze um 2 Uhr nachts zu löschen.

Mit dem Schieberegler **Speichere die Zusammenfassungen** stellen Sie ein, wie weit Sie generell E-Mails zurückverfolgen können wollen. Mit den Nachrichtenübersichtsinformationen können Sie lediglich in der Übersicht der Nachrichtenverfolgung sehen, ob und wann die gesuchte E-Mail angekommen ist und ob Sie angenommen oder abgewiesen wurde. Die Vorhaltezeit für die dazu gehörenden Nachrichtendetails wird mit dem Regler **Speichere die Details** eingestellt. In den Nachrichtendetails finden Sie die Bewertungen der einzelnen Filter, Informationen zum Ursprung der E-Mail und zur Dauer der Überprüfung sowie weitere nützliche Informationen. Da diese Informationen den größten Teil der Nachrichtenverfolgung ausmachen, ist es möglich, diese über einen kürzeren Zeitraum als die Übersichtsinformationen aufzubewahren.

Der Regler **Speicher die Statistiken** ist für den Inhalt der Reports zuständig. Mit ihm können Sie einstellen, über welchen Zeitraum Sie generell Reports erstellen können möchten. Um einen einigermaßen aussagekräftigen Report erstellen zu können, empfehlen wir eine Mindestaufbewahrungsfrist von 12 Monaten.



Wenn Sie mehrere 10.000 E-Mails oder Spam-E-Mails pro Tag erhalten, kann das Limit der Datenbankgröße bei einem SQL-Server in der Express-Edition überschritten werden. Bei so vielen E-Mails sollten ggf. kürzere Aufbewahrungsfristen der Nachrichtenverfolungsdatensätze gewählt werden oder eine SQL Server Datenbank ohne diese Beschränkung installiert werden.

Neben den Einstellungen für die Nachrichtenverfolgung können Sie in diesem Dialog auch noch konfigurieren, wie lange NoSpamProxy E-Mails zurückhält, für die auf einen Verschlüsselungsschlüssel gewartet wird.

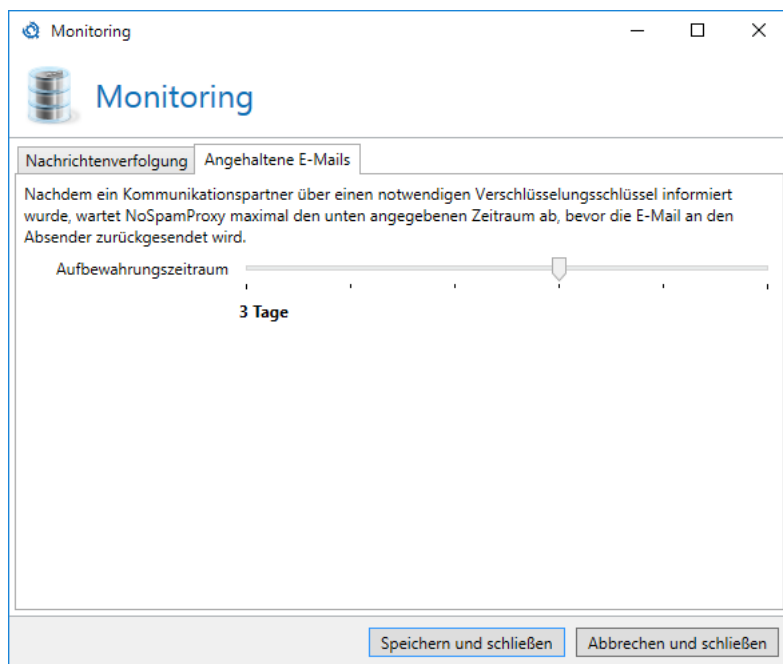


Bild 173: Anpassung der Aufbewahrungsfrist für angehaltene E-Mails

Betreffkennzeichnungen

Die Betreffkennzeichnungen definieren Schlüsselwörter, um die Verarbeitung von einzelnen E-Mails zu steuern. Das Einfügen eines Schlüsselwortes in den Betreff einer E-Mail zieht dann bestimmte Aktionen nach sich. Diese Schlüsselwörter werden vor dem Versand von NoSpamProxy aus der Betreffzeile entfernt.

Nutzen Sie die Betreffkennzeichnungen, indem Sie am Anfang oder Ende der Betreffzeile in Klammern die Schlüsselwörter aus der folgenden Liste angeben, die Ihre Aufgaben definieren. Leerzeichen und Unterschiede zwischen Groß- und Kleinschreibung werden im Schlüsselwort ignoriert. Das bedeutet, dass die folgenden Beispiele das gleiche Resultat ergeben. Alternativ können Sie auch das **Outlook Add-In von NoSpamProxy** nutzen.

Standardmäßig werden eckige Klammern verwendet, um die Betreffkennzeichnungen kenntlich zu machen. Über den Dialog zum Bearbeiten der Markierung können Sie festlegen, welche Art von Markierung verwendet werden soll ([Bild 174](#)).

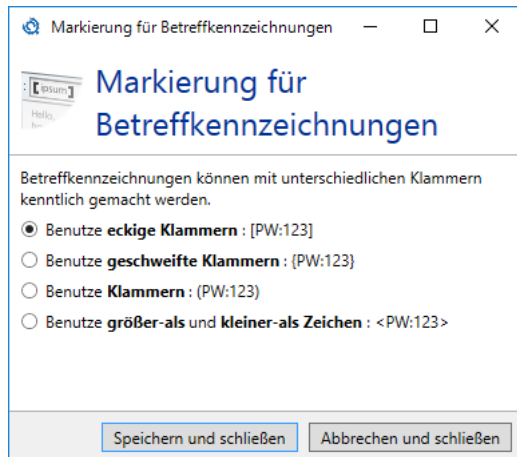


Bild 174: Konfigurieren Sie die Marker für Betreffkennzeichnungen

Beispiele für den Einsatz von Betreffkennzeichnungen in der Betreffzeile:

[pw:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument

[PW : geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument

Oder auch mehrere Kennzeichnungen gleichzeitig in einer Klammer [Unverschlüsselt, PDF, PW:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument

Oder auch mehrere Kennzeichnungen gleichzeitig in unterschiedlichen Klammern

[Unverschlüsselt] [PDF] [PW:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument



Die Betreffkennzeichnungen müssen am Anfang oder am Ende der Betreffzeile stehen, um Ordnungsgemäß verarbeitet zu werden.



In Abhängigkeit der von Ihnen lizenzierten Funktionen können Ihnen andere Kennzeichnungen zur Verfügung stehen, als die im obigen Beispiel genannten. Die obigen Hinweise gelten bei allen Kennzeichnungen.

Die folgenden Betreffkennzeichnungen stehen Ihnen zur Verfügung:

- **[LFT]**
Diese Kennzeichnung wird nur vom Outlook Add-In für die **Large Files** verwendet.

Sie können die Betreffkennzeichnungen an Ihre Bedürfnisse anpassen ([Bild 175](#)) und auch wieder auf ihre Standardwerte zurücksetzen.



Im Outlook Add-In können Sie einstellen, dass an Stelle der X-Header die Betreffkennzeichnungen verwendet werden. Nehmen Sie in diesem Fall keine Änderungen in diesem Bereich vor. Das Add-In wird sonst nicht mehr funktionieren.

PDF-Verschlüsselungspasswort

PDF-Verschlüsselungspasswort

Betreffkennzeichnungen können genutzt werden um die Verarbeitung von ausgehenden E-Mails zu kontrollieren. Sie können diese Kennzeichnungen in die Betreffzeile einfügen. Geben Sie an, wie Sie diese Betreffkennzeichnung über die Betreffzeile einer E-Mail steuern möchten.

☒ Benutze den Standardnamen **PW**

☐ Nutze einen alternativen Namen

Name

Die Zeichen 'A-Z', 'a-z', '0-9' and '.' sind in der Betreffkennzeichnung erlaubt.
Es wird keine Unterscheidung zwischen Groß- und Kleinbuchstaben gemacht.

Der Header **X-enQsig-SymmetricEncryptionPassword** wird benutzt um die Betreffkennzeichnung zu kontrollieren.

☐ Verwende zusätzlich zu obigem Header den Folgenden

Header-Name

Bild 175: Betreffkennzeichnungen bearbeiten

Beim automatisierten Versand von E-Mails können Sie anstatt der [Betreffkennzeichnungen](#) auch E-Mail-Header in die Nachricht einfügen, um diese Informationen anzugeben. Die E-Mail-Header werden im Folgenden erklärt. In der Oberfläche finden Sie neben der Betreffkennzeichnung den dazu gehörigen X-Header. Wenn Sie bereits eine Software einsetzen, die Betreffkennzeichnungen setzt und diese für die Funktion in NoSpamProxy einsetzen, so können Sie im Bearbeiten-Dialog einen zusätzlichen Header definieren. Dieser wird dann zusätzlich zum normalen Header verwendet.



Anstatt der Nutzung der 'Betreffkennzeichnungen' können Sie auch das **Outlook Add-In** für NoSpamProxy installieren. Das Outlook Add-In wird an Stelle der Betreffkennzeichnungen mit Outlook 2007 und Outlook 2010 verwendet.

Level-of-Trust-Konfiguration

Das Level-of-Trust-System ist ein mehrschichtiges Konzept, das die Vertrauenswürdigkeit einer Kommunikationsbeziehung oder einer Domäne beurteilt. "Vertrauen" muss sich ein Absender verdienen. Stärkster Pluspunkt dabei ist eine verlässliche und dauerhafte Verbindungshistorie.

Das System bewertet verschiedene Kriterien, u.a. Absenderadressen und Prüfsummen, vor allem aber auch die Adressbeziehungen zwischen Absendern und Empfängern von E-Mails.

Bei E-Mails an externe Adressen wird die Kommunikationsbeziehung (zwischen Absender und Adressat) in der Datenbank mit einem sehr hohen Vertrauensbonus gespeichert. Um diese Daten zu schützen, wird die Beziehung nicht im Klartext gespeichert, sondern nur in Form eines Hashwertes (Prüfsumme) festgehalten. Des Weiteren ist die Relation von Absender, Betreff und Domäne des Empfängers eine interessante Perspektive. Es liegt nahe, auch eine Antwort eines Kollegen oder eines Stellvertreters, und gegebenenfalls eine alternative Adresse, als "gut" bewerten zu können. Zusätzlich wird bei E-Mails das Vertrauen in die Domäne des Adressaten um einen bestimmten Wert erhöht. Damit erhalten auch die Antwort-E-Mails des Adressaten an andere Nutzer des Systems einen Bonus. Wird eine E-Mail an lokale Adressen als Spam klassifiziert, verringert sich das Vertrauen in die Domäne.

Findet über einen gewissen Zeitraum keine Kommunikation mit einem bestimmten Absender mehr statt, verringert sich der Level of Trust automatisch. Diese Abnahme des Wertes geschieht sowohl bei Bonus- als auch bei Malus-Werten. Einem längeren "Schweigen" wird auf diese Art und Weise sowohl im Positiven wie auch im Negativen Rechnung getragen: verlässliche, dauerhafte Kommunikation hinterlässt einen immer besseren Eindruck, Spam-Wiederholungstäter einen immer schlechteren.

Das Level-of-Trust-System muss pro Regel aktiviert werden. Die Einstellungen werden jedoch im Menü "Level of Trust" global vorgenommen ([Bild 176](#)).

Allgemeine Einstellungen

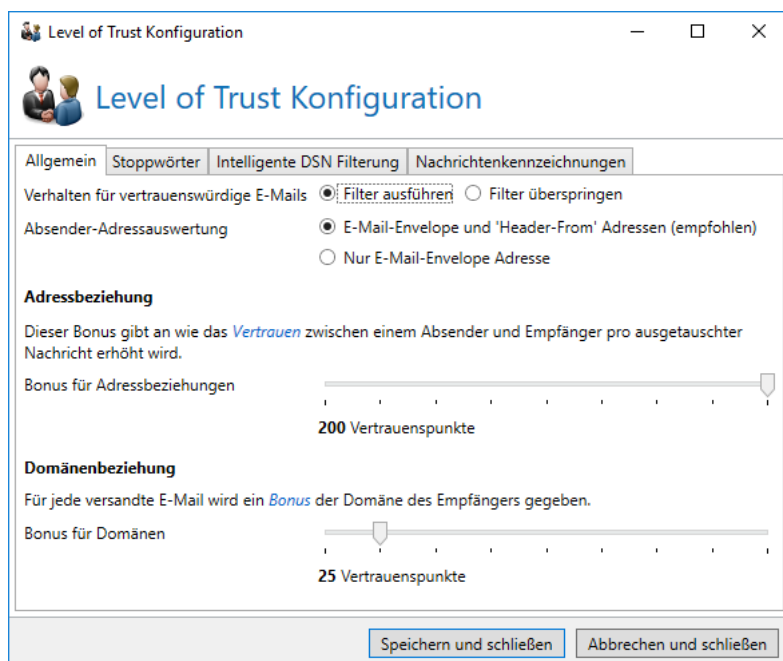


Bild 176: Definieren Sie die allgemeinen Einstellungen des Level-of-Trust-Systems

Wenn die Funktion **Filter für vertrauenswürdige E-Mails überspringen** aktiviert wird, werden E-Mails an lokale Adressen mit einer hinreichend hohen Level-of-Trust-Bewertung als vertrauenswürdig markiert.

Filter, die auf einer Regel definiert sind, werden dann übersprungen. Lediglich Aktionen - wie zum Beispiel die [Cyren-Premium-AntiVirus-Aktion](#) - können die Annahme der E-Mail dann noch verhindern.

Bei unterschiedlichen E-Mail-Adressen im E-Mail-Envelope und im 'Header-From' können Sie einstellen, welche von NoSpamProxy für die Analyse genutzt werden. Falls beide Adressen validiert werden und das Ergebnis des E-Mail-Envelopes die weitere Zustellung erlaubt, wird dieses Ergebnis durch die Analyse der 'Header-From'-Adresse überschrieben. Das bedeutet, dass ein bedenkliches Ergebnis in der E-Mail-Envelope- oder 'Header-From'-Adresse, immer sicher die E-Mail abweist.

Mit der Einstellung **Bonus für Adressbeziehungen** legen Sie fest, um wie viele Punkte das Vertrauen zwischen einem Absender und einem Empfänger pro Nachricht erhöht wird (Adressbeziehung). Mit dem Schieberegler können Sie hier einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht dabei (-0,1) Punkten für den SCL.

Für jede E-Mail an externe Adressen wird nicht nur der sogenannte Adressbeziehungsbonus erhöht, sondern auch ein Bonus für die jeweilige Empfängerdomäne. Um wie viele Punkte das geschieht, stellen Sie mit dem Schieberegler **Bonus für Domänen beträgt...** ein. Dieser Wert sollte kleiner sein als der Bonus für Adressbeziehungen. Auch hier können Sie mit dem Schieberegler einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht auch dabei (-0,1) Punkten für den SCL.

Stoppwörter

Auf der Registerkarte **Stoppwörter** definieren Sie die sogenannten Stoppwörter ([Bild 177](#)).

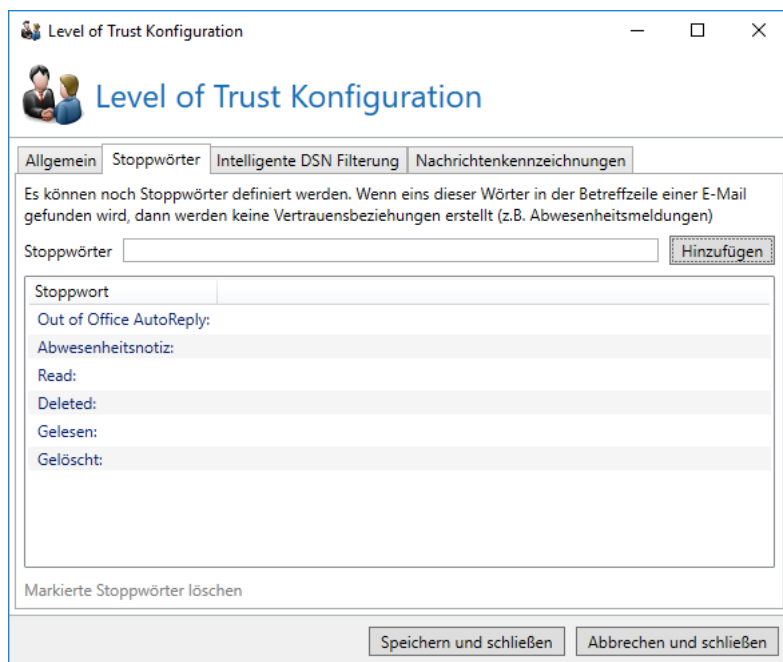


Bild 177: Definierten Stoppwörter, die Veränderungen der Level-of-Trust-Beziehungen unterbinden

Sobald die Gateway Rolle eines dieser Wörter im Betreff einer E-Mail an externe Adressen findet, bleiben sowohl der Adressbeziehungsbonus, als auch der Domänen Bonus gleich und werden nicht erhöht. Bei automatisch generierten E-Mails wie Abwesenheitsnotizen ist das eine sinnvolle Einstellung.

Intelligente DSN-Filterung

Die intelligente DSN-Filterung überprüft Delivery Status Notifications (DSNs) an lokale Adressen. Da NoSpamProxy weiß, welche E-Mails aus dem Unternehmen versendet wurden, kann die Software auch feststellen, ob für den gerade vorliegenden DSN eine entsprechende E-Mail das Unternehmen verlassen hat ([Bild 178](#)).

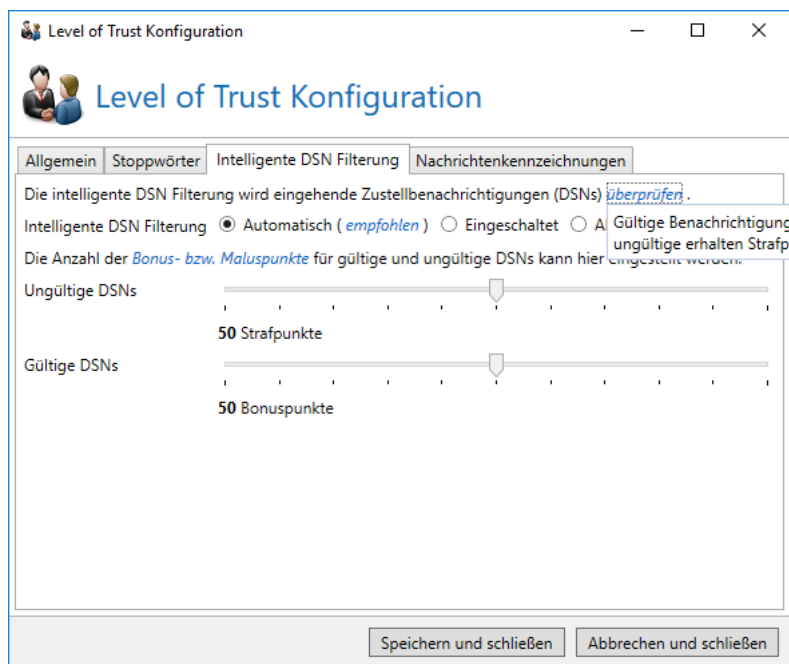


Bild 178: Konfigurieren Sie die intelligente DSN-Filterung

Ein Beispiel: Es kommt ein DSN an und NoSpamProxy stellt fest, dass die Originalnachricht für diesen DSN von schmidt@example.com an schulze@netatwork.de gesendet wurde. Dann überprüft das Mail Gateway, ob es ein Adresspaar schmidt@example.com/schulze@netatwork.de in der Level-of-Trust-Datenbank gibt. Wenn das nicht der Fall ist, kann der vorliegende DSN nicht gültig sein und erhält Maluspunkte. Findet sich ein passendes Adresspaar, erhält der DSN Bonuspunkte.

Damit diese Überprüfung stattfinden kann, müssen zwei Voraussetzungen gegeben sein: Zum einen muss ein RFC-konformer DSN vorliegen. Das bedeutet, dass die Originalnachricht als Anhang an dem DSN hängt, damit NoSpamProxy das Original-Adresspaar ermitteln kann. Des Weiteren muss sichergestellt sein, dass das Mail Gateway alle E-Mails an externe Adressen wirklich kennt. In Netzwerken mit verteilten Internetanbindungen kann das unter Umständen ein Problem sein.

Mit der Einstellung **Intelligente DSN-Filterung** können Sie die intelligente DSN-Filterung direkt beeinflussen. Setzen Sie den Radio-Button auf **Automatisch**, wird NoSpamProxy zunächst in der Level-of-Trust-Datenbank nachsehen, ob sich darin Elemente befinden, die älter als 7 Tage sind.

Erst wenn das gegeben ist, wird das Mail Gateway ankommende DSNs bewerten. Das ist auch die Standardeinstellung. Wenn Sie den Radio-Button auf **Aktiviert** setzen, wird NoSpamProxy den DSN immer bewerten, auch wenn noch keine Datensätze in der Level-of-Trust-Datenbank stehen. Um die intelligente DSN-Filterung abzuschalten, setzen Sie den Radiobutton auf **Deaktiviert**.

Nachrichtenkennzeichnungen

Das Level-of-Trust-System benötigt zum Teil konsistente Betreffzeilen über eine Konversation. Nachrichtenbezeichnungen wie z.B. 'AW:' oder 'WG:' müssen dazu entfernt werden. Auf der Registerkarte **Nachrichtenkennzeichnungen** konfigurieren Sie alle Kennzeichnungen, die Ihr E-Mail-System verwendet ([Bild 179](#)).

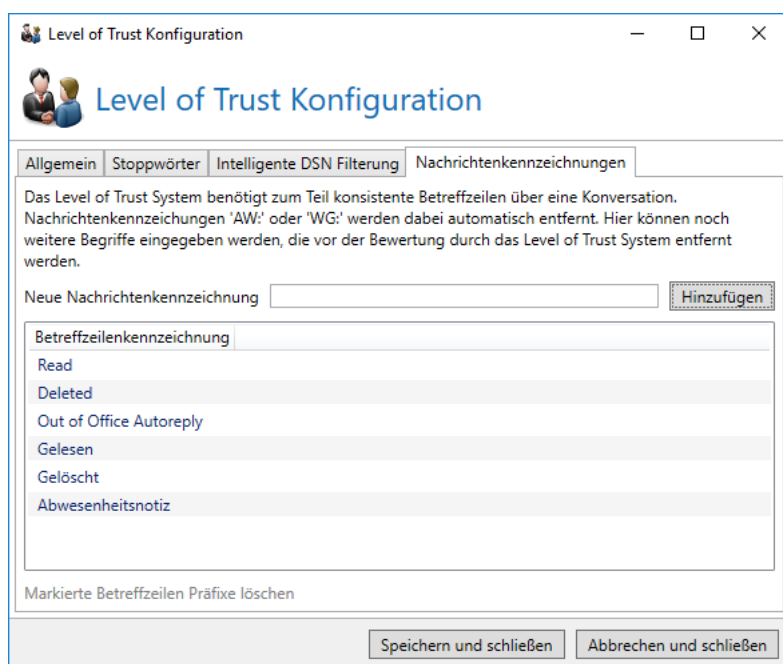


Bild 179: Definieren Sie Nachrichtenkennzeichnungen, die in den Betreffzeilen Ihrer E-Mails vorkommen

SMTP-Protokolleinstellungen

Die Protokolleinstellungen regeln das Verhalten beim Empfang von E-Mails, die SMTP-Timeouts und die SMTP-Statusmeldungen.

Verhalten

Wenn eine E-Mail an mehrere Empfänger geht, kann es sein, dass abhängig von den Empfängern unterschiedliche Regeln für diese E-Mail greifen. NoSpamProxy kann, bei entsprechender Einstellung, das einliefernde System dazu zwingen, für jeden einzelnen Empfänger eine eigene E-Mail zu schicken.

Diese Einstellung beugt Konflikten bei mehrfach adressierten E-Mails vor, wenn eine E-Mail über eine Verbindung an zwei Empfänger versendet wird und dabei zwei verschiedene Regeln zutreffen

würden. Durch die Verwendung von SMTP ist es nicht möglich, für einzelne Empfänger unabhängige Rückmeldungen zu liefern. Es kann immer nur die komplette Verbindung beendet werden.

Durch die Konfiguration der Option **Anwendung von Regeln** können Sie NoSpamProxy anweisen, an das einliefernde System die Fehlermeldung "Too many Recipients" zu senden, sofern Empfänger mit kollidierenden Regeln gesendet werden ([Bild 180](#)).

Laut RFC ist dies allerdings erst ab dem 101. Empfänger erlaubt, auch wenn bislang keine E-Mail-Server bekannt sind, die durch dieses Verhalten gestört werden.

Durch diese Einstellung wird jede E-Mail mit genau einem Empfänger versendet. So kann NoSpamProxy für jeden Empfänger die passende Regel anwenden. Allerdings werden die E-Mails entsprechend mehrfach vom Absender eingeliefert.

Die Aktivierung dieser Funktion erlaubt Ihnen die Steuerung der E-Mail-Bewertung für den Preis einer mehrfachen Übertragung und einem nicht ganz RFC-konformen Verhalten.

Ist diese Option deaktiviert, dann wird die Regel, die für den ersten Empfänger zutrifft, auf alle Empfänger dieser E-Mail angewendet.

Für alle anderen Empfänger gilt das gleiche Resultat.

NoSpamProxy kann erkennen, wenn dieselbe E-Mail mehrere Male empfangen wird. Das mehrfache Versenden derselben E-Mail tritt üblicherweise bei falscher Konfiguration, wie z.B. E-Mail-Schleifen, auf. Sie können einstellen, ob die E-Mails verworfen werden sollen oder nicht sowie wie groß das Zeitfenster für die Erkennung ist.

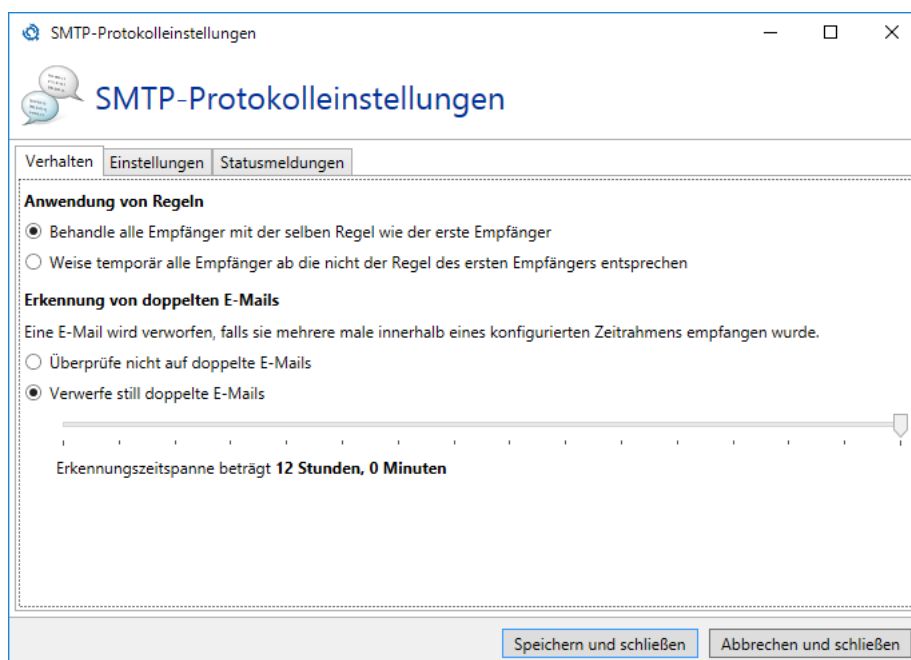


Bild 180: Verhalten beim Empfang von Nachrichten

Einstellungen

Das Anpassen der Timeouts ([Bild 181](#)) hat großen Einfluss auf den Ressourcenbedarf Ihres Servers bei starkem E-Mail-Verkehr.

Im Abschnitt **SMTP Protokoll Timeout Einstellungen** können Sie festlegen, ab wann NoSpamProxy bei Inaktivität eine Verbindung trennt. Dies wird für zwei Abschnitte innerhalb des SMTP-Protokolls festgelegt.

Mit der Einstellung **Envelope-Timeout beträgt n Sekunden** stellen Sie den Timeout für die Kommandos innerhalb des sogenannten Envelope Teils ein. Das betrifft alle Kommandos bis zum DATA-Befehl (HELO/EHLO, MAIL FROM, RCPT TO). Sobald der DATA-Befehl gesendet wurde, gilt die Einstellung **Body-Timeout beträgt n Sekunden**. Eine Trennung der Timeouts ist sinnvoll, da bei der Übertragung des Body Teils durch dazwischen geschaltete Filter und Aktionen Timeouts häufiger auftreten können als beim Envelope. Dieser wird bei einer normalen Übertragung sehr zeitnah und flüssig übertragen. Eine längere Wartezeit in diesem Teil der Mailübertragung deutet eher auf einen DoS-Angriff oder Ähnliches hin. Daher haben Sie die Möglichkeit, im Notfall den Timeout des Envelope Teils zu reduzieren. Mit den Schiebereglern bei den jeweiligen Einstellmöglichkeiten können Sie einen Wert zwischen 30 und 600 Sekunden einstellen.

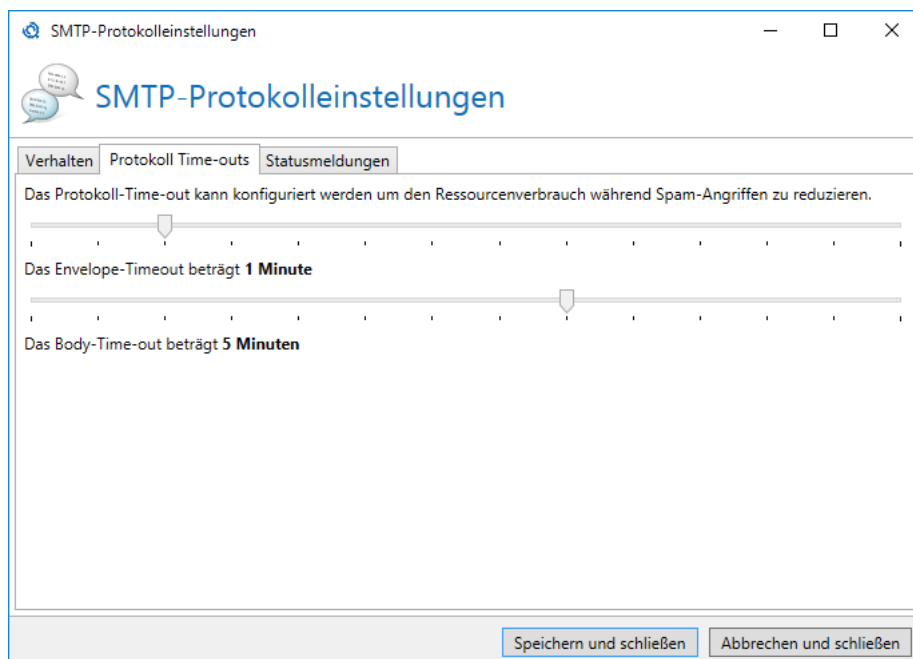


Bild 181: Timeouts

Statusmeldungen

Die Statusmeldungen ([Bild 182](#)) bestimmen mit welchen Texten sich das Gateway gegenüber anderen Servern meldet.

Die SMTP Antworten sind Standardangaben im SMTP-Handshake, die für den normalen User in der Regel nicht sichtbar sind. Dennoch kann es sinnvoll sein, die Angaben nach eigenem Bedarf zu ändern. Auf diese Art und Weise können Administratoren bei einer Fehlersuche die E-Mails mitunter leichter analysieren. Die Meldungen "Rejected mail" und "Blacklisted Address" sind beispielsweise wichtige Informationen für den Absender einer geblockten E-Mail.

Um eine Meldung zu ändern, klicken Sie einfach in das zugehörige Eingabefeld und ändern den Text.



Für SMTP Meldungen dürfen Sie keine Umlaute verwenden. Umlaute werden von dem verwendeten SMTP Protokoll nicht unterstützt.

Bild 182: Textuelle SMTP-Statusmeldungen von NoSpamProxy an andere Server

SSL/TLS-Konfiguration

Bei der Transportverschlüsselung wird die Verbindung über SSL oder TLS abgesichert. Dabei greift die Gateway Rolle auf das Betriebssystem zurück und dessen Einstellungen werden bei Verbindungen verwendet. In letzter Zeit haben sich einige Verschlüsselungsverfahren (z.B. DES oder RC4) als nicht mehr sicher herausgestellt. Daher ist sinnvoll, diese zu deaktivieren. Einige Cipher Suites unterstützen ein Verfahren namens [Perfect Forward Secrecy](#). Dies verhindert, kurz gesagt, dass die Inhalte von Verbindungen von unbefugten Dritten entschlüsselt werden können, selbst wenn der private Schlüssel des Server-Zertifikats bekannt ist. In der Standardeinstellung verwendet Windows diese Verfahren aber nicht bevorzugt. Sie können daher hier in der Oberfläche die empfohlenen Einstellungen anwenden ([Bild](#)

[183](#)). Damit die Änderungen wirksam werden, muss der Server neu gestartet werden. Dies können Sie direkt in dem Dialog veranlassen.



Hierbei handelt es sich um eine systemweite Änderung, die sich auch auf andere Programme auswirken kann.

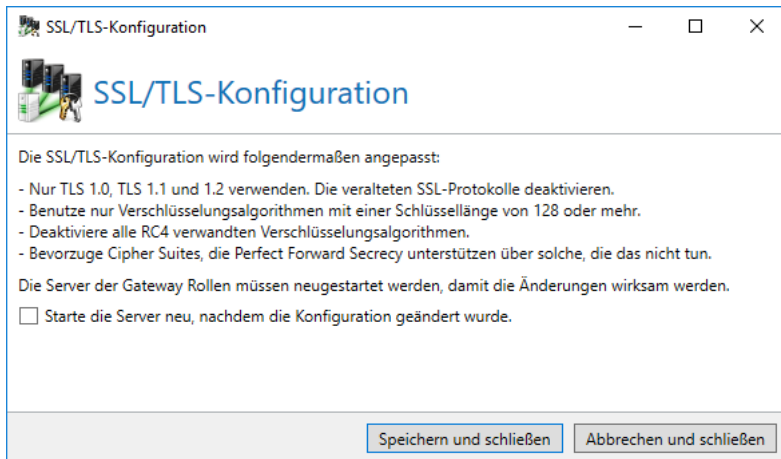


Bild 183: Empfohlene Einstellungen für die SSL/TLS-Konfiguration von Windows anwenden

Sie haben in diesem Bereich außerdem die Möglichkeit, die Standardwerte von Windows wiederherzustellen ([Bild 184](#)). Auch hier ist wieder ein Neustart des Servers notwendig, den Sie über den Dialog veranlassen können.

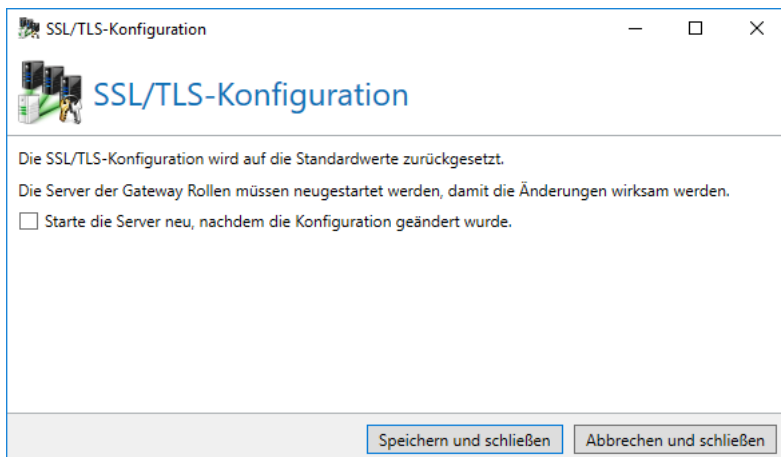


Bild 184: Auf Standardwerte für die SSL/TLS-Konfiguration zurückfallen

10. Troubleshooting

Unter dem Menüpunkt **Troubleshooting** befinden sich Werkzeuge, um Protokolle der Aktivitäten oder auch eine neue Datenbank für die einzelnen Rollen von NoSpamProxy zu erstellen ([Bild 185](#)). Das erneute Erstellen einer Datenbank kann notwendig werden, falls die alte Datenbank Schaden genommen hat.

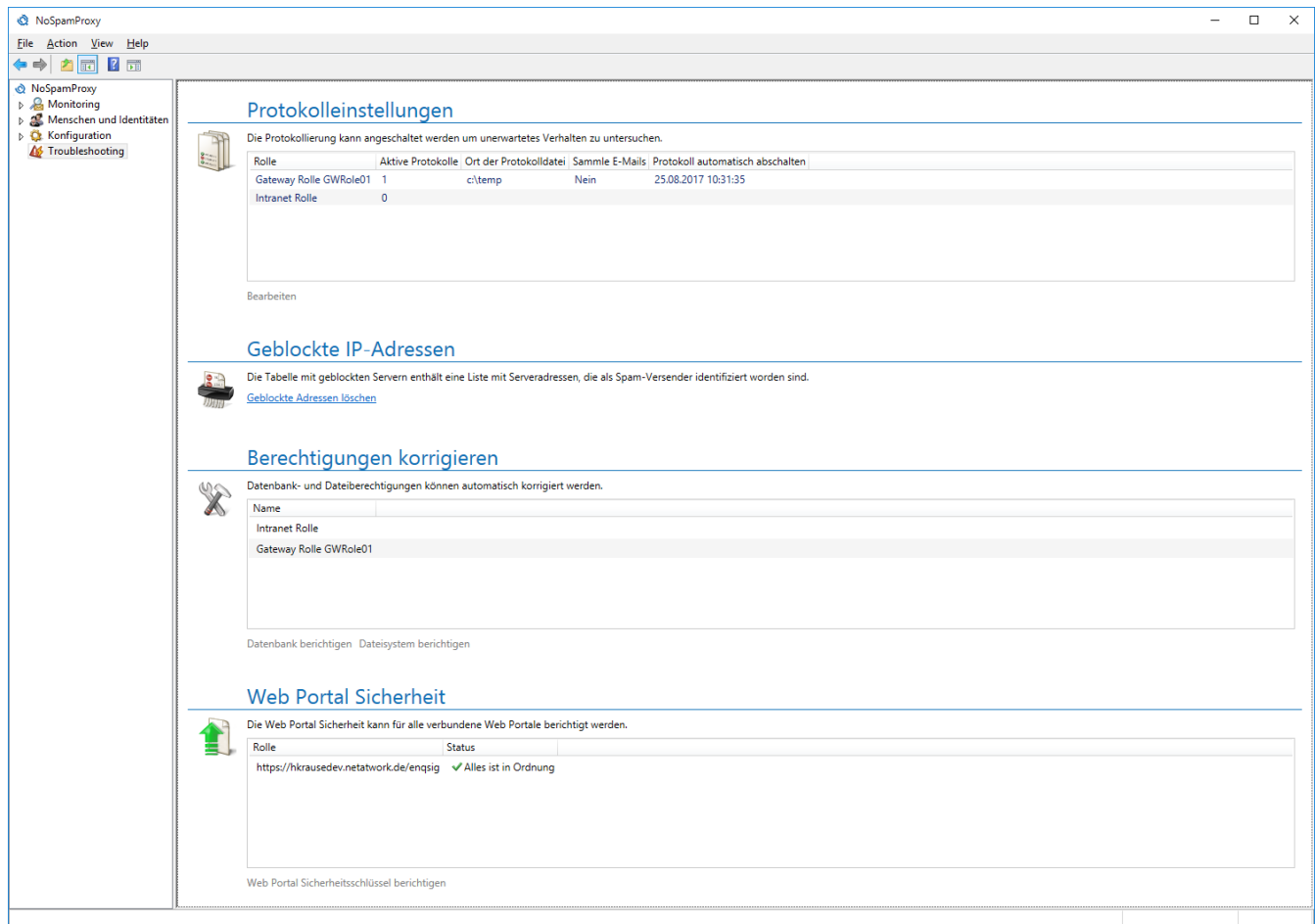


Bild 185: Werkzeuge für das Troubleshooting

Protokolleinstellungen

Konfigurieren Sie in der ersten Karteikarte den Speicherort für die Log-Dateien und wählen Sie die Kategorien, für die Sie die Protokollierung aktivieren möchten ([Bild 186](#)).



Je nachdem, welche Kategorien Sie hier auswählen, können die Logdateien sehr schnell mehrere hundert Megabytes groß werden. Wählen Sie für die Dateien ein Laufwerk, auf dem genug Speicherplatz frei ist.

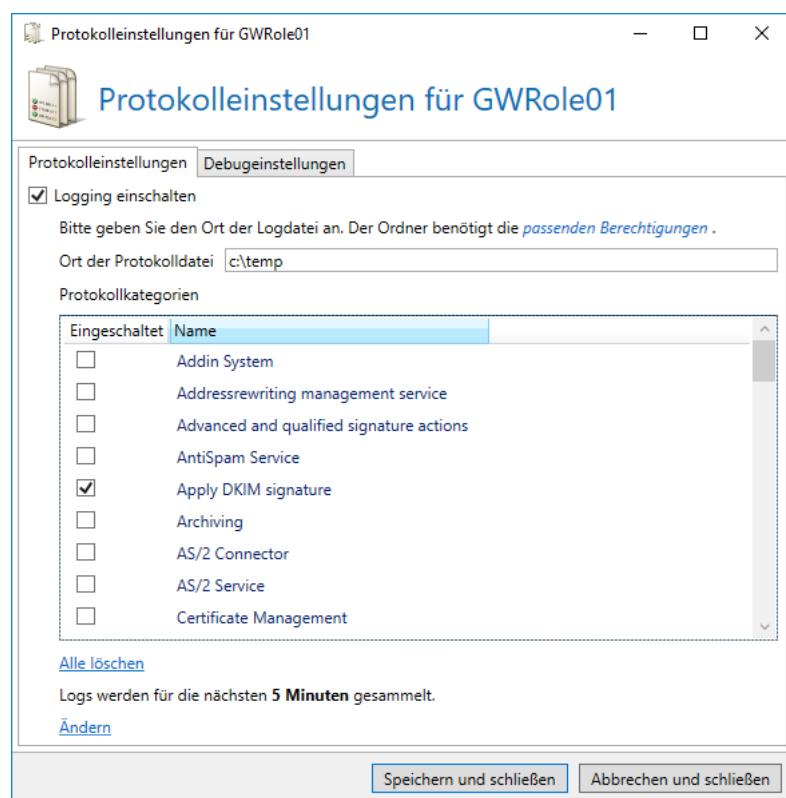


Bild 186: Konfigurieren Sie die Protokolleinstellungen

Zusätzlich ist es möglich, das Log auch nur für eine festgelegte Zeitspanne erstellen zu lassen ([Bild 187](#)). Nach dieser Zeit wird das Logging automatisch ausgeschaltet und Sie können die Logdateien für eine Analyse direkt benutzen.

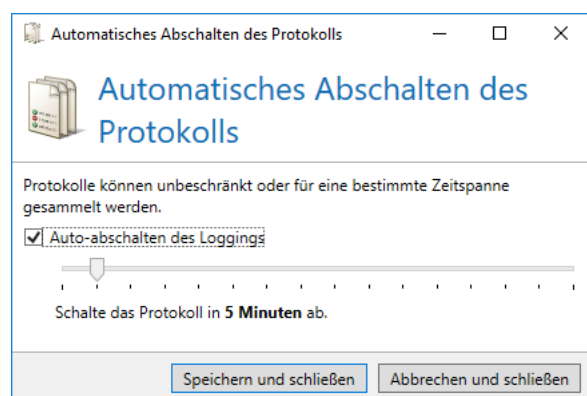


Bild 187: Automatisches Abschalten des Loggings

In der Karteikarte **Einstellungen zur Fehlersuche** können Sie zusätzlich alle E-Mails vor und nach der Bearbeitung durch NoSpamProxy auf die Festplatte schreiben lassen ([Bild 188](#)). Dieser Reiter ist nur bei Gateway Rollen vorhanden. Auf der Intranet Rolle können Sie dies nicht konfigurieren.

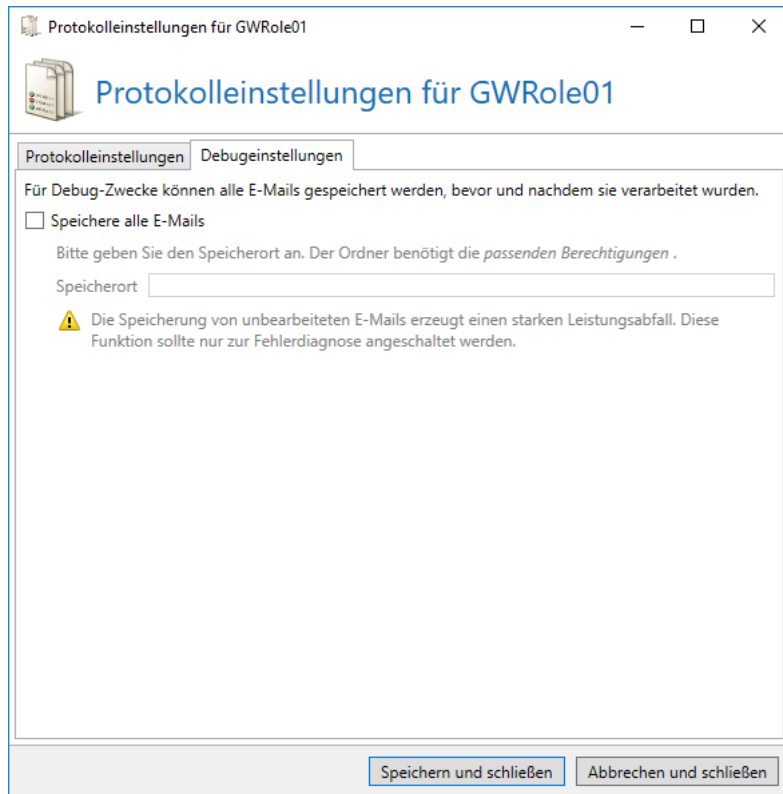


Bild 188: Speichern von E-Mails zur Fehlerdiagnose



Beachten Sie, dass die Speicherung aller E-Mails auf der Festplatte einen hohen Platzbedarf haben kann und starke Leistungseinbußen des Servers nach sich ziehen kann. Nutzen Sie diese Funktion deshalb nur zur Fehlerdiagnose und schalten Sie sie danach wieder ab.

Geblockte IP-Adressen

Wie bereits erwähnt, sperrt NoSpamProxy nach Erhalt einer Spam-E-Mail das einliefernde Gateway standardmäßig für 30 Minuten aus. Falls aus Versehen eine vertraute IP-Adresse in diese Blacklist aufgenommen wird, so können Sie hier die Liste der gesperrten Gateways löschen ([Bild 189](#)).

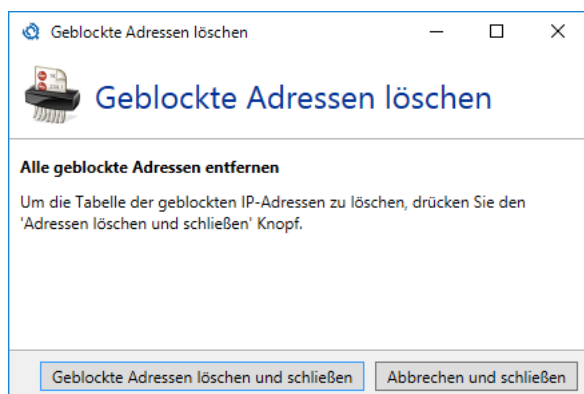


Bild 189: Löschen Sie gepblockte IP-Adressen über diesen Dialog

Berechtigungen korrigieren

Falls die Dateisystemberechtigungen Ihres NoSpamProxy durch z.B. Drittprogramme so verändert wurden, dass die Funktion eingeschränkt wird, können Sie das hier korrigieren. Es können Berechtigungen im Dateisystem ([Bild 190](#)) sowie auf der verwendeten Datenbank ([Bild 191](#)) korrigiert werden.

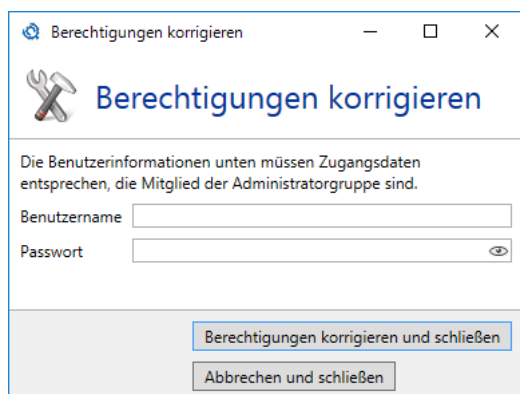
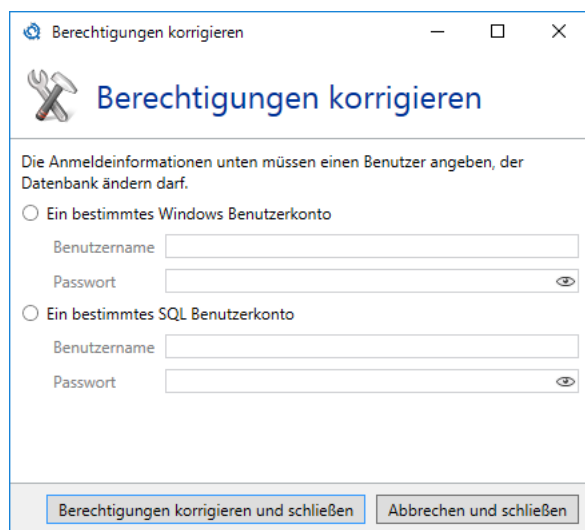


Bild 190: Lassen Sie Berechtigungen im Dateisystem korrigieren



Berechtigungen korrigieren

Berechtigungen korrigieren

Die Anmeldeinformationen unten müssen einen Benutzer angeben, der Datenbank ändern darf.

☐ Ein bestimmtes Windows Benutzerkonto

Benutzername

Passwort

☐ Ein bestimmtes SQL Benutzerkonto

Benutzername

Passwort

Berechtigungen korrigieren und schließen Abbrechen und schließen

Bild 191: Lassen Sie Berechtigungen in der Datenbank korrigieren

Web Portal Sicherheit

Für die Sicherheit aller installierten Web Portale müssen bestimmte Informationen synchron gehalten werden. Falls Sie mehrere Web Portale einsetzen, müssen nach der Installation des zweiten Web Portals diese Informationen synchronisiert werden. Solch ein Vorfall wird auf der Übersichtsseite angezeigt. Zusätzlich sehen Sie hier, welches Portal es betrifft.

Wählen Sie für alle Portale, die den Text anzeigen **Der Sicherheitsschlüssel ist falsch** die Funktion **Web Portal Sicherheitsschlüssel berichtigen**.

Solange die Schlüssel nicht synchron sind, werden die Formulare auf dem Web Portal Fehler anzeigen und in ihrer Funktion beeinträchtigt sein.

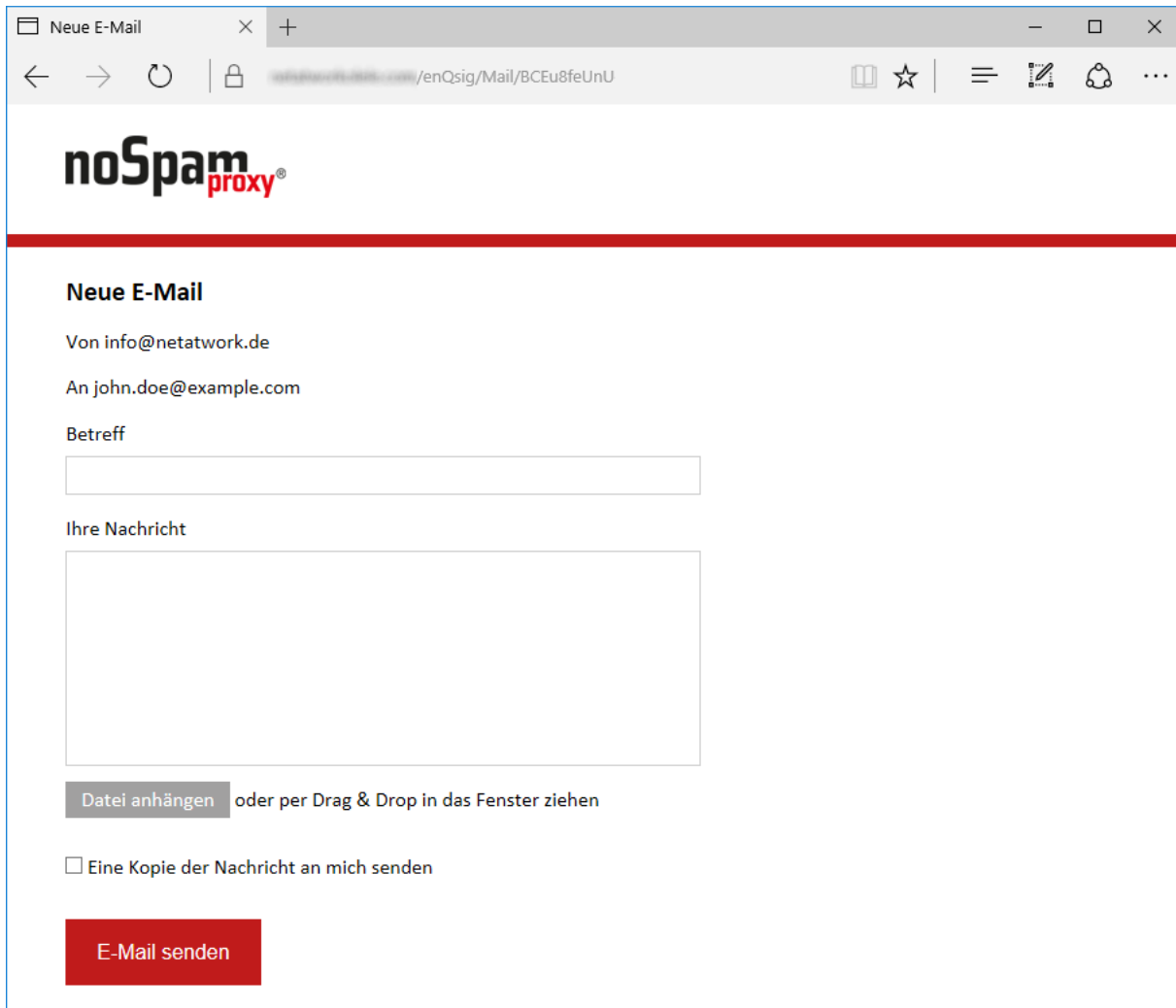
11. Das Web Portal

Das Web Portal ermöglicht Ihren Kommunikationspartnern das Übertragen großer Dateien an interne Benutzer. Für diese Funktion müssen die **Large Files** lizenziert sein.

Large Files

Wenn Sie die Funktion **Large Files** lizenziert haben, können Ihre Benutzer einem externen Kommunikationspartner die Möglichkeit geben, Ihnen Dateien zu übermitteln, die zu groß für die Übertragung per E-Mail sind. Der interne Benutzer schickt dafür über das Outlook Add-In einen Link an den Empfänger, den dieser dann verwenden kann, um Dateien zu übertragen.

Hat Ihr Kommunikationspartner eine Einladung für Large Files bekommen, so kann er über das Web Portal dem Absender auf sichere Art und Weise eine oder mehrere Dateien zukommen lassen ([Bild 192](#)).



The screenshot shows a web browser window with the address bar displaying 'https://nospam-proxy.com/enQsig/Mail/BCEu8feUnU'. The page features the 'noSpam proxy' logo at the top. Below the logo, the form is titled 'Neue E-Mail'. It contains the following fields and elements:

- 'Von info@netatwork.de' (Sender)
- 'An john.doe@example.com' (Recipient)
- 'Betreff' (Subject) with an empty text input field.
- 'Ihre Nachricht' (Your message) with a large empty text area.
- A button labeled 'Datei anhängen' (Attach file) followed by the text 'oder per Drag & Drop in das Fenster ziehen' (or drag & drop into the window).
- A checkbox labeled 'Eine Kopie der Nachricht an mich senden' (Send a copy of the message to me).
- A red button labeled 'E-Mail senden' (Send E-Mail).

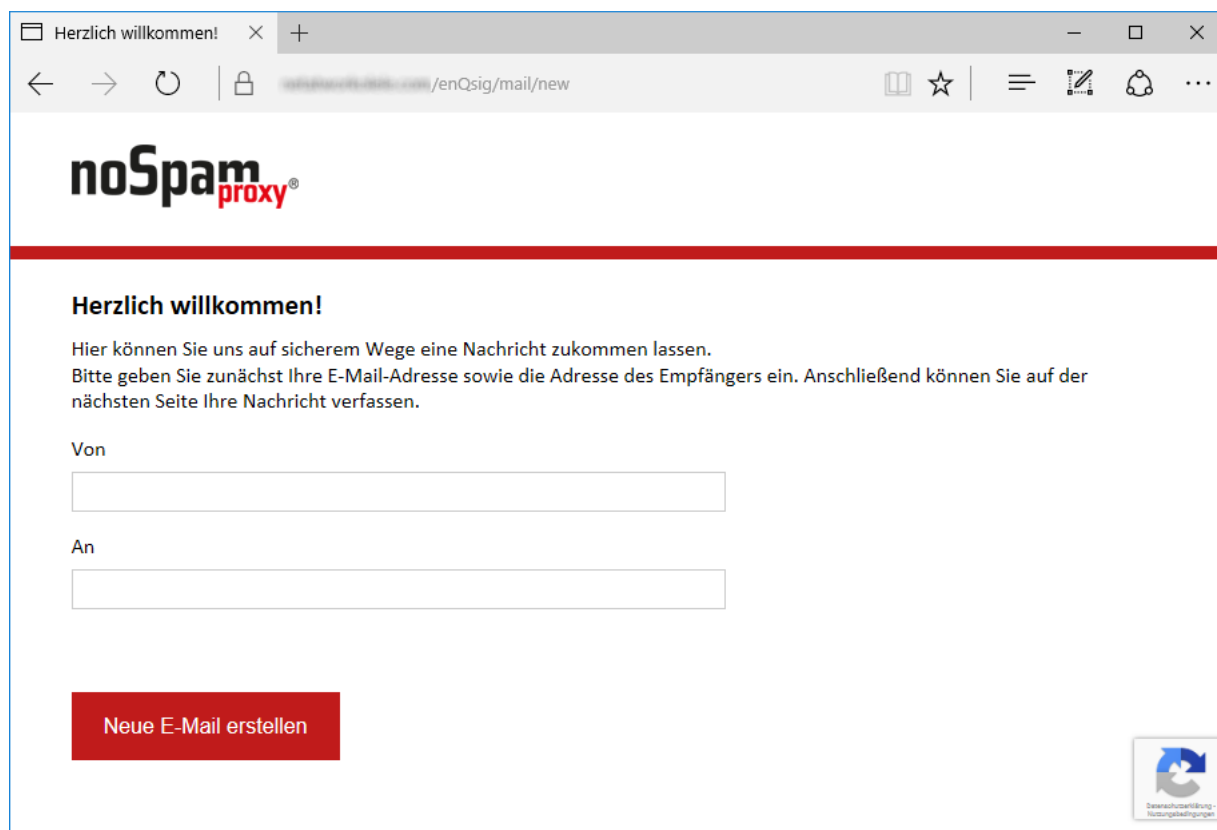
Bild 192: Dateien sicher übertragen über das Web Portal

Empfänger und Betreff sind festgelegt und können nicht geändert werden. Es ist dem Kommunikationspartner möglich, neben angehängten Dateien auch noch eine Nachricht zukommen zu lassen.

Je nach Konfiguration werden Dateien entweder direkt an die E-Mail angehängt oder den Empfängern über Large Files bereitgestellt. Die Schwellwerte hierfür - sowie die maximale Größe pro Anhang - können vom Administrator [festgelegt](#) werden.

Sichere E-Mails über das Web Portal ohne Einladung

Damit ein externer Kommunikationspartner jederzeit in der Lage ist, eine sichere E-Mail an Nutzer von NoSpamProxy zu senden, ist es möglich, das Web Portal auch ohne Einladung zu verwenden. Dabei muss der Partner nur seine E-Mail-Adresse und eine gültige Empfängeradresse angeben und gegebenenfalls ein Captcha lösen ([Bild 193](#)).



The screenshot shows a web browser window with the address bar displaying "https://www.noSpam-proxy.com/enQsig/mail/new". The page features the "noSpam proxy" logo at the top. Below the logo, a red horizontal bar separates the header from the main content. The main content area has the heading "Herzlich willkommen!" followed by a paragraph: "Hier können Sie uns auf sicherem Wege eine Nachricht zukommen lassen. Bitte geben Sie zunächst Ihre E-Mail-Adresse sowie die Adresse des Empfängers ein. Anschließend können Sie auf der nächsten Seite Ihre Nachricht verfassen." Below this text are two input fields: "Von" and "An". At the bottom left, there is a red button labeled "Neue E-Mail erstellen". At the bottom right, there is a small logo for "Datenschutzprüfung - Nutzungshinweise".

Herzlich willkommen!

Hier können Sie uns auf sicherem Wege eine Nachricht zukommen lassen.
Bitte geben Sie zunächst Ihre E-Mail-Adresse sowie die Adresse des Empfängers ein. Anschließend können Sie auf der nächsten Seite Ihre Nachricht verfassen.

Von

An

Neue E-Mail erstellen

Datenschutzprüfung - Nutzungshinweise

Bild 193: Maske für neue E-Mails ohne Einladungslink

Nach der erfolgreichen Validierung der Absender- und Empfängeradresse sowie des Captchas kann die E-Mail, wie in den vorherigen Kapiteln beschrieben, versandt werden.

12. Disclaimer



Für die Nutzung des Disclaimers in NoSpamProxy muss dieser lizenziert sein.

Die NoSpamProxy-Funktion **Disclaimer** bietet eine integrierte Möglichkeit, E-Mail-Disclaimer während des Versands in E-Mail einzufügen.

Die Disclaimer werden dabei über eine Webseite erstellt und konfiguriert, so dass die dafür zuständigen Mitarbeiter weder einen direkten Zugriff auf NoSpamProxy, die Verwaltungskonsole oder Ihren E-Mail-Server benötigen, noch ein spezielles Programm installiert haben müssen.

Öffnen Sie die Webseite mit dem Disclaimer indem Sie auf der [Übersichtsseite der Management Konsole](#) den Link **Disclaimer-Webseite öffnen** wählen.

Die Webseite gliedert sich nach einer beschreibenden Einstiegsseite in zwei Bereiche, **Vorlagen** und **Regeln**. Eine Vorlage bestimmt den HTML- und Nur-Text-Inhalt eines Disclaimers. Eine Regel bestimmt wann, wie und wo ein Vorlage an eine E-Mail hinzugefügt wird. Durch die flexiblen Kombinationen aus den erstellten Vorlagen und Regeln ist es möglich, einen Disclaimer aus einer oder mehreren Vorlagen zusammen zu bauen und in eine E-Mail einzufügen.

In den Inhalt einer Vorlage können auch Platzhalter eingefügt werden. Diese müssen vorher durch den NoSpamProxy Administrator bereit gestellt werden. Sie werden dann beim Versenden der E-Mail durch den im Benutzer hinterlegten Wert ersetzt. Zusammen können zum Beispiel Werte wie Namen, Telefonnummern und Abteilungen dynamisch eingefügt werden.

Bereitstellen von Platzhaltern

Für die Bearbeitung der Disclaimer muss der Administrator zuerst die benötigten **Zusätzlichen Benutzerfelder** erstellen, die als Platzhalter für den endgültigen Wert in eine Vorlage eingefügt werden können. Gehen Sie dazu in den Knoten **Zusätzliche Benutzerfelder** und legen Sie die benötigten Felder an ([Bild 194](#)).

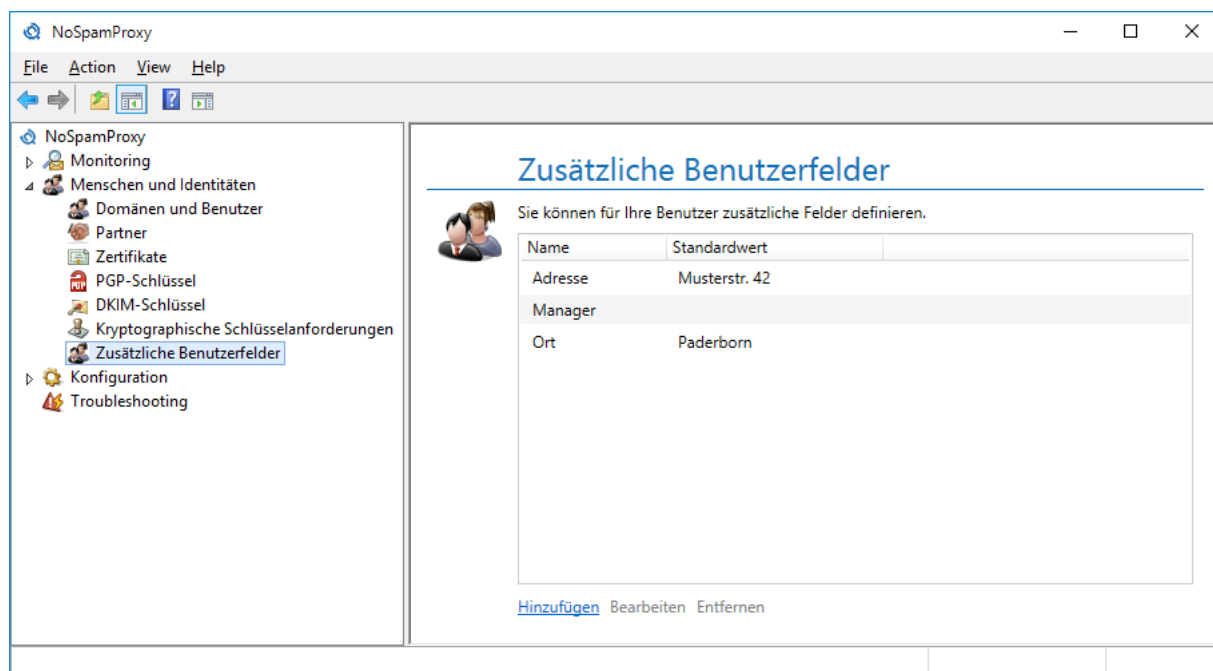


Bild 194: Die Übersicht über alle verfügbaren zusätzlichen Benutzerfelder

Für die meisten Anwendungsfälle ist es empfehlenswert, **Standardfelder erstellen** zu wählen. Dadurch werden die häufig benutzten Felder direkt in die Liste eingetragen. Beim Erstellen der Felder können zusätzlich auch die Zuordnungen der Benutzerfelder zu Active-Directory-Feldern in den bereits bestehenden Active-Directory-Benutzerimporten konfiguriert werden ([Bild 195](#)).

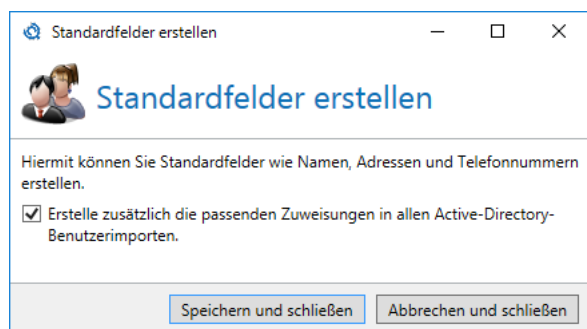


Bild 195: Das Erstellen von häufig genutzten Standardfeldern

Die erstellten Felder können an dieser Stelle optional mit Standardwerten belegt werden. Diese werden immer dann benutzt, wenn dem Benutzer keine eigenen Werte zugeordnet werden. In das Feld für die Telefonnummer kann zum Beispiel die Nummer der Zentrale eingetragen werden, in das Feld für die E-Mail-Adresse die E-Mail-Adresse der Zentrale etc.

Die erstellten Felder sind sofort in den manuell eingetragenen Unternehmensbenutzern sowie in den Active-Directory-Benutzerimporten verfügbar.

Zusätzliche Benutzerfelder im manuell eingetragene Benutzer

Öffnen Sie einen manuell eingetragenen Unternehmensbenutzer auf dem Knoten **Domänen und Benutzer**. Auf der Seite **Zusätzliche Benutzerfelder** sehen Sie die zuvor auf dem Knoten **Zusätzlichen Benutzerfelder** definierten Felder ([Bild 196](#)).

The screenshot shows a window titled 'Max Mustermann' with a user icon and name. Below the title bar, the section 'Zusätzliche Benutzerfelder' is displayed. A text block states: 'Sie können für jedes zusätzliche Benutzerfeld Werte festlegen. Diese Felder werden auf dem Knoten 'Zusätzliche Benutzerfelder' konfiguriert.' Below this is a table with two columns: 'Name' and 'Benutze Wert'.

Name	Benutze Wert
Adresse	Musterstr. 42 (Standard)
Manager	Christopher Musterschef
Ort	Paderborn (Standard)

At the bottom left of the table area is a link 'Bearbeiten'. At the bottom right are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

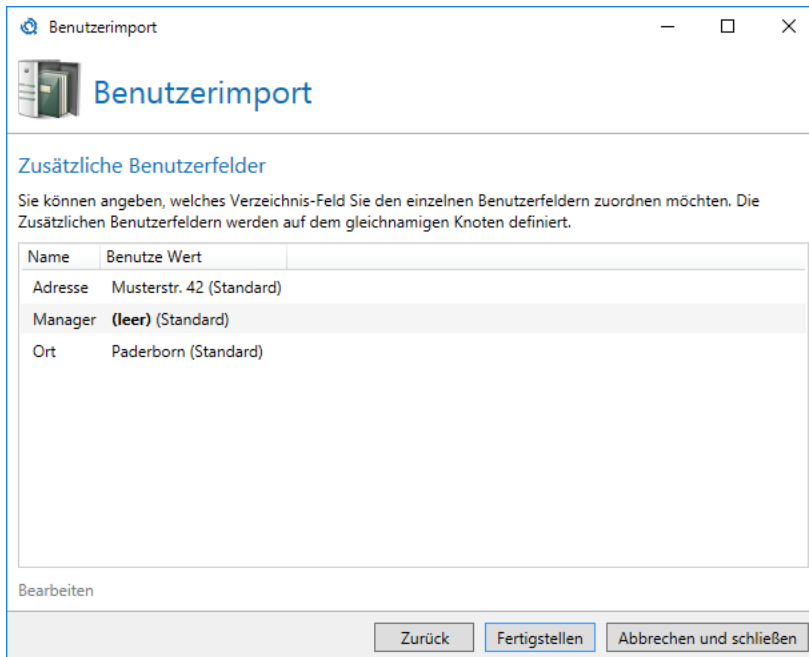
Bild 196: Zusätzliche Benutzerfelder

Für jedes Feld können sie entweder einen eigenen Wert setzen oder den Standardwert des Feldes übernehmen.

Zusätzliche Benutzerfelder im Benutzerimport

Bei dem Import aus einem Active Directory oder einem generischen LDAP-Verzeichnis können Sie zusätzliche Benutzerfelder mit Werten aus dem konfigurierten Verzeichnis füllen. Dies ist nützlich, wenn Sie Disclaimer-Vorlagen für Ihre Benutzer personalisieren möchten ([Bild 197](#)).

Definieren Sie zunächst im Knoten Zusätzliche Benutzerfelder eigene Felder oder erstellen Sie die Standard-Benutzerfelder. Anschließend können Sie in diesem Dialog für jedes Feld einstellen, aus welchem Feld des Verzeichnisses die Daten übernommen werden sollen.



Name	Benutze Wert
Adresse	Musterstr. 42 (Standard)
Manager	(leer) (Standard)
Ort	Paderborn (Standard)

Bild 197: Konfiguration zusätzlicher Benutzerfelder

Für jedes Feld können sie entweder einen Wert aus dem Active Directory zuordnen oder den Standardwert des Feldes übernehmen.



Die Werte, die Sie im Active-Directory-Benutzerimport zugeordnet haben, stehen erst beim nächsten Durchlauf dieses Benutzerimports zur Verfügung.

Benutzung der Felder im Disclaimer

Nachdem die Felder im Knoten **Zusätzliche Benutzerfelder** angelegt sind, können diese auf der Disclaimer-Website in den Vorlagen benutzt werden. Der Ersteller der Vorlagen sieht eine Liste mit den Namen der Felder, wenn er in einer Vorlage auf **Feld hinzufügen** klickt ([Bild 198](#)). Die Namen der Felder können - auch nachdem Sie bereits in Vorlagen verwendet werden - noch vom Administrator umbenannt werden, um zum Beispiel das Benutzererlebnis zu verbessern.

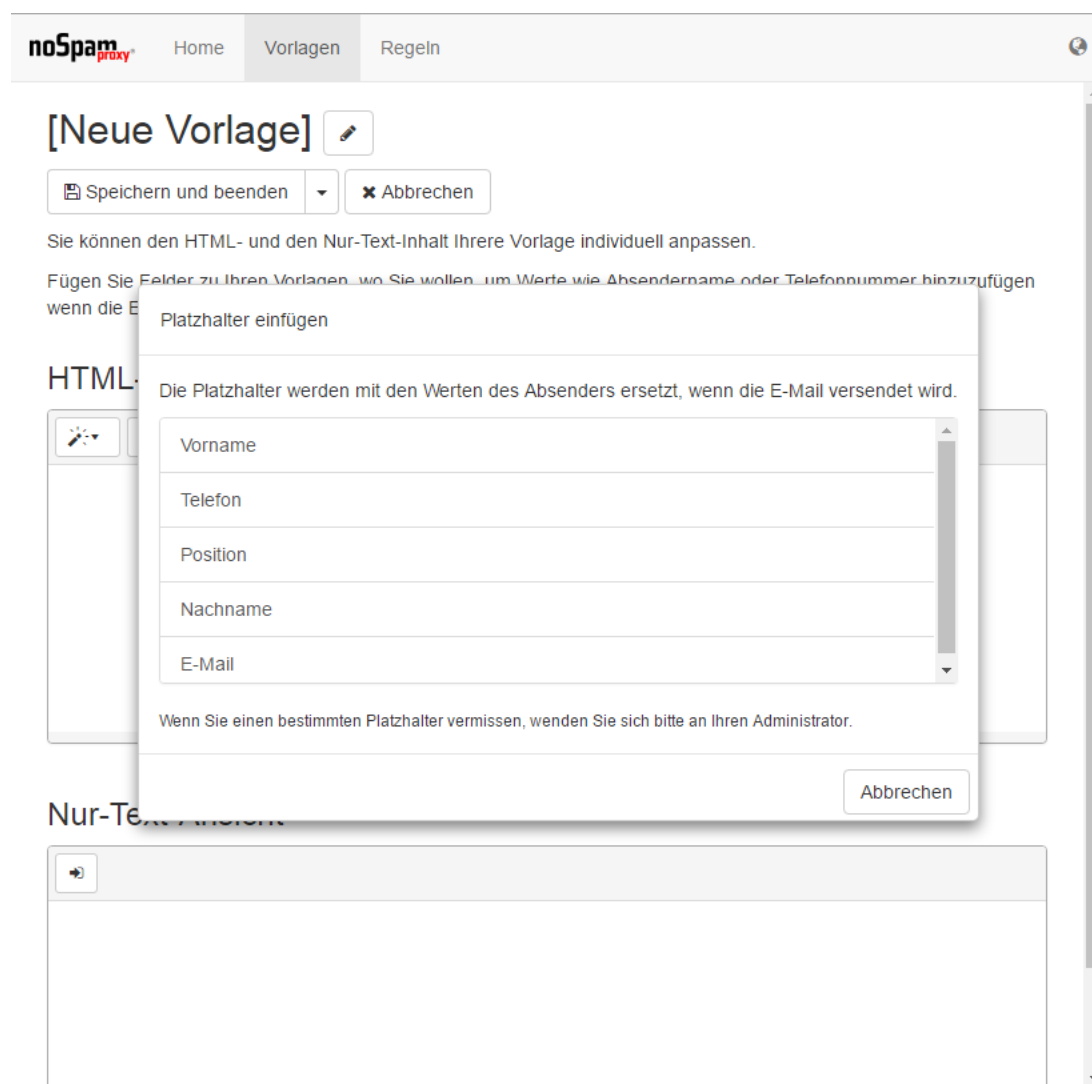


Bild 198: Die Auswahl aus der vom Administrator konfigurierten Liste der 'Zusätzlichen Benutzerfelder'

13. Anhang

Mehrfach verwendete Einstellungen in der Konfiguration

Einige Einstellungen werden in der Konfiguration mehrmals verwendet. Um die Lesbarkeit des Handbuchs zu erhöhen, werden diese hier ausführlich erläutert und bei der eigentlichen Verwendung in den unterschiedlichen Konfigurationen auf dieses Kapitel verwiesen. Dadurch werden immer wiederkehrende Erläuterungen vermieden.

Passwörter

Passwörter können in der Oberfläche auf folgende Arten ausgeführt sein:

- **Einfache Passworteingabe**
Die einfache Passworteingabe ist die häufigst verwendete Passworteingabe. Durch einen Klick auf das Auge können Sie das Passwort kurzzeitig sichtbar machen. Die Anzeige unterstützt bei der Eingabe sowie bei der Fehlersuche. Diese Eingabe wird bei allen Eingaben benutzt, bei denen der Administrator zuvor auch selbst das Passwort eingeben hat.
- **Doppelte Passworteingabe**
Bei der doppelten Passworteingabe muss zweimal dasselbe Passwort eingegeben werden. Die Eingabe wird bei sehr sensiblen Passwörtern verlangt, deren Falscheingabe unbedingt vermieden werden soll. Die doppelte Passworteingabe kann, wie die einfache Passworteingabe, durch einen Klick auf das Auge-Symbol eingesehen werden. Diese Eingabe wird z.B. beim Schutz der sensiblen Daten von NoSpamProxy verwendet.
- **Passworteingabe ohne spätere Ansicht**
Hier wird das Passwort nicht im Dialog angezeigt, sondern nur ein Hinweis, ob ein Passwort bereits eingegeben wurde oder nicht. Der Administrator kann das Passwort dann gegebenenfalls löschen oder auf einen neuen Wert setzen. Diese Art der Eingabe stellt sicher, dass durch Dritte eingegebene Passwörter nicht nach der Eingabe über die Oberfläche einsehbar sind. Um Schreibfehler zu vermeiden, wird die verdeckte Eingabe immer als doppelte Passworteingabe ausgeführt. Diese Eingabe wird z.B. in den Verschlüsselungspasswörtern der externen Partner verwendet.

Auswahl von Zertifikaten

Bei der Auswahl von Zertifikaten erscheint der Dialog mit dem Titel **Wählen Sie ein Zertifikat aus** ([Bild 199](#)).

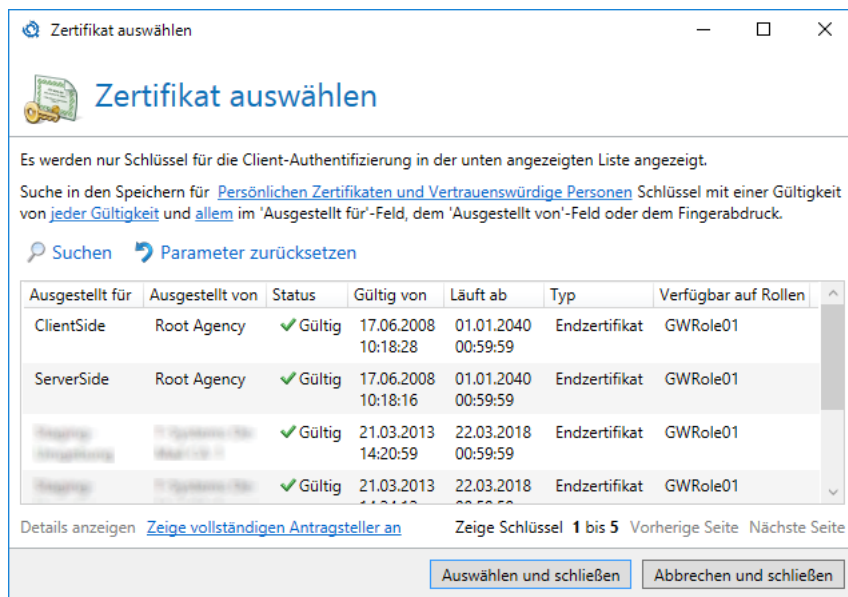


Bild 199: Die Liste der verfügbaren Zertifikate

Dabei werden Ihnen, je nach dem in welchem Bereich Sie diese Zertifikate auswählen möchten, Zertifikate für die folgenden Verwendungszwecke angezeigt.

- **E-Mail-Authentifizierung**
Ein Zertifikat, das dazu genutzt wird, den Versender einer E-Mail zu identifizieren.
- **Server-Authentifizierung**
Ein Zertifikat, das dazu benutzt wird, einen Server eindeutig zu identifizieren.
- **Client-Authentifizierung**
Ein Zertifikat, das dazu benutzt wird, einen Rechner, der sich mit einem Server verbinden will, eindeutig zu identifizieren.

Hier werden alle Zertifikate aus dem Zertifikatsspeicher der lokalen Maschine (die Maschine, auf der die zu konfigurierende Rolle läuft) angezeigt. Wählen Sie das gewünschte Zertifikat aus und klicken Sie danach auf **Auswählen und schließen** um das gewählte Zertifikat zu nutzen. Alternativ kontrollieren Sie vorher mit **Zertifikatsdetails anzeigen** alle Details des ausgewählten Zertifikats.



Einige Zertifikate, z.B. für De-Mail, sind durch identische Einträge im Feld **Ausgestellt für** schwer zu unterscheiden. Um diese Zertifikate zu unterscheiden, wählen Sie die Funktion **Zeige vollständigen Antragsteller an**. Dadurch wird der Antragstellernamen jedes Zertifikats ohne Kürzungen angezeigt.

Sicherung und Wiederherstellung

Um NoSpamProxy im Falle eines Systemausfalls wiederherzustellen, ist es notwendig, alle für den Betrieb notwendigen Daten regelmäßig zu sichern.

Betriebssystem, Treiber und Software

Die Sicherung des Windows Betriebssystems sollten Sie mit erprobten Programmen durchführen. Da NoSpamProxy sehr wenige Abhängigkeiten mit dem Betriebssystem selbst hat, ist es nach einem Ausfall auch möglich, den Ersatzserver frisch zu installieren. Wägen Sie daher ab, ob eine Neuinstallation des Betriebssystems und dessen Einstellungen und der Programme oder die Wiederherstellung der geeignete Weg ist.

Bei der Neuinstallation sollten Sie die bisher installierten Produkte und Einstellungen dokumentieren und die Datenträger vorhalten.

Weitere Informationen finden Sie in den Online Handbüchern und Anleitungen von Microsoft zu Windows Server und NTBACKUP.

Lizenzen von NoSpamProxy

Ihre Lizenz liegt als Datei auf dem Server im Verzeichnis

```
%ProgramData%\Net at Work Mail Gateway\Configuration\License.xml
```

und kann über ein normales Backup problemlos gesichert werden. Sie können die XML-Datei auch zusätzlich in einen sicheren Ordner kopieren. Die Datei ist auch im Betrieb nicht gesperrt und wird nicht beschrieben.

Konfigurationsdateien der Rollen

Die Konfiguration von NoSpamProxy wird in einer XML-Datei auf dem Server selbst gespeichert. Auch diese Datei kann mit einer handelsüblichen Backup Software ohne Probleme gesichert werden.

Allerdings schreibt das Gateway diese Datei bei Veränderungen der Konfiguration zurück, so dass hier ein Konflikt beim zeitgleichen Backup auftreten kann.

NoSpamProxy legt während des Schreibens der Konfiguration die neue Datei als temporäre Datei an, benennt die originale Datei in z.B. "GatewayRole.config.backup" und benennt erst danach die temporäre Datei in "GatewayRole.config" um. Bei einer normalen dateibasierten Sicherung haben Sie daher immer entweder die aktuellste Kopie oder die kurz zuvor geänderte Version der Konfiguration gesichert.

Es ist ratsam, auch vor größeren Änderungen an der Konfiguration diese Datei zu kopieren, um einfach zu dem vorherigen Stand zurückkehren zu können.

Die Konfigurationsdateien aller Rollen in der Standardkonfiguration werden nachfolgend aufgelistet. Sollten Sie NoSpamProxy in einem anderen Pfad installiert haben oder von einer früheren Version des NoSpamProxy das Programm aktualisiert haben, so muss der Pfad entsprechend angepasst werden.

- **Gateway Rolle**

```
%ProgramData%\Net at Work Mail Gateway\Configuration\GatewayRole.config
```

- **Intranet Rolle**

%ProgramData%\Net at Work Mail Gateway\Configuration\IntranetRole.config

- **ServerManagement Service**

%ProgramData%\Net at Work Mail Gateway\Configuration
\ManagementService.config

Datenbanken von NoSpamProxy

NoSpamProxy speichert die meisten Informationen in mehreren SQL-Datenbanken ab, die Sie ebenfalls sichern sollten. Die Rollen von NoSpamProxy verwenden dabei folgende Datenbanken:

- **Gateway Rolle**

NoSpamProxyDB

- **Intranet Rolle**

NoSpamProxyAddressSynchronization

- **Web Portal**

enQsigPortal

Wenn NoSpamProxy Ihren bestehenden Standard oder Enterprise SQL Server nutzt, können Sie dort mit dem Enterprise Manager eine periodische Sicherung aller Datenbanken konfigurieren. Beim Einsatz der SQL Server Express Edition müssen Sie manuell mit einem Skript die Datenbank sichern und bei Bedarf wieder herstellen.

Sichern Sie die Datenbanken über die Kommandozeile mit folgenden Befehlen:

Für die Datenbank der Gateway Rolle: `osql -S (local)\NoSpamProxyDB -E -Q "BACKUP DATABASE NoSpamProxyDB TO DISK = 'c:\NoSpamProxyDB.bak'"`

Für die Datenbank der Intranet Rolle: `osql -S (local)\NoSpamProxyAddressSynchronization -E -Q "BACKUP DATABASE NoSpamProxyAddressSynchronization TO DISK = 'c:\NoSpamProxyAddressSynchronization.bak'"`

Für die Datenbank des Web Portal: `osql -S (local)\enQsigPortal -E -Q "BACKUP DATABASE enQsigPortal TO DISK = 'c:\enQsigPortal.bak'"`

Diese Zeilen sichern die entsprechenden Datenbanken in Dateien, ohne die Datenbank dazu herunter zu fahren. Sie sollten daher prüfen, ob Sie einen entsprechend angepassten Aufruf mit der Windows Aufgabenplanung als regelmäßige Aufgabe einplanen.

Die Rücksicherung erfolgt mit folgenden Zeilen:

Für die Datenbank der Gateway Rolle: `osql -S (local)\NOSPAMPROXYDB -E -Q "RESTORE DATABASE NoSpamProxyDB FROM DISK = 'c:\nospamproxydb.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Für die Datenbank der Intranet Rolle: `osql -S (local)\NoSpamProxyAddressSynchronization -E -Q "RESTORE DATABASE NoSpamProxyAddressSynchronization FROM DISK = 'c:\NoSpamProxyAddressSynchronization.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Für die Datenbank des Web Portal: `osql -S (local)\enQsigPortal -E -Q "RESTORE DATABASE enQsigPortal FROM DISK = 'c:\enQsigPortal.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Die Datenbanken müssen für die Wiederherstellung aber schon bestehen.



Da der SQL-Server die Datenbanken selbst permanent geöffnet hält, können diese nicht über eine normale Sicherung der Dateien wie zum Beispiel über NTBACKUP erfasst werden.

Fehlersuche

NoSpamProxy beruht auf einer sehr einfachen Funktionsweise. Seine Implementierung als SMTP-Proxy verbindet die Vorteile dieses Prinzips mit der Einfachheit des Betriebs. Trotzdem kann es sein, dass das Gateway nach der Installation nicht so funktioniert, wie Sie es erwartet haben. Die häufigsten Fehler und Möglichkeiten zum Test beschreiben wir hier.

Support durch E-Mail

Unterstützung erhalten Sie unter der folgenden E-Mail-Adresse:

support@nospamproxy.de

Bitte fügen Sie folgende Informationen Ihrer E-Mail bei:

- **Ihre Kundennummer**
Wir erfassen und pflegen alle Supportfälle in einem Support-System. Ihre Kundennummer dient als Schlüssel, um Support-Anfragen eindeutig zuordnen zu können. Sie haben Ihre Kundennummer bei der Anforderung der Testlizenz oder dem Erwerb einer Lizenz erhalten. Sollte Sie Ihre Kundennummer nicht zur Hand haben, können Sie diese auch in der Lizenzdatei nachschlagen. Die Kundennummer, in unserem Beispiel die "C12345", liegt in einem mit "ContactNumber" benannten Bereich: `<field name="ContactNumber">C12345</field>` Sie können diese Nummer ebenfalls als Kundennummer angeben.
- **Die Konfiguration von NoSpamProxy**
Die Lage der Konfigurationsdateien im Dateisystem wird im Abschnitt [Konfigurationsdateien der Rollen](#) beschrieben. Bitte hängen Sie diese, vor allem aber die Konfigurationsdatei der Gateway Rolle, an die E-Mail für unser Support Team an.
- **Netzwerkplan und Ihre Planung**
Sofern Sie eine Beschreibung Ihrer Umgebung haben, hilft uns diese beim Verständnis, wie Sie NoSpamProxy nutzen wollen. Besonders interessant ist dabei Ihre SMTP-Domänen, die IP-Adressen des internen E-Mail-Servers und wie Sie Ihre E-Mails aus dem Internet erhalten und versenden. Auch Informationen über Firewalls in den Übertragungswegen sind sehr hilfreich.
- **Informationen über Ihre Internetanbindung**
Um NoSpamProxy einzusetzen, müssen Sie Ihre E-Mails per SMTP empfangen. Ein Zugriff von extern auf ihr System über Port 25/TCP muss daher möglich sein. Welche Komponenten stehen

zwischen dem Mail Gateway und dem Internet? Ein Router mit Port Filter und NAT oder eine vollwertige Firewall?

- **Informationen über den Server**

Welches Betriebssystem und Service Packs haben Sie installiert? Haben Sie Port-Filter oder eine Firewall auf dem Server aktiviert?

- **Fehlerbeschreibung**

Bitte beschreiben Sie möglichst genau, welchen Fehler Sie haben bzw. welche Funktion nicht gegeben ist.

Wir versuchen Ihnen schnellstens zu helfen. Bitte lesen Sie dennoch die folgenden Hinweise, um häufige Fehler zu erkennen und selbst zu beheben.

NoSpamProxy kontrollieren

Der erste Blick sollte der Management Oberfläche von NoSpamProxy gelten. Der Statusbildschirm auf der Übersichtsseite gibt Ihnen sehr schnell einen Überblick über ihr System. Sie können hier unmittelbar sehen, ob alle Einstellungen fehlerfrei eingetragen sind ([Bild 200](#)).

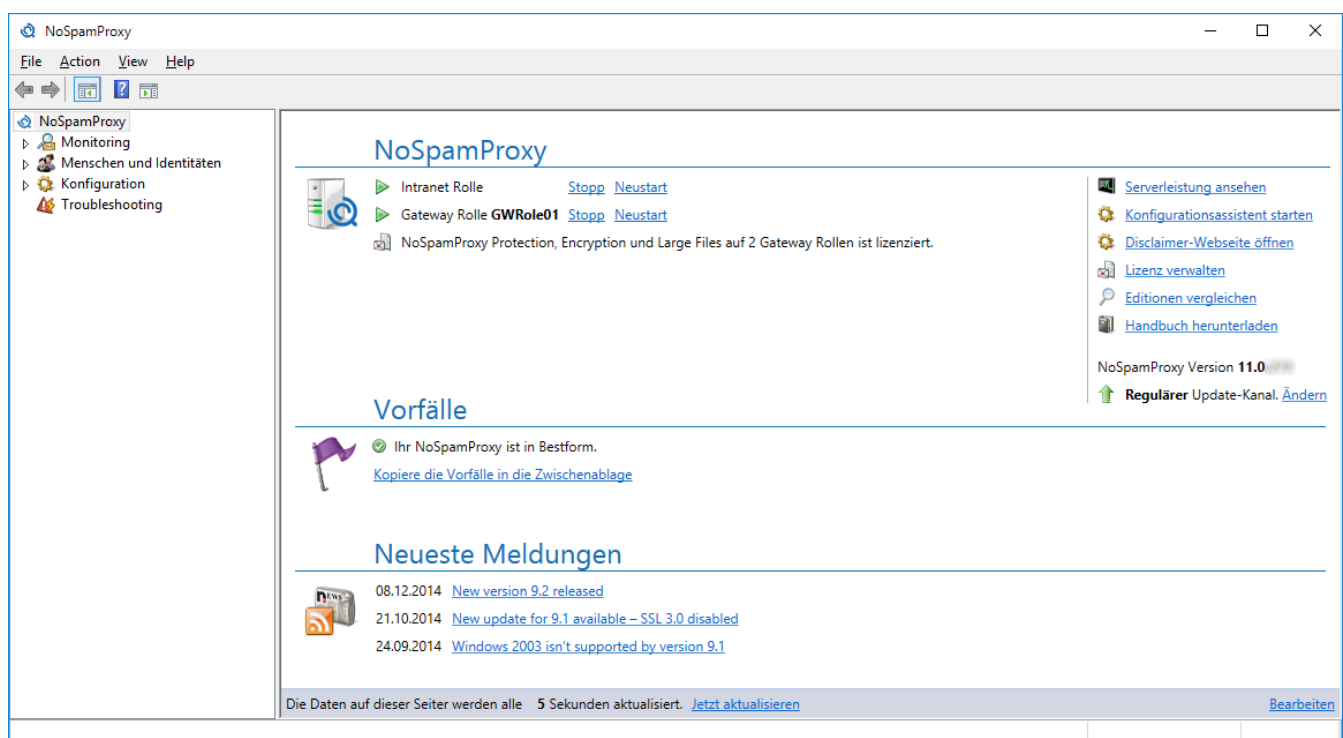


Bild 200: Die Übersicht zeigt eine vollständige Konfiguration von NoSpamProxy an

Kontrollieren Sie bitte die folgenden Punkte um Fehlerursachen zu finden.

- **Sind alle Rollen gestartet?**

Alle Rollen sollten den Status "gestartet" haben. Sie können die Rollen auch über die Oberfläche starten.

- **Werden Fehler angezeigt?**

Fehler in der Konfiguration einer Rolle werden in der Übersicht über NoSpamProxy angezeigt ([Bild 201](#)). Fehler sollten in einem vollständig konfigurierten Gateway immer beseitigt werden.

- **Werden Warnungen angezeigt?**

Warnungen sind ähnlich zu betrachten wie Fehler. Der Unterschied ist, dass Warnungen unter bestimmten Bedingungen durchaus auftreten können. Gehen Sie Warnungen genauso wie Fehlern auf den Grund und wägen Sie ab, ob die Warnung durch Ihre beabsichtigte Konfiguration von NoSpamProxy hervorgerufen wird oder besser behoben werden sollte.

- **IP-Adressen und Ports**

Kontrollieren Sie, ob die Gateway Rolle von NoSpamProxy auf den richtigen IP-Adressen und Ports Verbindungen annimmt.

- **Werden überhaupt E-Mails übertragen?**

Auf dem Statusschirm erkennen Sie die Anzahl der Verbindungen und übertragenen E-Mails als auch die Datenmenge. Stehen hier alle Werte auf 0, dann erhält NoSpamProxy keine E-Mails. Die gleichen Werte können Sie mit den Windows Leistungsindikatoren auslesen.

- **Meldungen im Ereignisprotokoll**

NoSpamProxy zeigt Ihnen in der Windows-Ereignisanzeige Fehlermeldungen, die seine Funktion behindern.

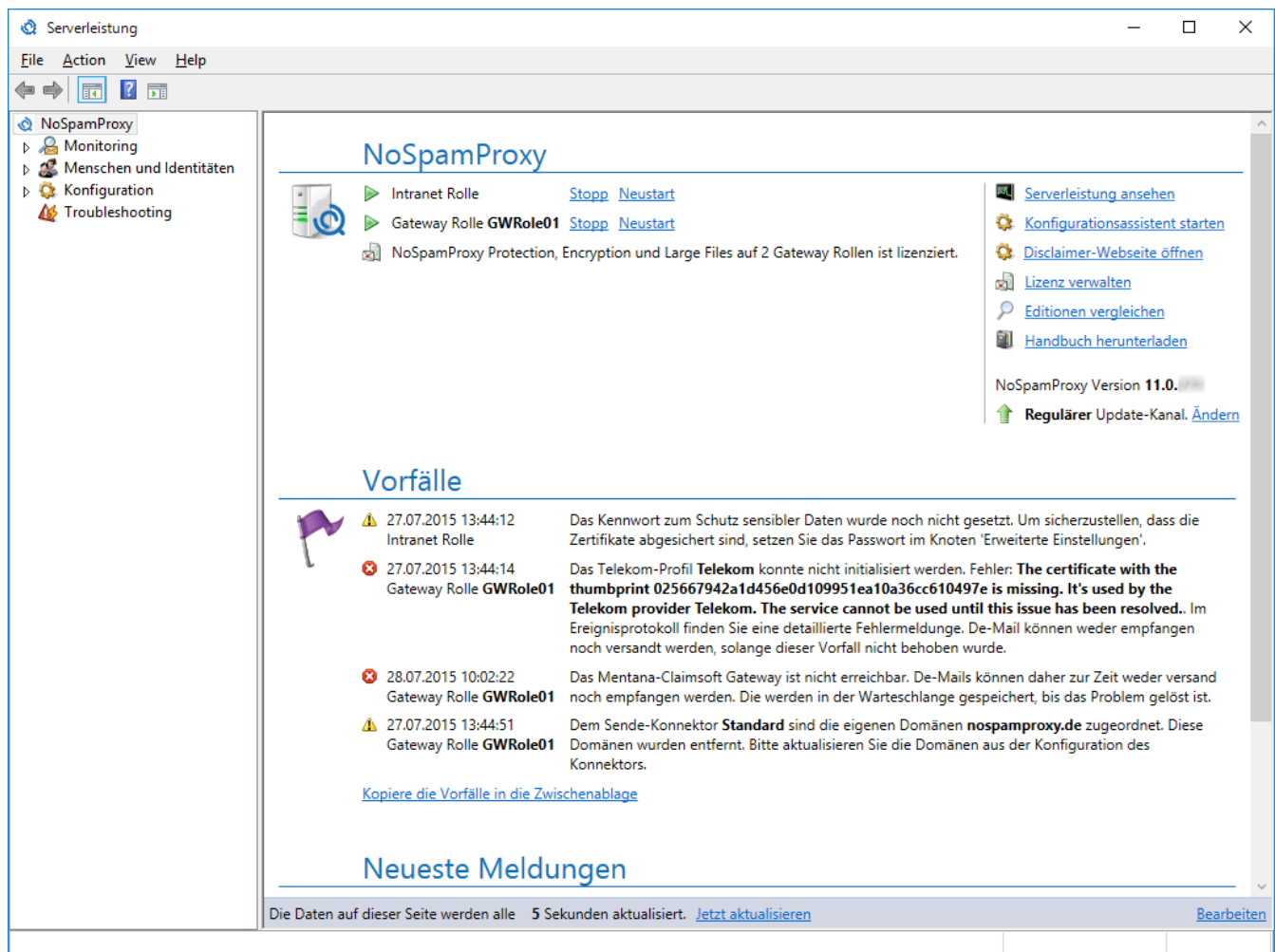


Bild 201: Fehler in den Konfigurationen von NoSpamProxy

NoSpamProxy testen

Die Basisfunktionen von NoSpamProxy lassen sich mit zwei Programmen testen, die ein Bestandteil von Windows sind:

- **TELNET**
Der Versand einer E-Mail per SMTP ist sehr einfach und kann mit TELNET auch von Hand erfolgen.
- **NSLOOKUP**
Dieses Programm dient zur Fehlersuche im Bereich der Namensauflösung. Das Mail Gateway nutzt DNS intensiv, z.B. um RBL-Listen abzufragen oder Zertifikate auf Gültigkeit zu überprüfen.

TELNET

Wenn ein E-Mail-Server eine E-Mail an einen anderen E-Mail-Server sendet, so erfolgt dies über TCP/IP über den Port 25. Diese Kommunikation können Sie mit TELNET auch manuell durchführen und dabei

sehr gut das Verhalten des entfernten E-Mail-Servers oder des eigenen NoSpamProxy testen. Eine E-Mail per SMTP senden Sie einfach mit dem Programm Telnet. Dazu starten Sie den Verbindungsaufbau mit:

```
TELNET name-des-mailserver 25
```

Der E-Mail-Server sollte danach mit einer 220-Meldung den Verbindungsaufbau bestätigen. An dieser Stelle sind Sie nun mit Ihrem E-Mail-Server verbunden und können wie folgt eine E-Mail versenden. Geben Sie dazu folgende Befehle, immer gefolgt von einem "Return" <CR>, ein. Warten Sie nach jedem Befehl auf die Bestätigung des E-Mail-Servers.

```
HELO name.des.absenderservers<CR>
```

```
MAIL FROM: mailadresse@absender.de<CR>
```

```
RCPT TO: mailadresse@zieldomäne.de<CR>
```

```
DATA<CR>
```

Ab nun geben Sie alles ohne weitere Rückmeldung des Servers ein:

```
Subject: Dies ist der Betreff<CR>
```

```
<CR>
```

```
Und hier ist der Body<CR>
```

```
. <CR>
```

Zum Abschluss enthält die letzte Zeile nur einen "Punkt". Damit wird das Ende der E-Mail gekennzeichnet und der E-Mail-Server bestätigt den erfolgreichen Empfang der E-Mail. Mit dem Befehl `QUIT` wird die Verbindung zum E-Mail-Server geschlossen.

NSLOOKUP

Das Programm NSLOOKUP ist das Hilfsmittel zur Kontrolle der DNS-Namensauflösung. Starten Sie NSLOOKUP einfach in einem DOS-Fenster mit den entsprechenden Optionen.

Beispiele:

```
nslookup -q=A www.microsoft.com
```

Sie erhalten die Liste der IP-Adressen, welche die Webseite von Microsoft betreiben.

```
nslookup -q=MX netatwork.de
```

Sie erhalten die E-Mail-Server, welche E-Mails für die Domäne `netatwork.de` annehmen.

```
nslookup -q=A
```

```
nslookup -q=A 3.4.5.80.dnsbl.sorbs.net
```

Sie erhalten von der Liste "Sorbs" die Information, dass dieser Servername die IP-Adresse 127.0.0.10 hat und damit auf der Liste der dynamischen IP-Adressen steht.

NSLOOKUP ist daher ein nützliches Hilfsmittel, um Fehler in der DNS-Konfiguration des Windows Server zu diagnostizieren.

Häufige Fehler und Ihre Ursachen

NoSpamProxy ist so entwickelt, dass nur die Schnittstellen gebunden und genutzt werden, die auch konfiguriert wurden. Gerade bei Systemen mit vielen Netzwerkkarten und IP-Adressen ist es daher wichtig, die Konfiguration gewissenhaft durchzuführen. Prüfen Sie daher folgende Einstellungen:

- **Port und IP-Adresse**
Stellen Sie sicher, dass NoSpamProxy wirklich auf den Adressen Verbindungen annimmt, die Sie ihm zugedacht haben. Vielleicht liegt nur ein Zahlendreher in der Konfiguration vor?
- **Telnet auf 127.0.0.1 Port 25 geht nicht**
Beachten Sie hier, dass NoSpamProxy nicht auf der localhost-Adresse arbeitet, wenn Sie den Dienst auf eine spezifische IP-Adresse gebunden haben.
- **Firewall**
Gibt es auf dem Server eine Firewall oder einen Port-Filter, die eine Verbindung zu NoSpamProxy auf TCP/IP-Ebene verhindern? Testen Sie die Erreichbarkeit von NoSpamProxy auf dem Server selbst mit einem TELNET Befehl auf die IP-Adresse. Damit schließen Sie eine externe Firewall testweise aus.
- **Andere Dienste?**
NoSpamProxy versucht beim Start die angegebenen Schnittstellen einzubinden. Dies ist nicht möglich, wenn bereits ein anderes Programm die entsprechenden Schnittstellen eingebunden hat. Das Gateway zeigt dieses als Fehlermeldungen in der Ereignisanzeige und im Statusbild an.

NoSpamProxy Protection filtert nicht

Wenn NoSpamProxy Protection korrekt installiert ist und E-Mails zwar durchgeleitet, aber keine blockiert werden, so kontrollieren Sie bitte folgendes:

- **Lizenz installiert**
Wenn NoSpamProxy Protection keine gültige Lizenz findet, dann werden alle Verbindungen auf "Durchreichen" gestellt, d.h. die E-Mails werden ohne weitere Beachtung der Regeln durchgelassen.
- **Regeln**
Kontrollieren Sie, ob Ihre Regeln Ihren Anforderungen entsprechen und die Filter und Grenzen passend eingestellt sind. Die Entscheidung "Durchreichen" lässt alle E-Mails dieser Regel passieren. Auch die Reihenfolge der Regeln ist wichtig. Die Regeln werden sequentiell abgearbeitet. Die erste zutreffende Regel wird abgearbeitet und alle anderen werden nicht beachtet. Zum Testen empfiehlt es sich z. B. eine Regel am Anfang der Regelliste zu definieren, die E-Mails an eine bestimmte E-Mail-Adresse abweisen. Dieses könnte man z.B. mit der richtigen Einstellung im Reiter "Kriterien" erreichen. Eine Test-E-Mail an diesen Empfänger muss von NoSpamProxy Protection abgelehnt werden. Wenn dies erfolgt, dann landet die IP-Adresse des Testsystems in der Blacklist und Sie wissen, dass NoSpamProxy Protection im Prinzip schon funktioniert. Allerdings müssen Sie nun Ihr Regelwerk noch einmal genauer untersuchen.

- **E-Mail Nachrichtenverfolgung**

Detaillierte Informationen zum Ablauf einer E-Mail bietet Ihnen die Nachrichtenverfolgung. Jede E-Mail, die durch NoSpamProxy Protection verarbeitet wurde, ist in der Nachrichtenverfolgung zu finden. Dort finden Sie auch sehr einfach die Regel und die Filter bzw. Aktionen, die auf einer E-Mail angewendet wurde, inklusive der Bewertung. Im Falle eines Fehlverhaltens oder Eintreffen eines "False Positive"-Ereignisses bezüglich der E-Mail-Abwicklung durch NoSpamProxy Protection, sollten sich in der Nachrichtenverfolgung ausreichende Hinweise diesbezüglich befinden.

NoSpamProxy lehnt alle E-Mails an lokale Adressen ab

NoSpamProxy verhindert die unautorisierte Weiterleitung von E-Mails (Relaying) und ist sehr gut gegen Missbrauch von außen als auch von innen geschützt. Dies bedeutet aber, dass Sie, ähnlich wie bei einer Firewall, genau die Funktionen erst frei schalten müssen, die Sie benötigen. Dazu gehören zwingend zwei Einstellungen:

- **Lokale E-Mail-Domänen**

Sie müssen in dem Gateway die Liste der Domänen pflegen, die Sie intern betreiben. Anhand der Standardregeln nimmt es von extern nur E-Mails für diese Domänen an. Haben Sie hier keine Domänen gepflegt, so nimmt das Gateway keine E-Mails von extern an. **Ausnahme:** Sie haben die Standardregeln verändert, so dass dieser Schutz nicht mehr gewährleistet wird.

- **Lokale E-Mail-Server**

Damit E-Mails an externe Adressen durch NoSpamProxy zugestellt werden können, müssen alle E-Mail-Server, von denen das Gateway E-Mails weiterleiten soll, in die Liste der lokalen E-Mail-Server eingetragen werden. Fehlen E-Mail-Server in der Liste, ist es nicht möglich von diesen Servern E-Mails weiter zu leiten.

Lehnt NoSpamProxy externe E-Mails ab, erstellt der sendende E-Mail-Server eine Unzustellbarkeitsmeldung. Sie selbst können mit der TELNET-Testmethode ebenfalls eine E-Mail von extern an das Gateway übermitteln und die Meldung von NoSpamProxy ablesen, die den Grund für die Ablehnung nennt. Des Weiteren bietet Ihnen auch hier die Nachrichtenverfolgung ein hilfreiches Werkzeug zur Fehlereinkreisung.

SQL-Datenbank steht nicht zur Verfügung

Wenn Sie in den Regeln als Empfängerkriterium die Unternehmensbenutzer ausgewählt haben, damit E-Mails an ungültige E-Mail-Adressen abgewiesen werden, lehnt NoSpamProxy die E-Mail temporär ab, sobald er auf die SQL-Tabelle nicht zugreifen kann. Stellen Sie sicher, dass der SQL-Server Dienst ordnungsgemäß gestartet ist und das Gateway fehlerfrei auf die Datenbank zugreifen kann. Fehlermeldungen finden Sie unter anderem in der Ereignisanzeige von NoSpamProxy und in der Übersichtseite.

NoSpamProxy Protection findet keine Viren

NoSpamProxy Protection kann sowohl alle E-Mails auf virenverseuchte Anhänge prüfen und je nach Einstellung die komplette E-Mail ablehnen oder nur die Anhänge entfernen. Damit NoSpamProxy Protection E-Mails mit Anhängen auf Viren überprüfen kann, müssen zwei Faktoren erfüllt sein:

- **Installierter Virens Scanner**

Auf dem Server von NoSpamProxy Protection muss ein beliebiger Virenschanner installiert sein, der in Echtzeit die Zugriffe auf das Dateisystem überwacht und den Versuch, eine virenverseuchte Datei abzuspeichern, unterbindet.

- **Aktion 'Dateibasierter Virenschanner' muss eingebunden sein**

Diese Aktion ist standardmäßig nicht mit eingebunden, da diese Aktion nur in Verbindung mit einem installierten Virenschanner einen Sinn ergibt. Beachten Sie, dass NoSpamProxy Protection nicht feststellen kann, ob ein Virenschanner installiert ist. Um die Funktion eines Virenschutzes zu nutzen, müssen Sie daher einen dateibasierten Virenschanner installieren und dann die Aktion in die entsprechenden Regeln einbinden. Die Funktion des dateibasierten Virenschanners können Sie prüfen, in dem Sie den EICAR-Testvirus über die Seite <http://www.eicar.com/> herunterladen oder sich zusenden lassen.

Smartcard nicht per RDP verwaltbar

Wenn Sie Zertifikate von einer Smartcard einsetzen, können Sie die Smartcard in einer RDP-Sitzung nicht verwalten. Das funktioniert nur in einer Sitzung direkt auf dem Host. In virtuellen Umgebungen basierend auf Hyper-V muss zum Beispiel der SCVMM Admin benutzt werden, in VMware Umgebungen der VMware Admin.

Exchange-Management-Konsole startet nicht mehr

Wenn NoSpamProxy und Exchange 2010 auf demselben Server installiert sind, funktioniert die Exchange-Management-Konsole nicht mehr ordnungsgemäß. Der Grund hierfür ist das .NET Framework 4.6.2. Die Exchange-Management-Konsole benötigt das .NET Framework in der Version 2.0, die NoSpamProxy Management-Konsole hingegen arbeitet ausschließlich mit der Version 4.6.2.

Damit standardmäßig die richtige .NET Framework Version verwendet wird, legt NoSpamProxy eine Umgebungsvariable mit dem Namen `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` an. Diese Variable verweist auf einen Pfad, in dem eine Konfigurationsdatei mit den entsprechenden Einstellungen gespeichert ist. Beim Aufruf jeglicher Management-Konsole wird die entsprechende Variable, und somit die Konfigurationsdatei, verwendet. Beim Öffnen der Exchange MMC verursacht dies die bekannten Probleme. Um die Exchange MMC wieder benutzen zu können, gibt es nur den folgenden Workaround: Die Umgebungsvariable wird dauerhaft gelöscht und die NoSpamProxy MMC muss über eine Batchdatei aufgerufen werden, in der die notwendigen Umgebungsvariable vorher definiert wird. Der Vorteil ist, dass die Umgebungsvariable in diesem Fall nur für Programme angewendet wird, die aus dem Kontext der Batchdatei aufgerufen werden.

Öffnen Sie über `Start -> Ausführen -> sysdm.cpl` die 'Erweiterten Systemeinstellungen' ([Bild 202](#)). Wählen Sie in der Karteikarte **Erweitert / Advanced** die Schaltfläche **Umgebungsvariablen... / Environment Variables...**

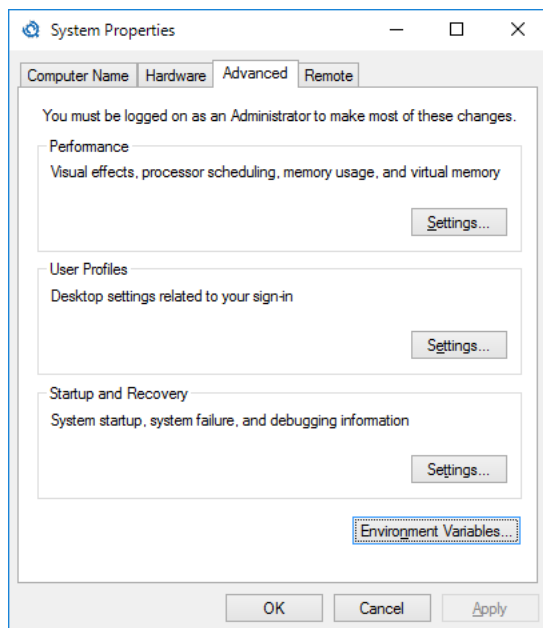


Bild 202: Die erweiterten Systemeinstellungen

Es öffnet sich das Fenster mit den 'Umgebungsvariablen' ([Bild 203](#)).

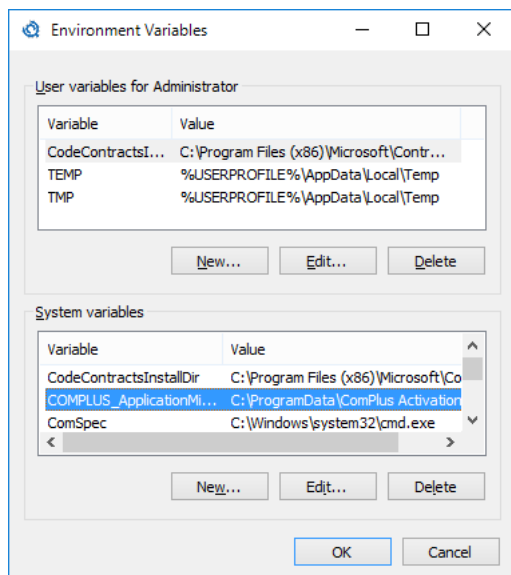


Bild 203: Die Umgebungsvariablen des Systems und des angemeldeten Benutzers

Wählen Sie im Abschnitt **Systemvariablen** den Eintrag `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` aus und klicken anschließend auf **Bearbeiten / Edit**. Kopieren Sie sich den Pfad, der im Feld **Wert / Value** steht, in

die Zwischenablage. Anschließend löschen Sie den kompletten Eintrag. Schließen Sie die beiden offenen Dialoge jeweils mit **OK**. Öffnen Sie nun Notepad. Fügen Sie den gerade kopierten Pfad aus der Zwischenablage in Notepad ein. Zusätzlich fügen Sie bitte folgende Zeilen dazu (kopieren sie den folgenden Text hintereinander, ohne zusätzliche Leerschritte, in eine Zeile):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```

Kopieren Sie den Pfad aus der Zwischenablage hinter die erste Zeile ein. Die Notepad-Datei sollte dann sinngemäß wie folgt aufgebaut sein (kopieren sie den folgenden Text hintereinander, ohne zusätzliche Leerschritte, in eine Zeile):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=C:\
ProgramData\ComPlus Activation Configurations\mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```



Bitte beachten Sie, dass die Darstellung der Batch-Datei durch automatische Zeilenumbrüche verfälscht wird. Der Befehl muss in einer Zeile stehen.

Passen Sie zum Schluss gegebenenfalls den Pfad zur MSC-Datei der Management Console an und speichern Sie anschließend den Notepad-Inhalt als NoSpamProxy-MMC.bat. Wenn Sie die Batch-Datei aufrufen, sollte sich die NoSpamProxy MMC erfolgreich öffnen lassen. Ab Windows 2008 mit aktiviertem UAC müssen Sie die Batchdatei jedoch stets als Administrator ausführen. Die Exchange MMC sollte sich nun ebenfalls fehlerfrei öffnen lassen.

Kontrolle der Verbindungen

NoSpamProxy arbeitet allein als SMTP-Proxy und in dieser Funktion ist NoSpamProxy auf die Erreichbarkeit der E-Mail-Server angewiesen. Es gibt mehrere Faktoren, die eine Erreichbarkeit des Gateway oder der E-Mail-Server verhindern. Ursachen könnten sein:

- **Fehlende Namensauflösung**
NoSpamProxy nutzt je nach Einstellung die angegebene IP-Adresse oder den Servernamen der E-Mail-Server. Wird der Servername angegeben, so muss dieser über DNS auflösbar sein.
- **Falsch konfigurierte E-Mail-Server**
Stellen Sie sicher, dass die E-Mail-Server auch Verbindungen von NoSpamProxy annehmen. Gerade bei der Umstellung auf NoSpamProxy kann es passieren, dass der E-Mail-Server nur E-Mails von dem bisherigen System annimmt. Des Weiteren muss beim E-Mail-Smarthost für externe Adressen sichergestellt sein, dass das Gateway diesen Smarthost als Relay benutzen darf.
- **Verbaute Wege**
Prüfen Sie, ob der NoSpamProxy die Verbindung zu den anderen E-Mail-Servern aufbauen kann oder ob eine Firewall auf dem NoSpamProxy Server, dem Zielsystem oder auf dem Weg dorthin eine Verbindung verhindert.

Um die Verbindung zu anderen Servern zu kontrollieren, können Sie das bereits beschriebene Programm [Telnet](#) nutzen. Folgende vier Tests sind durchführbar:

- **Simulation: NoSpamProxy zu internem E-Mail-Server**
Starten Sie auf dem Server von NoSpamProxy das Programm `TELNET ip-adresse-des-internen-mailservers 25`. Ihr interner E-Mail-Server muss sich melden. Ist dies nicht der Fall, so müssen Sie die Netzwerkverbindung, Firewall-Regeln und den internen E-Mail-Server prüfen. Solange sich NoSpamProxy nicht mit diesem internen E-Mail-Server verbinden kann, wird es auch keine Verbindung von Extern annehmen.
- **Simulation von extern**
Starten Sie auf NoSpamProxy eine TELNET-Verbindung auf die als extern angegebene IP-Adresse des Servers und erstellen Sie eine E-Mail. NoSpamProxy muss diese Verbindung als "von extern" erkennen. Sobald Sie den Envelope (HELO, MAIL FROM, RCPT TO, DATA) eingegeben haben, wird das Gateway die bisher ermittelten Daten prüfen und dann eine Verbindung zum internen E-Mail-Server aufbauen. Dies können Sie z. B. auch im Statusüberblick von NoSpamProxy sehen.
- **Weitergabe nach extern**
Analog zur Verbindung an lokale Server muss NoSpamProxy auch E-Mails an externe Adressen über einen E-Mail-Server versenden. Kontrollieren Sie mit `TELNET zielserver 25`, ob dieser Server von NoSpamProxy erreichbar ist und E-Mails annimmt. Dieser E-Mail-Server muss NoSpamProxy erlauben, E-Mails in das Internet zu versenden, d.h. diesen Server als Relay zu nutzen. Ist dieser Server nicht erreichbar, so nimmt NoSpamProxy keine Verbindungen mehr von intern an.
- **Verbindung von Intern**
Dieser Test wird von Ihrem internen E-Mail-Server aus durchgeführt. Starten Sie hier `TELNET IP-Adresse-von-NoSpamProxy 25`. Diesmal muss sich NoSpamProxy melden und Ihre Testdaten annehmen.

Leistungsindikatoren

Die Leistungsindikatoren sind ein sehr vielseitiges Mittel, um Funktionen von NoSpamProxy in Echtzeit zu prüfen. Alle Leistungsindikatoren werden nicht über die Management Konsolen Oberfläche angezeigt, sondern sind über das Windows Programm "Zuverlässigkeits- und Leistungsüberwachung" ("perfmon.exe") einsehbar. Dadurch können Sie die Arbeit von NoSpamProxy, genau wie die Ihres Betriebssystems, überwachen. Dieses kann auch automatisiert durch eine weitere Software, wie zum Beispiel den Microsoft System Center Operations Manager, geschehen. Sie können beispielsweise nachsehen, wie oft E-Mails mit einem bestimmten Schwellenwert (SCL) geblockt wurden oder welches Datenvolumen die E-Mails aufweisen.



Die Leistungsindikatoren werden - bis auf wenige Ausnahmen - im "Serverleistung" Knoten, nicht in der Oberfläche angezeigt. Sie dienen eher zur automatischen Überwachung von NoSpamProxy durch Softwareprodukte Dritter.

Die für NoSpamProxy zur Verfügung stehenden Werte sind unten aufgeführt. Die Namen der Leistungsindikatoren sind, unabhängig von der gewählten Sprache des Betriebssystems oder der von NoSpamProxy, immer in englischer Sprache.

NoSpamProxy Globals

- Accepted mails
- Blocked connections
- Delivery failures
- Rejected at envelope level
- Rejected at body level

NoSpamProxy Network Utilization

- Bytes Sent
- Bytes Received
- Active inbound connections
- Active outbound connections

NoSpamProxy Assigned Spam Confidence Levels

- SCL lower than 0
- SCL between 0 and 0.9
- SCL between 1 and 1.9
- SCL between 2 and 2.9
- SCL between 3 and 3.9
- SCL between 4 and 4.9
- SCL between 5 and 5.9
- SCL between 6 and 6.9
- SCL between 7 and 7.9
- SCL between 8 and 8.9
- SCL between 9 and 10

NoSpamProxy Actions

- Number of times run
- Permanently blocked
- Temporarily blocked
- Active outbound connections

NoSpamProxy Performance

- Average Response Time

- Filter requests awaiting execution
- Average action execution time
- Average filter execution time
- Average filter queue time
- Pagefile usage

Einstellungen über die Konfigurationsdatei

Direkt Änderungen der Konfiguration können NoSpamProxy in einen nicht mehr startfähigen Zustand versetzen.

Aktivieren der Option 'Zustellen von ungültigen E-Mails'

Kann NoSpamProxy E-Mails aufgrund fehlerhaften Aufbaus nicht überprüfen, dann wird die E-Mail abgelehnt. Diese Funktion kann über die Konfigurationsdatei an- und abgeschaltet werden.



Beachten Sie, dass betroffene E-Mails von der Gateway Rolle nicht auf Spam und Viren überprüft werden können.

Um die Option zu aktivieren, öffnen Sie die Konfigurationsdatei der Gateway Rolle von NoSpamProxy. Der Pfad zu der Datei heißt im Allgemeinen %ProgramData%\Net at Work Mail Gateway\Configuration\GatewayRole.config. Bitte beachten Sie, dass Sie die Datei erst abspeichern können, wenn der Dienst der Gateway Rolle beendet ist. Anderenfalls werden alle Änderungen verworfen.

Bitte suchen Sie in der Datei zunächst die folgende Zeile:

```
</netatwork.nospamproxy.proxyconfiguration>
```

Suchen Sie in diesem Abschnitt **netatwork.nospamproxy.proxyconfiguration** nach dem Schlüssel **dispatchInvalidMails**. Sollten Sie ihn nicht finden, fügen Sie den Schlüssel wie folgt ein, oder ändern Sie ihn, falls gefunden, wie folgt ab:

```
<dispatchInvalidMails isEnabled="true" />
```

Die Zeilen sollten dann wie folgt aussehen:

```
<dispatchInvalidMails isEnabled="true" />
</netatwork.nospamproxy.proxyconfiguration>
```

Speichern Sie die Datei ab und starten Sie anschließend die Gateway Rolle wieder.

Verarbeitung von RTF-Dateien bei der Inhaltsfilterung

E-Mails im RTF-Format sowie beigefügte Anhänge werden im Microsoft-eigenen Format TNEF (Transport Neutral Encapsulation Format) kodiert. Diese werden dann zusammen mit allen Anhängen in einen Anhang umgewandelt, der standardmäßig den Namen `winmail.dat` erhält.

Wird bei der Konfiguration des Inhaltsfilters für eine Bedingung eine der Dateitypen ausgewählt, die im `winmail.dat`-Anhang enthalten sind, öffnet NoSpamProxy den so entstandenen TNEF-Container und fügt die einzelnen Anhänge der E-Mail bei.

Sie finden einen Hinweis über die Bearbeitung des TNEF-Containers und die so erfolgte Veränderung der E-Mail im Bereich [Nachrichtenverfolgung](#).

SMTP RFCs

Die meisten im Internet verwendeten Protokolle basieren auf Ideen und Vereinbarungen zwischen mehreren Personen, die nach einiger Zeit zum Standard deklariert wurden. Diese Dokumente tragen das Kürzel RFC (Request for Comment). In den Anfangszeiten des Internet haben mehrere Personen verschiedener Firmen und Institute an verschiedenen Projekten gearbeitet und in Ermangelung einer zentralen Koordinierungsstelle Ihre Überlegungen und Protokolldefinitionen zur Diskussion gestellt.

NoSpamProxy nutzt das Protokoll SMTP. Die Details, wie SMTP funktioniert und auf welche Aktion welche Reaktion zu erfolgen hat, ist in entsprechenden RFC-Dokumenten beschrieben.

Die folgende Liste zeigt die wichtigsten RFC-Dokumente:

- RFC 1123 for important additional information
- RFC 1893 und RFC 2034 for information about enhanced status codes
- RFC 2821 Simple Mail Transfer Protocol (SMTP)
- RFC 2822 Internet Message Format
- RFC 2554, AUTH, Authentication
- RFC 3207, STARTTLS, Start transport layer security

SMTP Errorcodes

Alle Rückmeldungen, die ein SMTP Server an das andere System meldet, beginnen mit einer Nummer. Der Text hinter der numerischen Angabe ist optional, kann sich von E-Mail-Server zu E-Mail-Server ändern und wird von Programmen nicht ausgewertet; er dient lediglich als Hilfe für Administratoren bei der Fehlersuche.

SMTP Errorcodes werden in diesen RFCs beschrieben:

- RFC 2821 Simple Mail Transfer Protocol (SMTP)
- RFC 2822 Internet Message Format
- Q257186 XIMS: SMTP Reply Codes (RFC 821)
- Q257167 XIMS: SMTP Reply Code 451

Die Return Codes setzen sich wie folgt zusammen. Jeder Code ist dabei dreistellig. Die erste Ziffer gibt dabei die Klassifizierung der Meldung an:

- 1yz = ok
- 2yz = completed
- 3yz = intermediate ok (Zwischenbescheid)
- 4yz = transient negative (vorläufig negativ)
- 5yz = permanent negative

Die zweite Stelle definiert die Quelle der Meldung:

- x0z = Syntax
- x1z = Info
- x2z = Connection
- x3z/x4z = nicht definiert
- x5z = Mailsystem

Die am häufigsten anzutreffenden Fehlernummern werden hier noch einmal aufgeführt:

- 200 (nonstandard success response, see RFC 876)
- 211 System status, or system help reply
- 214 Help message
- 220 <domain> Service ready
- 221 <domain> Service closing transmission channel
- 250 Requested mail Action okay, completed
- 251 User not local; will forward to <forward-path>
- 354 Start mail input; end with <CRLF>.<CRLF>
- 421 <domain> Service not available, closing transmission channel
- 450 Requested mail Aktion not taken: mailbox unavailable
- 451 Requested Aktion aborted: local error in processing
- 452 Requested Aktion not taken: insufficient system storage
- 500 Syntax error, command unrecognised
- 501 Syntax error in parameters or arguments
- 502 Command not implemented
- 503 Bad sequence of commands
- 504 Command parameter not implemented
- 521 <domain> does not accept mail (see RFC 1846)
- 530 Access denied
- 535 SMTP Authentication unsuccessful/Bad username or password

- 550 Requested Aktion not taken: mailbox unavailable
- 551 User not local; please try <forward-path>
- 552 Requested mail Aktion aborted: exceeded storage allocation
- 553 Requested Aktion not taken: mailbox name not allowed
- 554 Transaktion failed

Um eine genauere Unterscheidung der einzelnen Fehlerzustände anhand der dritten Stelle zu erlauben, wurden erweiterte Statusmeldungen eingeführt. Diese dienen dazu, mehr als 10 Unterschiedliche Statuscodes zurückzugeben.

Diese werden in dem folgenden RFC Dokument genauer definiert:

- Q256321 RFC 1893 (Q256321) for Enhanced Status Codes for Delivery Status Notification (DSN) messages

Die Rückmeldung eines Servers kann wie folgt aussehen:

```
250 2.1.0 user1@example.com....Sender OK
```

Hinter der dreistelligen Meldung 250 folgt die ausführliche Meldung 2.1.0.

SMTP Timeouts

Bei der Verbindung zwischen zwei Systemen kann es immer zu Verzögerungen bei der Verarbeitung kommen. Heutzutage ist eine überlastete Leitung selten die Ursache für Verzögerungen.

In der Regel muss der empfangende E-Mail-Server die Daten annehmen und abspeichern; hierfür benötigt er Zeit. Daher sendet er seine Statusmeldung erst nach dem Abschluss dieser Tätigkeiten.

Auch NoSpamProxy nimmt eine E-Mail teilweise an, was einige Zeit beansprucht, um anhand der Regeln entsprechende Aktionen zu starten. Erst nach dem Abschluss erhält das einliefernde System eine Meldung, um mit der Übertragung fortzufahren oder die Verbindung zu unterbrechen.

Auch diese maximalen Wartezeiten sind in der "RFC 2821- Simple Mail Transfer Protocol" definiert.

Folgende Zeiten gelten als Empfehlung:

- **Erste 220 Meldung nach dem Verbindungsaufbau: 5 Minuten**
Der Sender muss einen Unterschied zwischen einer nicht angenommenen Verbindung und einer verzögerten Antwort durch hohe Belastung unterscheiden können. Sehr häufig nimmt der TCP/IP-Stack eine Verbindung an; doch der SMTP Server verzögert die Versendung der 220 Nachricht bis das System die Verarbeitung weiterer E-Mails zulässt.
- **MAIL-Befehl: 5 Minuten**
Nach spätestens 5 Minuten muss ein E-Mail-Server auf das "MAIL FROM" geantwortet haben
- **RCPT-Befehl: 5 Minuten**
Nach spätestens 5 Minuten muss ein E-Mail-Server auf das "RCPT TO" geantwortet haben.
- **DATA: 2 Minuten**

Nach spätestens 2 Minuten muss ein E-Mail-Server auf den Befehl "DATA" reagieren. Dies ist ein für NoSpamProxy wichtiger Wert, da die Abarbeitung der Envelope Filter nicht länger dauern darf. Normalerweise antwortet dann der E-Mail-Server mit einem "354 Start Input"

- **Datenblock: 3 Minuten**

Die Übertragung der eigentlichen E-Mail erfolgt mittels TCP/IP-Blöcken. Die Bestätigung eines Blocks darf nicht länger als 3 Minuten ausbleiben.

- **DATA Abschluss: 10 Minuten**

Nach der Übertragung der E-Mail sendet der absendende E-Mail-Server eine letzte Zeile, die nur einen Punkt enthält und wartet auf die Bestätigung. Der empfangende E-Mail-Server hat bis zu 10 Minuten Zeit auf dieses Signal mit "250 OK" oder einer anderen Meldung zu antworten. Diese Zeit hat daher auch NoSpamProxy, um die E-Mail durch verschiedene Filter zu bewerten, durch Aktionen zu verändern und an den internen E-Mail-Server zuzustellen. Erst wenn der empfangende E-Mail-Server die E-Mail mit "250 OK" quittiert, übernimmt dieser auch die Verantwortung für die weitere Zustellung. Das Gateway sendet diese Meldung erst dann, wenn der interne E-Mail-Server die E-Mail komplett angenommen hat. NoSpamProxy ist daher zu keinem Zeitpunkt für die weitere Übermittlung verantwortlich.

- **Empfängertimeout: 5 Minuten**

Auch umgekehrt gibt es einen Timeout. Wenn der empfangende E-Mail-Server seine Antwort übermittelt hat, ist der Sender gefordert, die nächsten Befehle zu übermitteln. Bleibt die nächste Meldung jedoch aus, so sollte der Empfänger mindestens 5 Minuten warten, ehe die Verbindung unterbrochen wird.

Glossar

- **API**

Programmierschnittstelle, damit andere Programme auf das eigene Software System zugreifen können. <http://de.wikipedia.org/wiki/Programmierschnittstelle>

- **C-Nummer**

Die C-Nummer ist Ihre eindeutige Lizenz-Nummer. Sie hilft dem Support-Team von Net at Work, Ihre Anfragen schnellstmöglich zu bearbeiten.

- **CER**

Dateiendung zur Kennzeichnung von Dateien, die öffentliche Zertifikate enthalten.

- **DER**

Dateiendung zur Kennzeichnung von Dateien, die öffentliche Zertifikate enthalten.

- **FQDN**

Voll qualifizierten Domänenname. Ein Computer mit dem Name mailserver in der DNS-Domäne example.com besitzt als FQDN den Namen mailserver.example.com. http://de.wikipedia.org/wiki/FQDN#Fully_Qualified_Domain_Name_.28FQDN.29

- **OCSP - Online Certificate Status Protocol**

Ein Internet Protokoll, um den Status eines Zertifikats bei einem Validierungsdienst nachzufragen. Durch einen OCSP Dienst können z.B. ungültige Zertifikate schon vor Ablauf ihrer Gültigkeit als ungültig erklärt werden. http://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol

- **Öffentliche Zertifikate**

Öffentliche Zertifikate sind Zertifikate, die keinen privaten Schlüssel enthalten. Man kann mit diesen Zertifikaten nur verschlüsseln. http://de.wikipedia.org/wiki/Digitales_Zertifikat

- **Persönliche Zertifikate**

Persönliche Zertifikate sind Zertifikate, die einen privaten Schlüssel und einen öffentlichen Schlüssel enthalten. Man kann mit diesen Zertifikaten Nachrichten signieren und Nachrichten entschlüsseln, die zuvor mit dem öffentlichen Schlüssel dieses Zertifikats verschlüsselt wurden. http://de.wikipedia.org/wiki/Digitales_Zertifikat

- **Platzhalter**

Ein Platzhalter (oder Wildcard) bezeichnet reservierte Zeichen die zur Ersetzung durch andere Zeichen dienen. Das Sternchen '*' steht für beliebig viele (auch null) Zeichen. Beispiel: Eine suche nach 'max*' findet alle Worte die mit 'max' beginnen, also auch 'maximal', 'maximilian' usw. Eine Suche nach 'm?x' findet 'mix', 'mux', 'max', 'm4x' usw.

- **Signieren**

Der Vorgang des Signierens bezeugt die Authentizität einer Nachricht, in dem mit Hilfe der privaten Schlüssels eine Prüfsumme über die Nachricht erstellt wird. Dann wird der öffentliche Teil des Zertifikats an die Nachricht angehängt und Sie zum Empfänger übertragen. Der Empfänger kann mit Hilfe des öffentlichen Schlüssels die Prüfsumme überprüfen.

- **P12**

Dateiendung zur Kennzeichnung von Dateien, die private Zertifikate enthalten.

- **PFX**

Dateiendung zur Kennzeichnung von Dateien, die private Zertifikate enthalten.

- **RFC**

Technische und organisatorische Dokumente zur Festlegung der Kommunikationsstandards im Internet. http://de.wikipedia.org/wiki/Request_for_Comments

- **S/MIME**

Standard für die Signatur und Verschlüsselung von einer MIME-gekapselten E-Mail durch ein asymmetrisches Kryptographiesystem. <http://de.wikipedia.org/wiki/S/MIME>

- **StartTLS**

Ist ein Verfahren, um eine E-Mail-Verschlüsselung auf Transportebene einzuleiten. <http://de.wikipedia.org/wiki/STARTTLS>