Net at Work
Building IT-Excellence.

NoSpamProxy 12.2

Betriebshandbuch

- Encryption
- Large Files

Impressum

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Handelsmarken

17. April 2018

Inhalt

1. NoSpamProxy

NoSpamProxy Encryption

NoSpamProxy Encryption sichert als zentrales Gateway am Eingang Ihres Netzwerkes die Vertraulichkeit der E-Mail-Kommunikation sowie die Unveränderlichkeit von Nachrichten und ermöglicht so effiziente Geschäftsprozesse durch gesetzeskonforme elektronische Signatur.

Die Anbindung an das De-Mail-System ermöglicht das Versenden von De-Mails, als wären es ganz normale E-Mails. Für die Anbindung an weitere Systeme wie dem E-Postbrief, der Deutschland-Online - Infrastruktur sowie POP3-Postfächern können Sie NoSpamProxy Encryption ebenfalls nutzen.

PDF Mail

Mit PDF Mail ist es möglich, E-Mails an Kommunikationspartner zu verschicken und diese zertifikatslos zu verschlüsseln. Dazu wird der Inhalt der ursprünglichen E-Mail inklusive Anhängen in ein passwortgeschütztes PDF-Dokument umgewandelt. Das Passwort kann wahlweise vom Versender vorgegeben oder von NoSpamProxy Encryption generiert werden. Zusätzlich besteht für den Empfänger die Möglichkeit, das Passwort auf dem Web Portal des Versenders selber zu hinterlegen. Dazu benötigt er einen Einladungslink, den er per E-Mail erhält. Diese Möglichkeit stellt sicher, dass das Passwort dem Empfänger der PDF Mail nicht übermittelt werden muss und erhöht damit die Sicherheit der PDF Mail. Im Zuge der Konvertierung in das PDF Format bleibt das Format der Anhänge erhalten, so dass der Empfänger diese weiter bearbeiten kann.

Gesetzeskonform und effizient mit qualifizierter elektronischer Signatur

Auf vertrauenswürdiger E-Mail-Kommunikation lässt sich aufbauen; ein Beispiel ist der elektronische Versand von Rechnungen. Elektronische Rechnungen und andere Dokumente erfordern eine rechtsgültige Unterschrift, die durch eine sogenannte qualifizierte elektronische Signatur erreicht wird.

NoSpamProxy Encryption erstellt qualifizierte elektronische Signaturen und entlastet den Anwender von dem unhandlichen Umgang mit Smartcards und PIN durch Zentralisierung am Gateway. Gesetzliche Vorschriften fordern jedoch auch die Überprüfung qualifizierter elektronischer Signaturen, um deren Rechtsgültigkeit beim Empfang zu dokumentieren. NoSpamProxy Encryption erledigt dies ohne Benutzereingriff und übergibt die erzeugten Protokolle an das unternehmensinterne Archivsystem.

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 AntiSpam und AntiVirus

Bedrohungen und Mehrarbeit durch Spam und Viren sind gerade bei der Umsetzung vertrauenswürdiger E-Mail-Kommunikation ein zusätzliches Hindernis. Da NoSpamProxy Encryption auf den Technologien der bewährten AntiSpam-Software NoSpamProxy basiert, lassen sich dessen Funktionen einfach durch eine Lizenzerweiterung freischalten. So kann auf nur einem Gateway und mit einer einheitlichen Administration auch der Schutz gegen Spam und Malware umgesetzt werden.

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 Encryption prüft E-Mails an lokale Empfänger auf gültige Signaturen und entschlüsselt sie. E-Mails an externe Empfänger werden, je nach Konfiguration, signiert und verschlüsselt. Es stellt außerdem eine Schnittstelle zu De-Mail, E-Postbrief, Deutschland-Online - Infrastruktur und POP3-Postfächern bereit.

Intranet Rolle

Die Intranet Rolle enthält die gesamte Konfiguration von NoSpamProxy und verwaltet die kryptographischen Schlüssel. Des Weiteren findet auf dieser Rolle die Synchronisierung von Benutzerdaten aus dem Active Directory oder einem anderen Verzeichnisdienst, wie z.B. Lotus Domino statt. Die Intranet Rolle wird nur einmal installiert.

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

Web Portal

Das Web Portal ermöglicht Benutzern das Hinterlegen von Passwörtern für PDF Mail sowie das Verfassen von Antworten auf PDF Mails.

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).

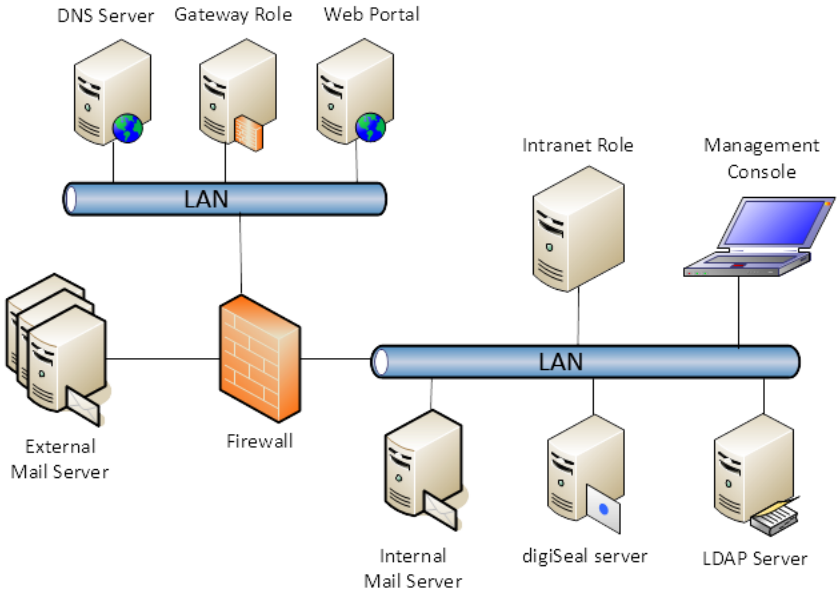


Bild 1: Komponenten von NoSpamProxy

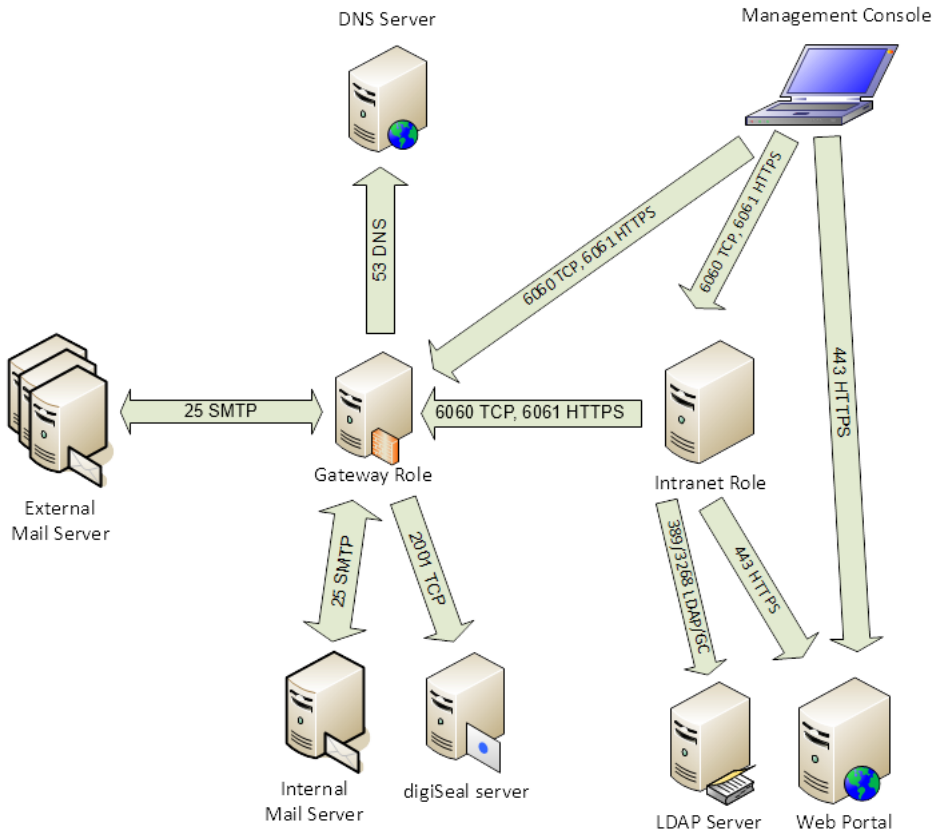


Bild 2: Kommunikation von NoSpamProxy untereinander und mit anderen Komponenten

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 sie ggf. verschlüsselt und signiert werden.

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).

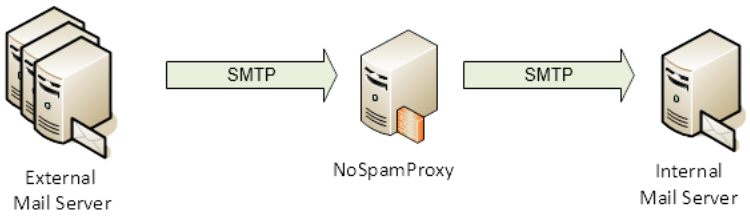


Bild 3: NoSpamProxy vor dem eigenen E-Mail-Server

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'.

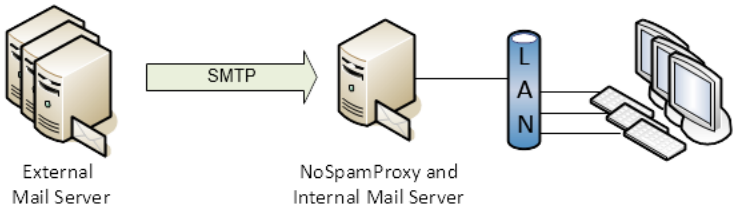


Bild 4: NoSpamProxy auf dem E-Mail-Server

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).

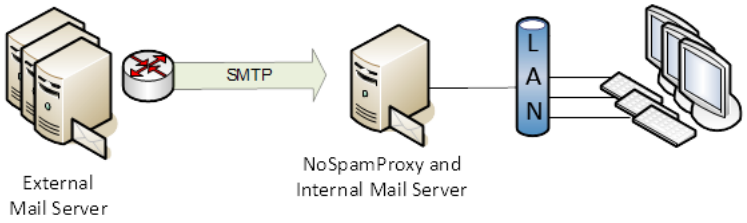


Bild 5: NoSpamProxy mit NAT Router

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.

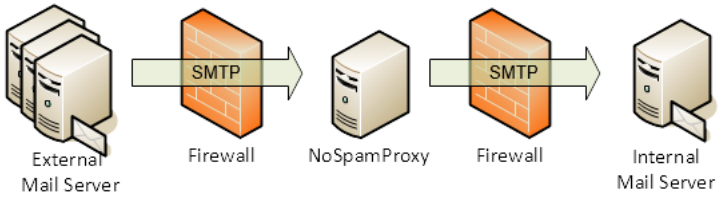


Bild 6: NoSpamProxy mit Firewall

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.

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 7).

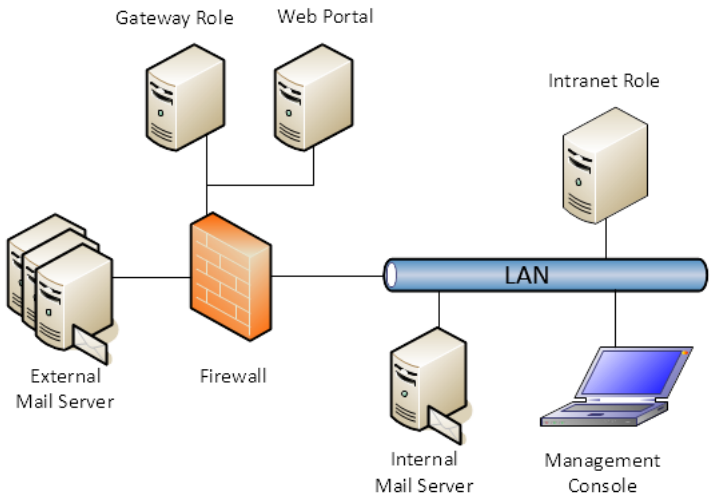


Bild 7: Installation von NoSpamProxy in der DMZ

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 8).

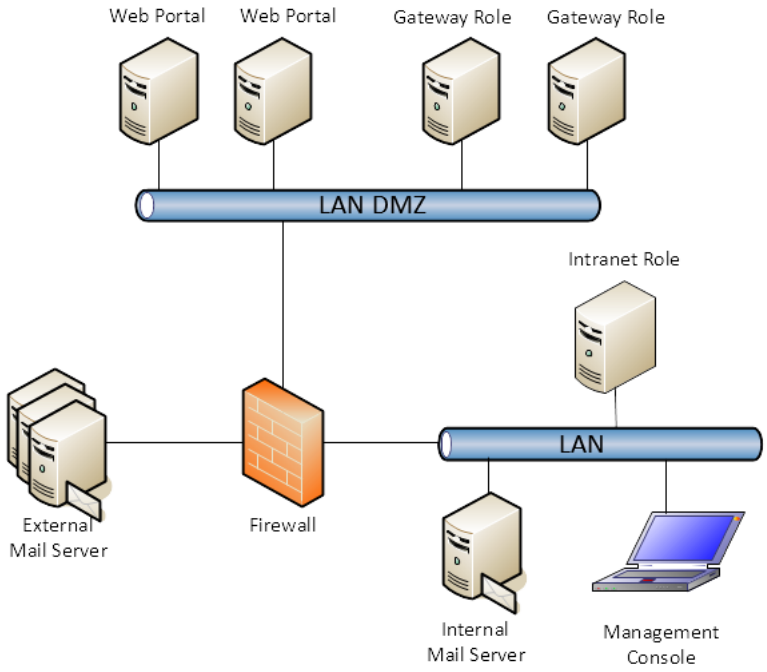


Bild 8: Rollen von NoSpamProxy auf verteilten Servern

E-Mails an externe Adressen

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 Verwaltungskonsole

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 Verwaltungskonsole von NoSpamProxy gliedert sich in folgenden Bereiche:

- **Die Übersichtsseite**
  Unter dem obersten Knoten der Verwaltungskonsole 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 9) dient Ihrem schnellen Überblick. Sie erhalten hier eine Übersicht über den Status der installierten Rollen.

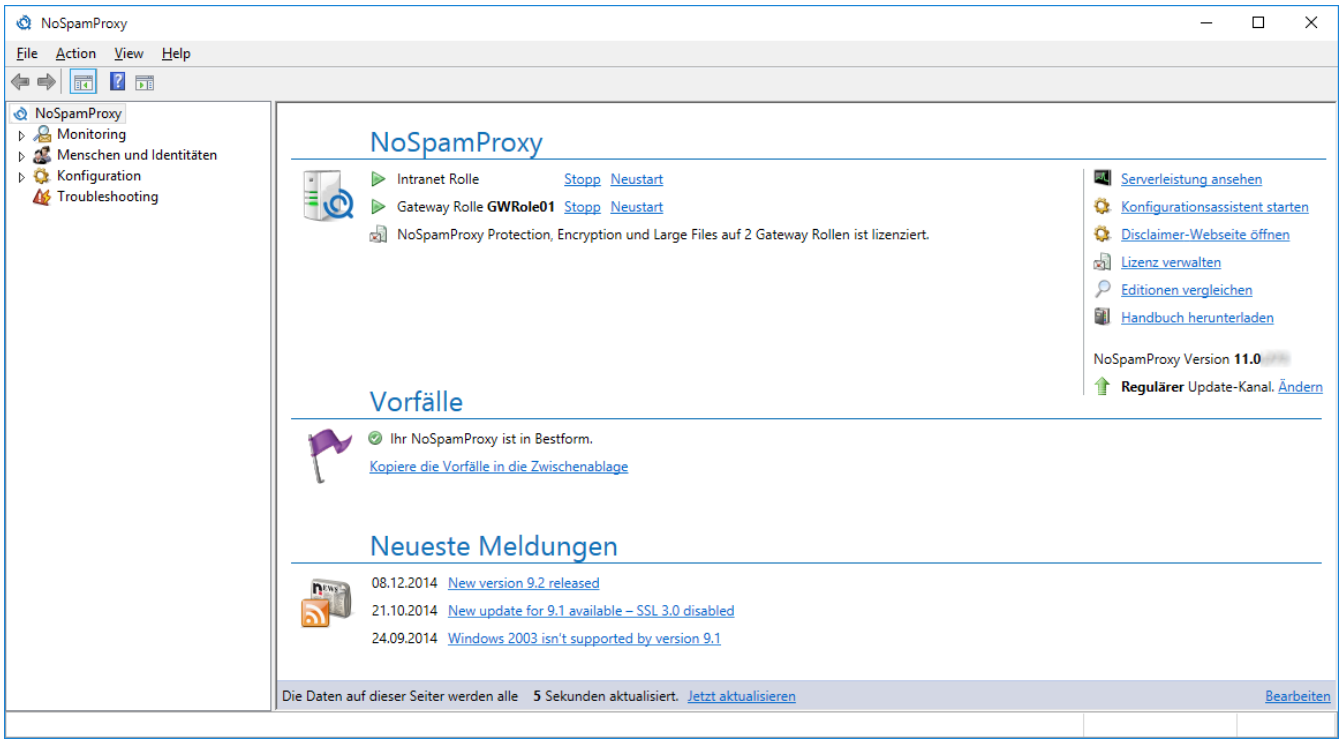


Bild 9: Die Übersicht über die Konfiguration der Gateway Rolle

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 10).

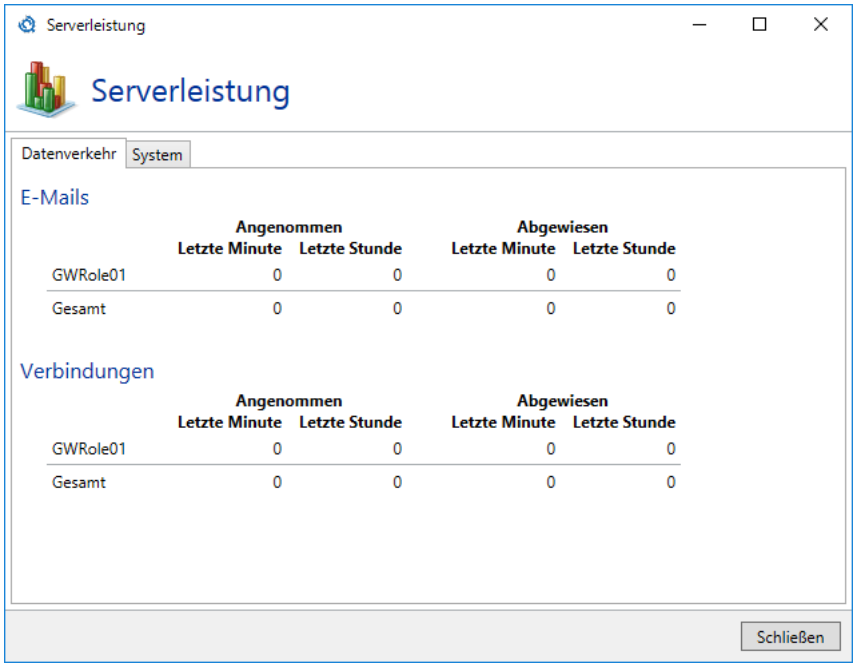


Bild 10: Die aktuell verarbeiteten Nachrichten

System

Die Seite **System** zeigt für jedes System mit Intranet oder Gateway Rollen die installierten Dienste, deren Status und die verwendeten Ressourcen (Bild 10).

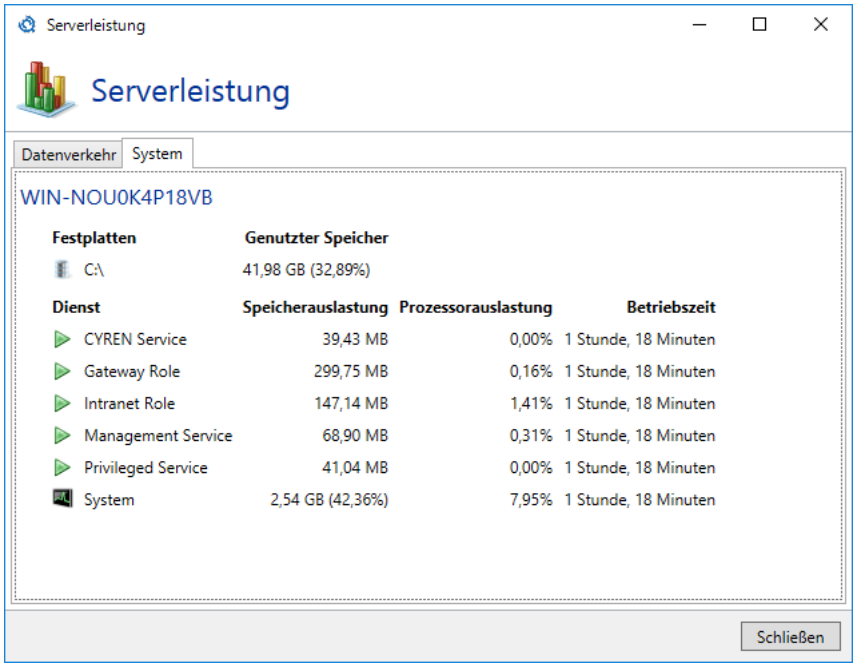


Bild 11: Die aktuell verwendeten und die zur Verfügung stehenden Ressourcen

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 folgende Schritte durch:

- Kontrollieren Sie die Konfiguration der Empfangskonnektoren.
- Spielen Sie Ihre eigenen persönlichen kryptographischen Schlüssel zur Benutzung von NoSpamProxy Encryption mit S/MIME oder PGP-Schlüsseln unter der Zertifikats- oder PGP-Schlüsselverwaltung ein.

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 12).

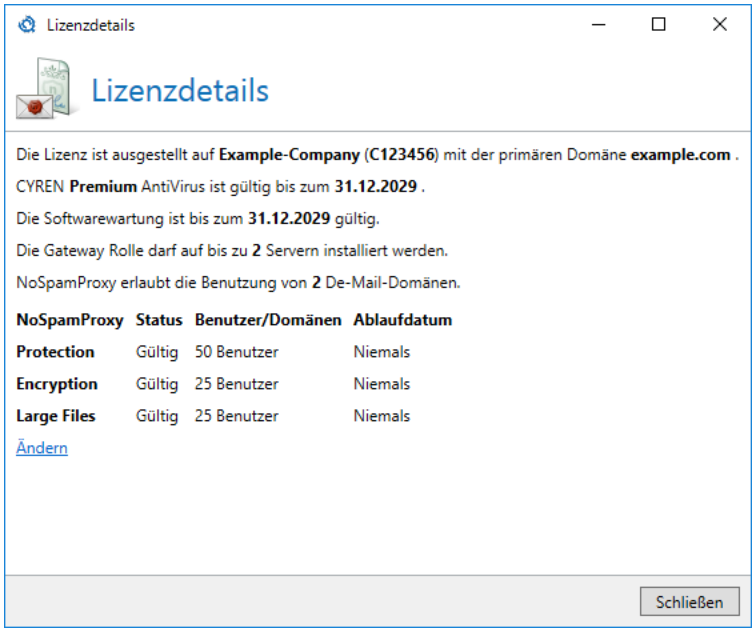


Bild 12: Die derzeitig eingespielte Lizenz

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 13). 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.

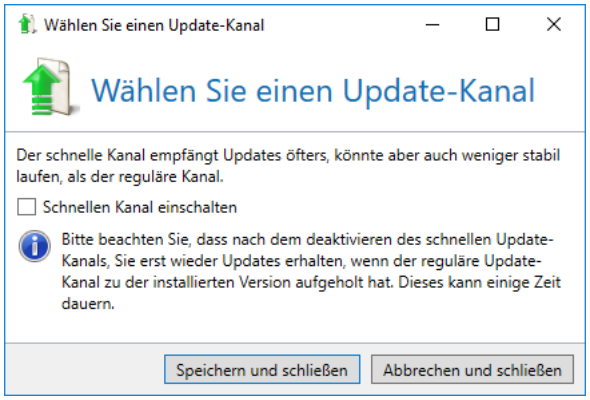


Bild 13: Einstellungen für den Update-Kanal

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 14) informieren Sie über den Empfang und Versand Ihrer E-Mails. Außerdem werden Status-Informationen über das System und den E-Mail-Verkehr angezeigt.

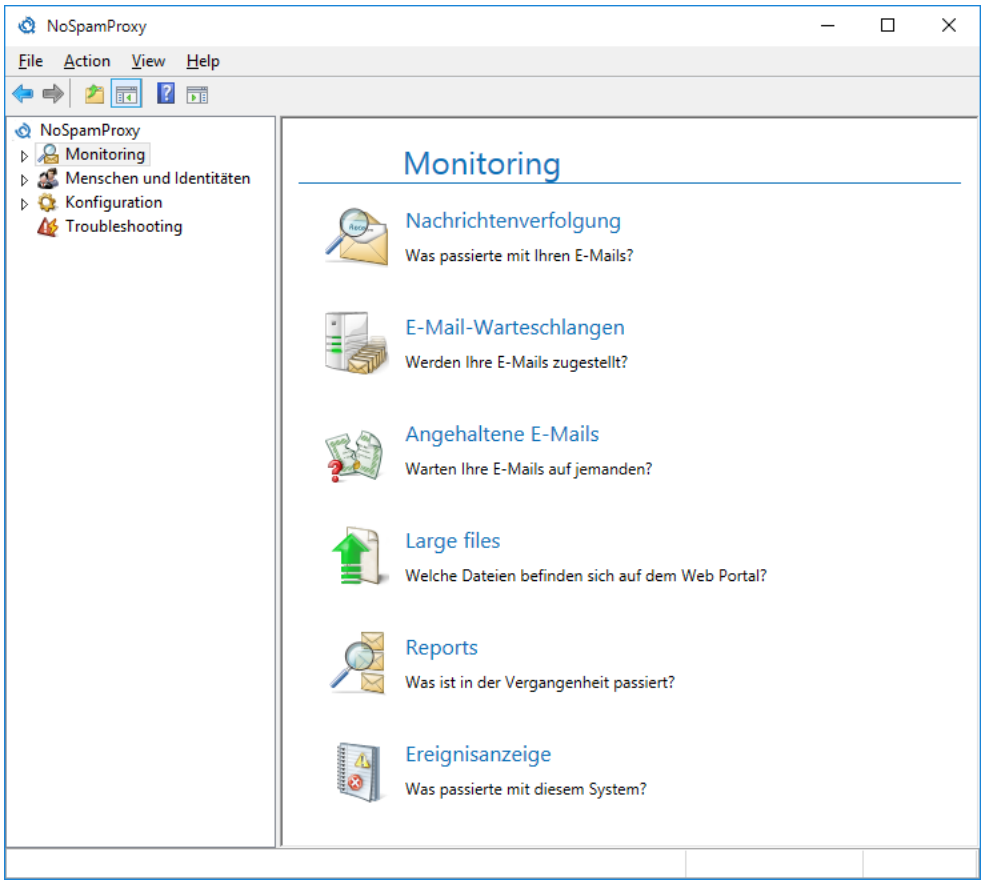


Bild 14: Übersicht über die Bereiche des Monitoring

Nachrichtenverfolgung

Die Nachrichtenverfolgung erlaubt Ihnen nachzuvollziehen, wann welche E-Mails geblockt oder durchgelassen wurden (Bild 15). 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.

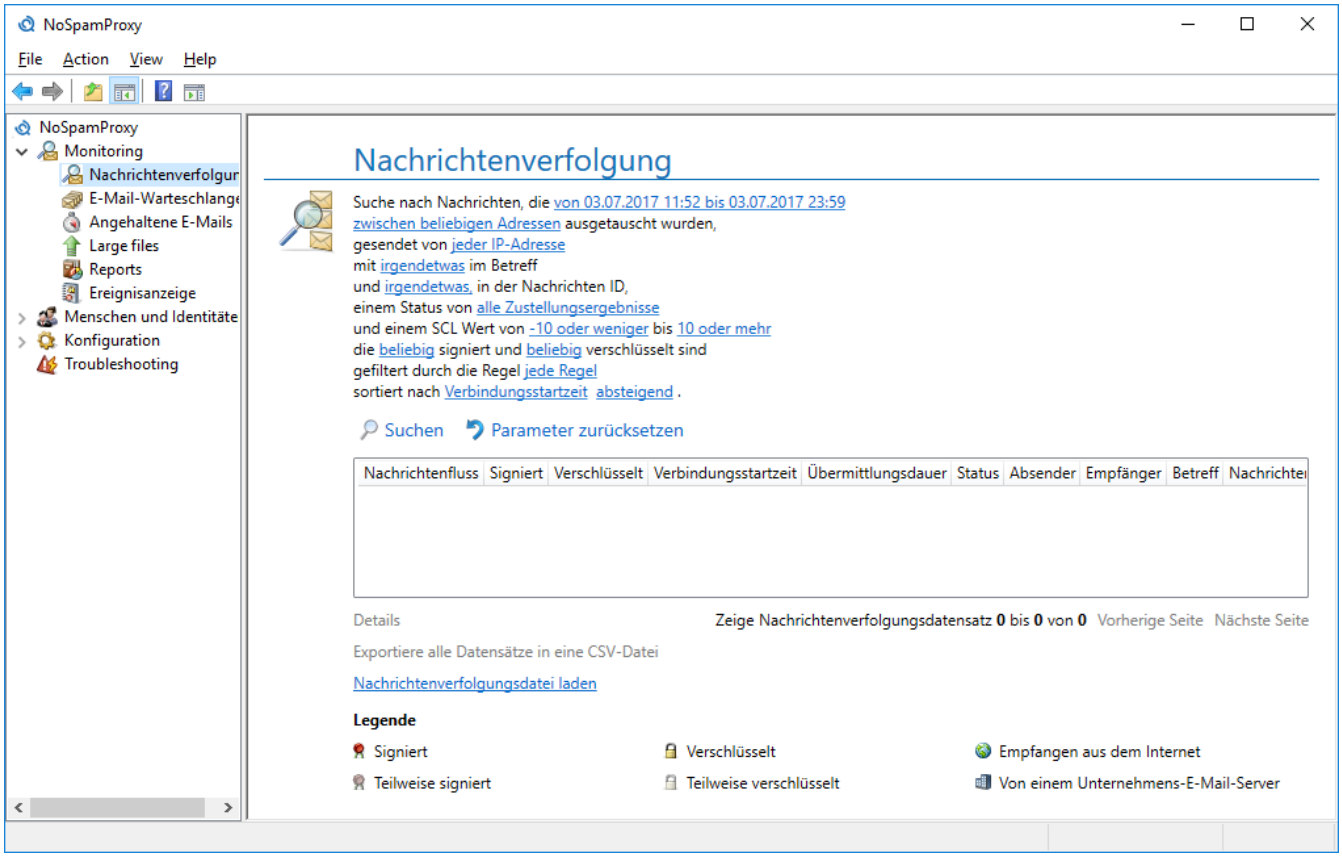


Bild 15: Die Suche der Nachrichtenverfolgungsdatensätze

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.
- Zustellergebnisse: 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 16). 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.

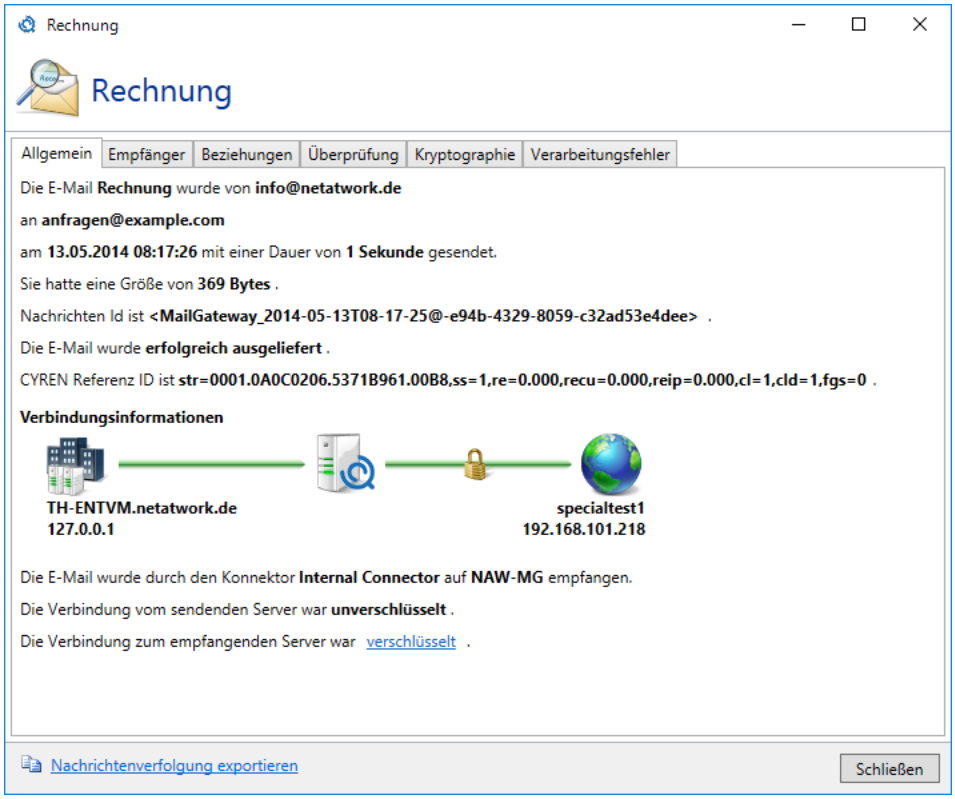


Bild 16: Das Ergebnis der E-Mail-Zustellung im Detail

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 17). 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.

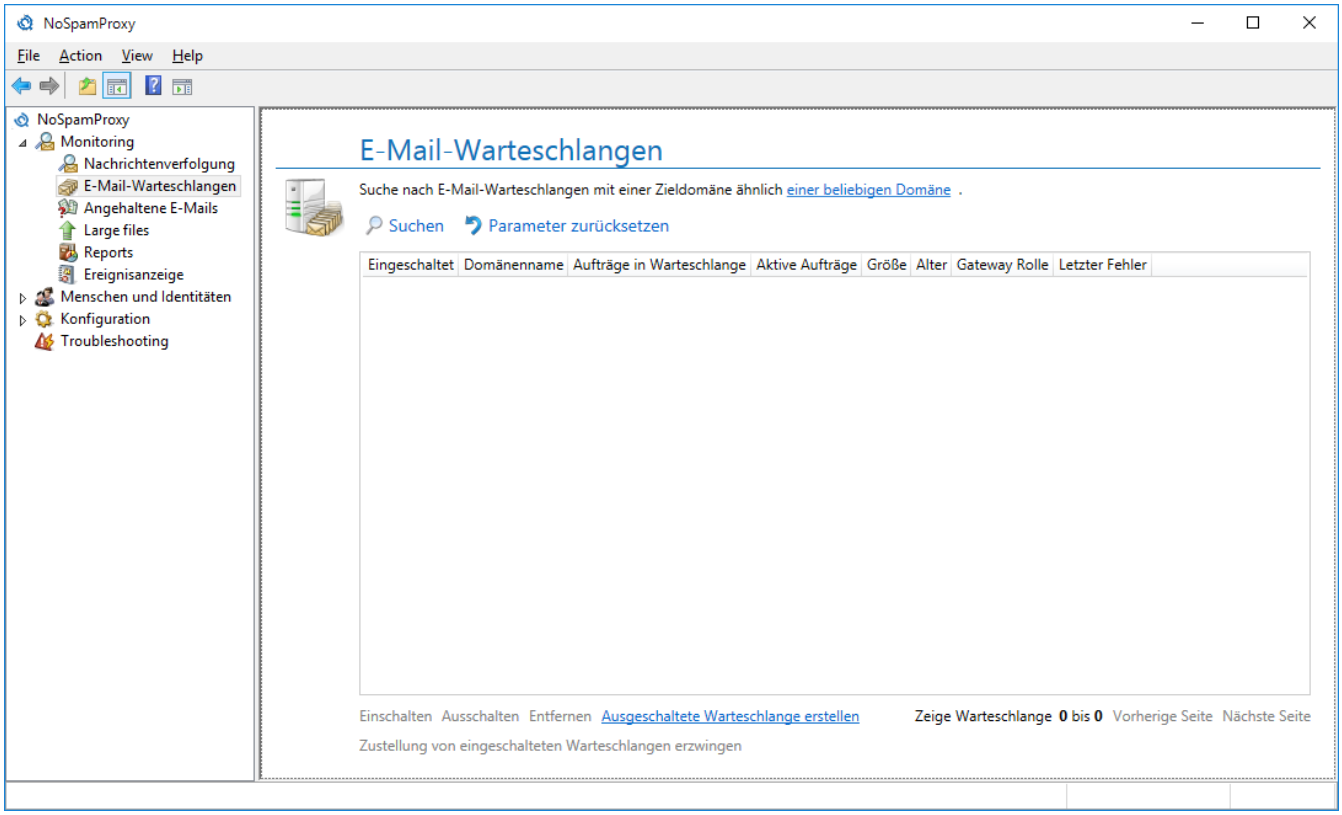


Bild 17: Alle unversendeten E-Mails befinden sich, gruppiert nach Domänenname, in Warteschlangen

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 18).

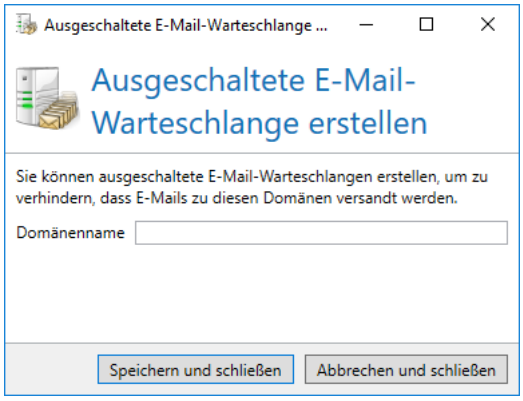


Bild 18: Erstellen einer "Ausgeschalteten Warteschlange"

Geben Sie unter **Domänenname für Warteschlange** den Domänennamen 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.

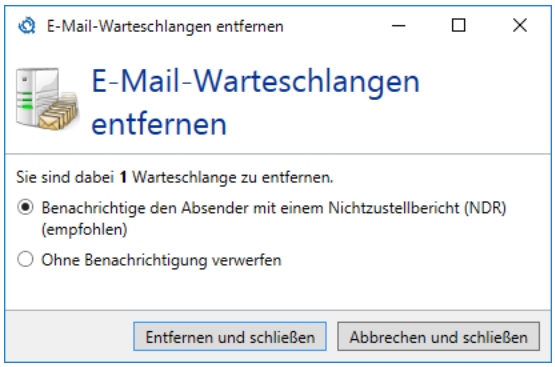


Bild 19: Entfernen von Warteschlangen

Angehaltene E-Mails

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 20).

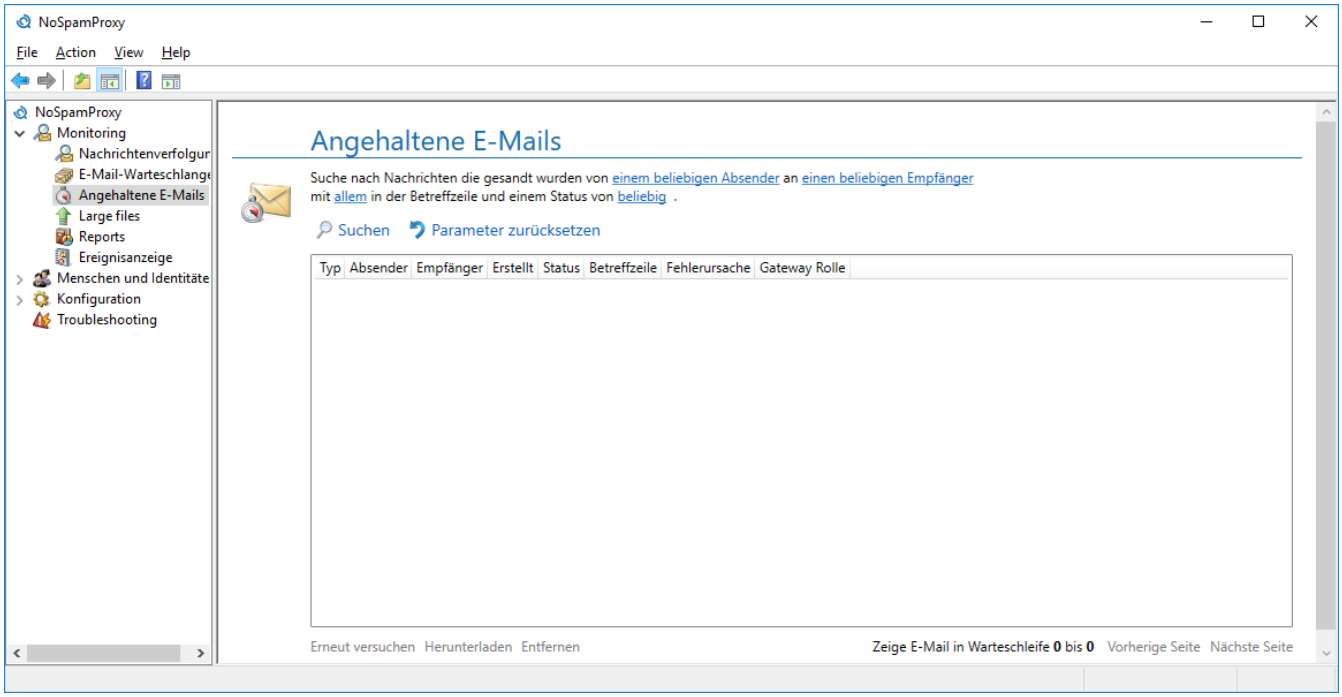


Bild 20: Die Liste aller angehaltenen E-Mails

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 eine E-Mail über die Aktion Anhänge mit einem Passwort schützen verschlüsseln möchten und die in der Aktion angegebenen Passwortquellen zurzeit keine Passworte liefern können, werden diese E-Mails in die Liste der angehaltenen E-Mails eingetragen.

Sollte bis zum angezeigten Ablaufdatum der E-Mail kein Passwort bereitgestellt werden oder keine signierte E-Mail vom ursprünglichen E-Mail-Empfänger eingehen, wird die Zustellung abgebrochen und der Absender benachrichtigt.

E-Mails, die beim Hinzufügen oder Validieren von digitalen Dokumentensignaturen nicht automatisch bearbeitet werden können, werden in der Liste der angehaltenen E-Mails eingetragen. Die E-Mails in dieser Liste wurden nicht zum eigentlichen Empfänger ausgeliefert, sondern werden mit Anzeige des aktuellen Status sowie der Ursache des Fehlschlags aufgelistet.

Falls Fehler während des Zustellprozesses auftreten, erscheinen De-Mails in der Liste.

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 21) 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 freigeben 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.

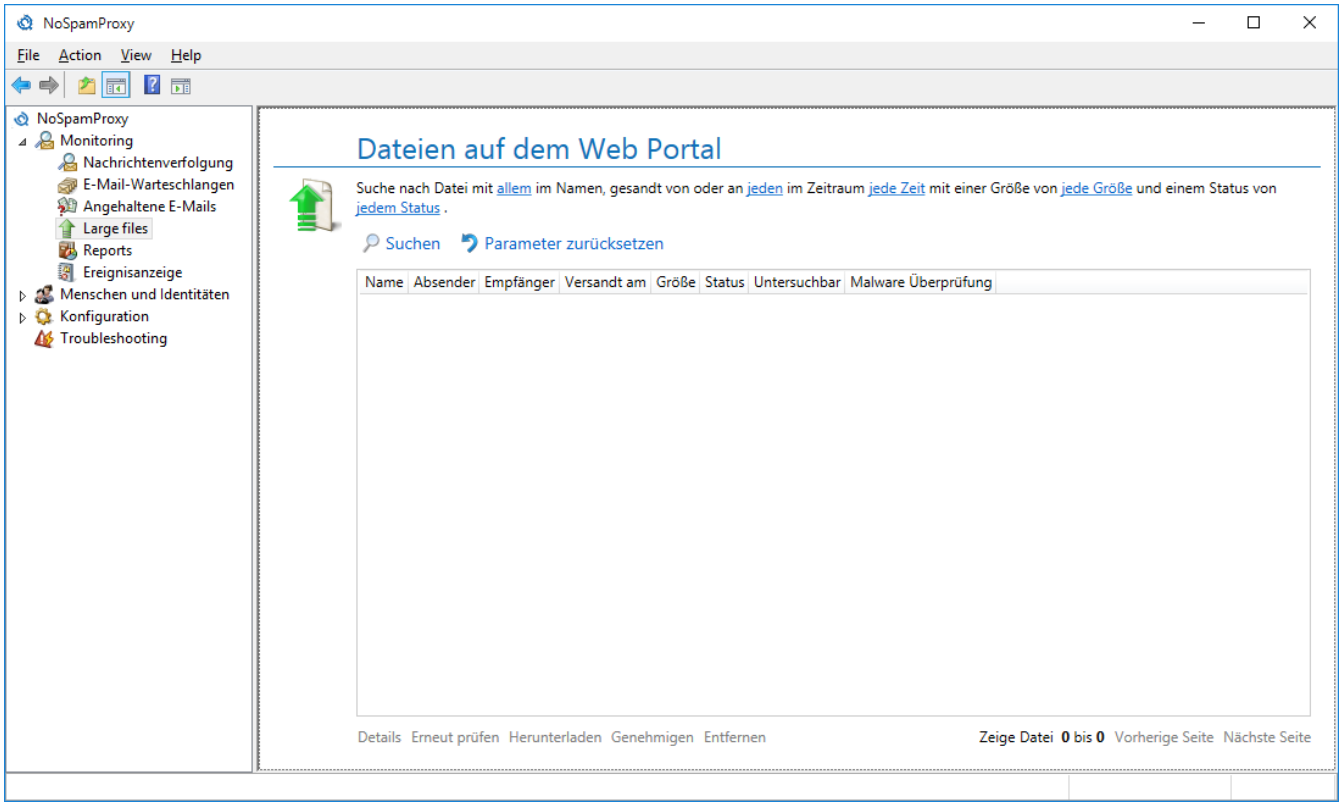


Bild 21: Die Dateien auf dem Web Portal

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 Schiebereglern.
- **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 22). 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.

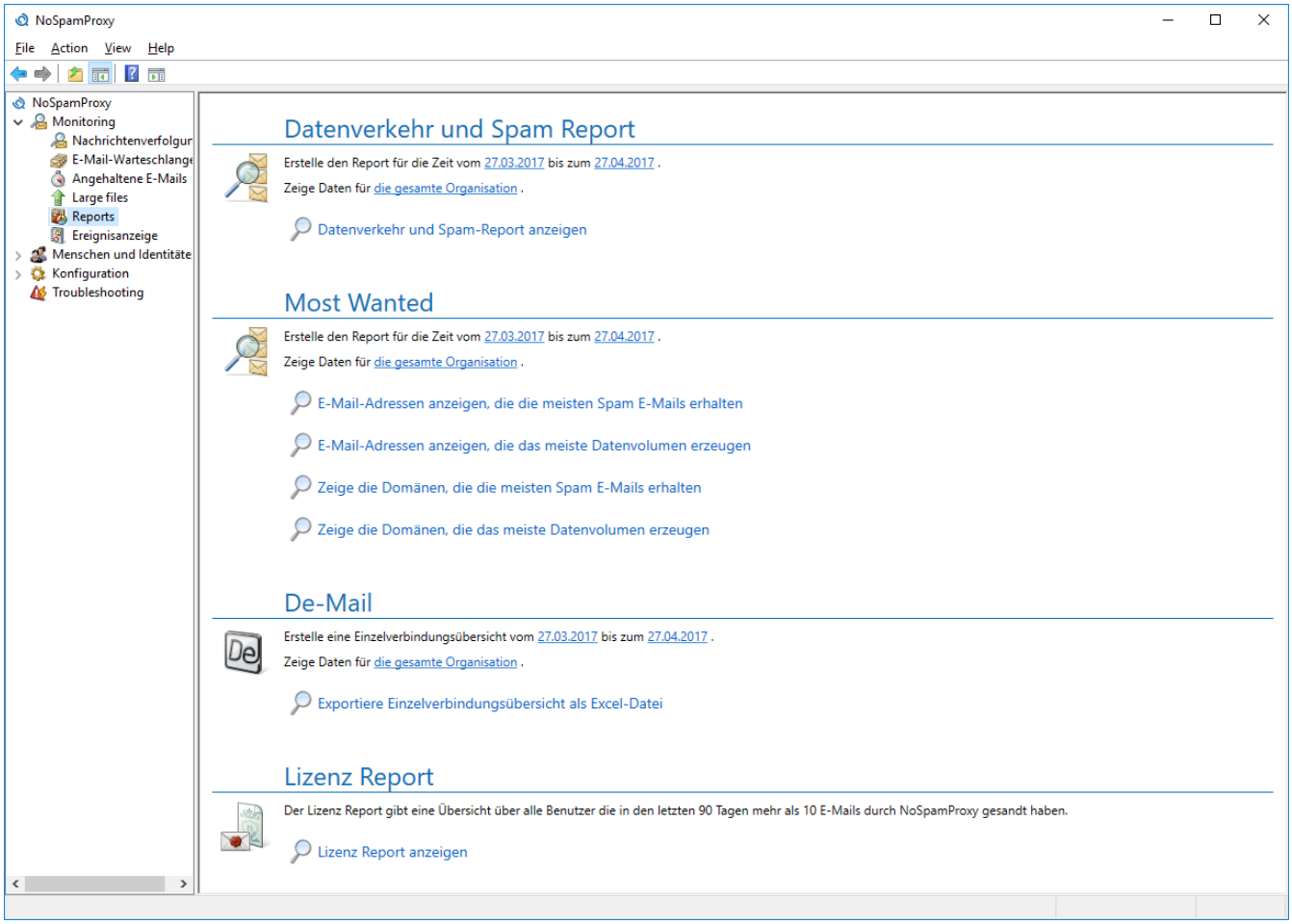


Bild 22: Auswertungen über die Daten der Nachrichtenverfolgung

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**.

Die Analyse des Spam-Anteils liefert nur Daten, wenn die in NoSpamProxy Protection lizenziert ist. Andernfalls wird der Spam-Anteil immer als "0" ausgewiesen.

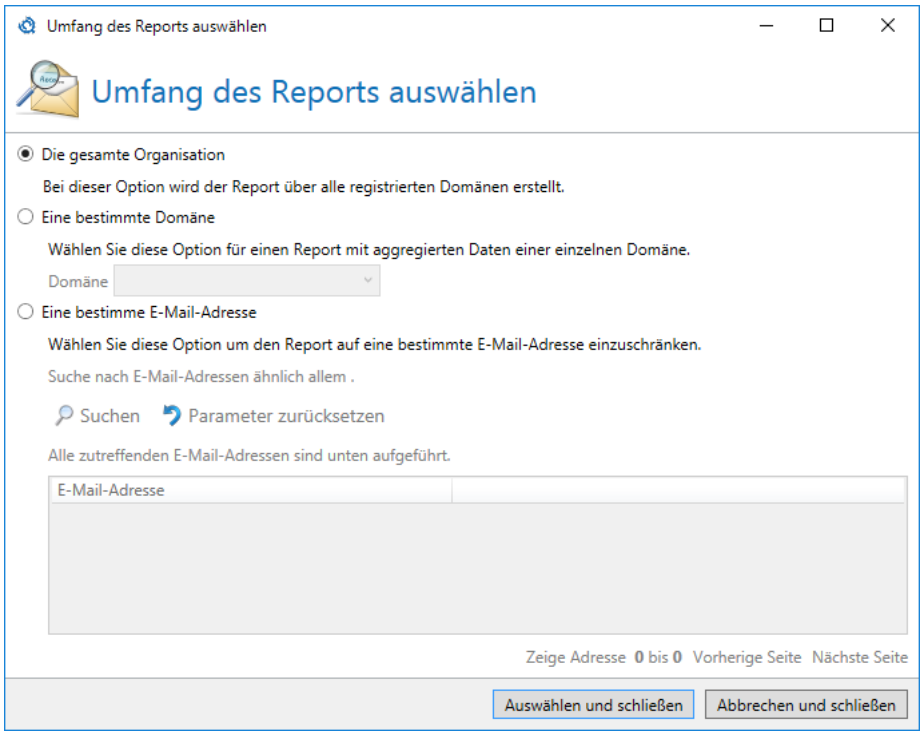


Bild 23: Der Umfang des Datenverkehr und Spam Reports

In dem erscheinenden Dialog (Bild 23) 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.

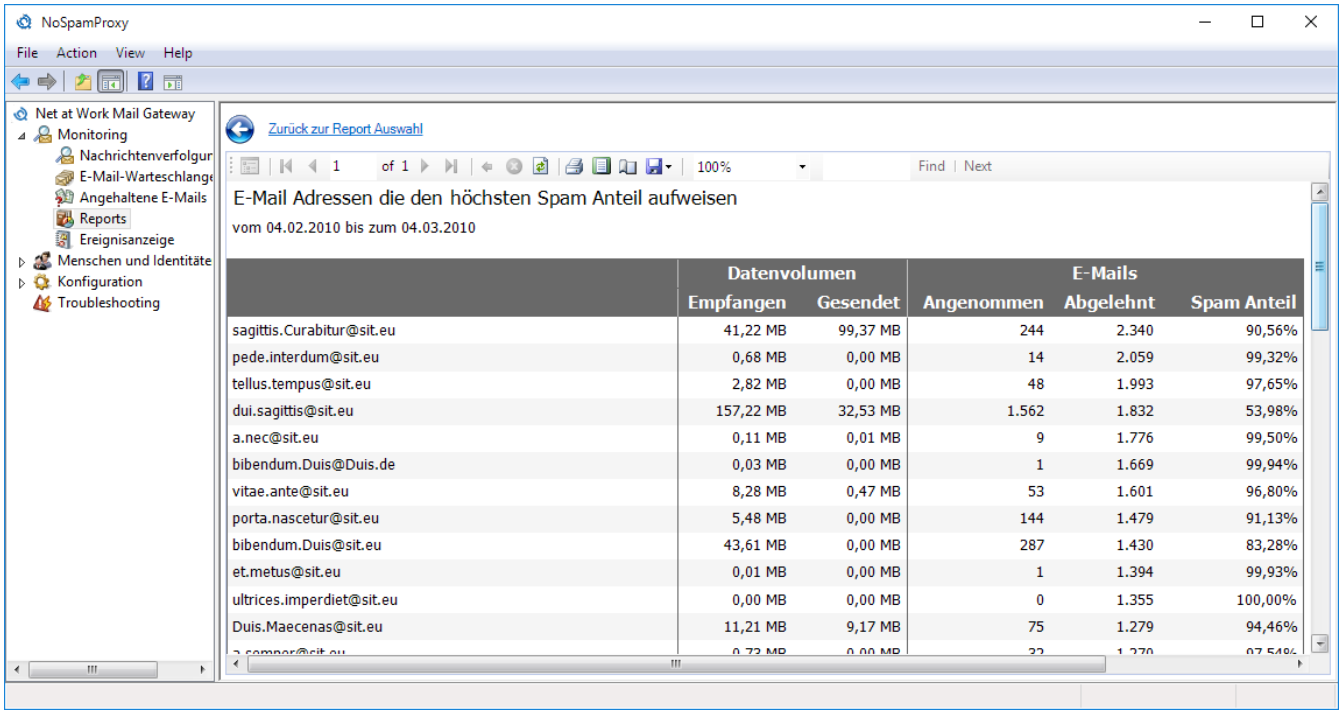
Es können nur Domänen und E-Mail-Adressen ausgewählt werden, die bereits E-Mails empfangen haben und somit in der Nachrichtenverfolgungsdatenbank auftauchen. Es findet kein Zugriff auf die Konfiguration der Gateway Rolle statt.

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

24) Wie auch im Abschnitt **Datenverkehr & Spam Report** können Sie den Zeitraum und den Umfang des jeweiligen Reports festlegen.



	Datenvolumen		E-Mails		
	Empfangen	Gesendet	Angenommen	Abgelehnt	Spam Anteil
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%

Bild 24: 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.

Die Analyse des Spam-Anteils liefert nur Daten, wenn die in NoSpamProxy Protection lizenziert ist. Andernfalls wird der Spam-Anteil immer als "0" ausgewiesen.

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 25).

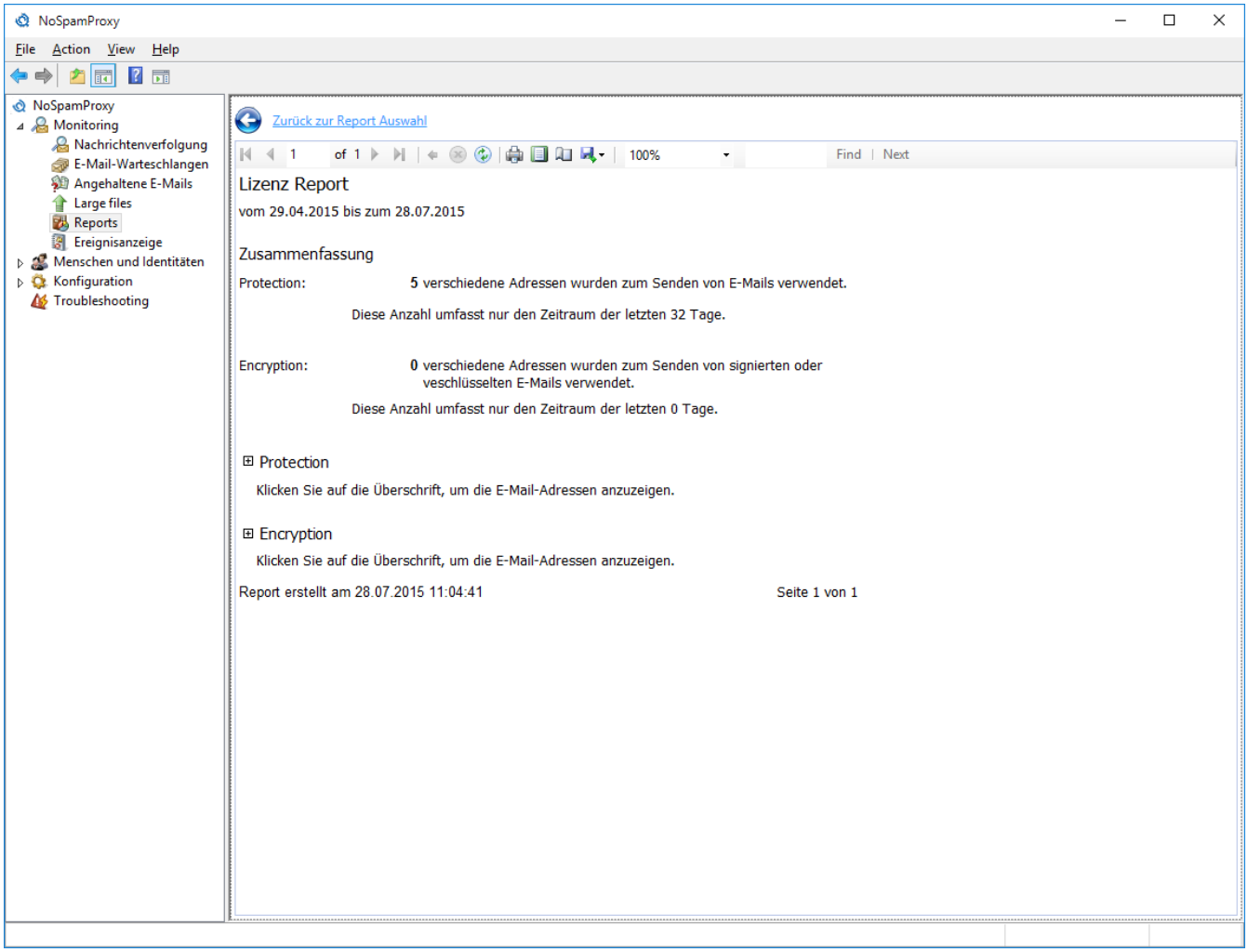


Bild 25: Der Report der tatsächlich genutzten Lizenzen

Der Lizenz-Report summiert alle Benutzer, die in den letzten 90 Tagen mehr als 10 E-Mails versandt haben. Für NoSpamProxy Encryption werden nur Absender von E-Mails in die Bewertung einbezogen, die signiert wurden.

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 26).

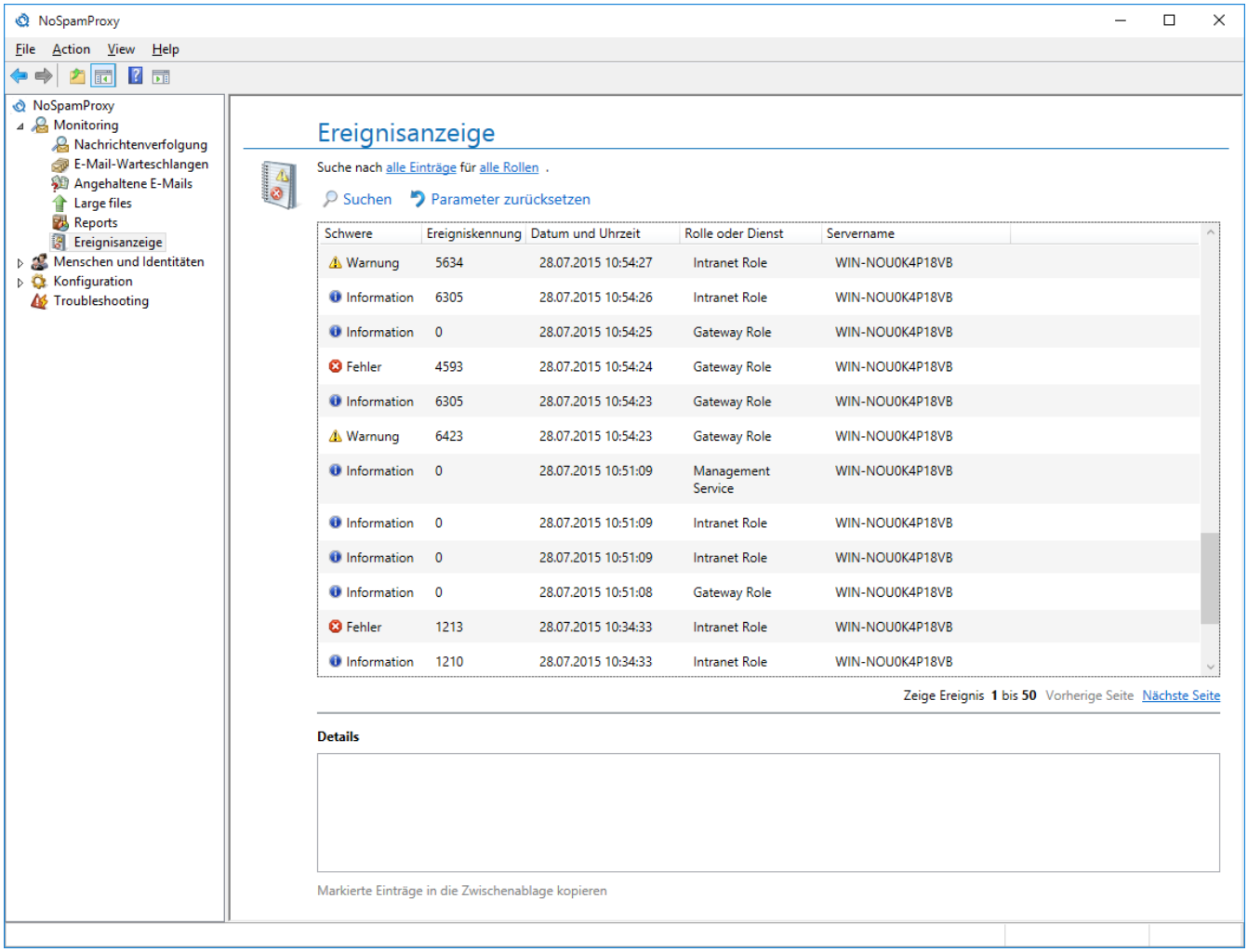


Bild 26: Die Ereignisanzeige zeigt die Ereignisse aller Rollen von NoSpamProxy an

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 und die dazugehörigen kryptographischen Schlüssel und Passworte (Bild 27).

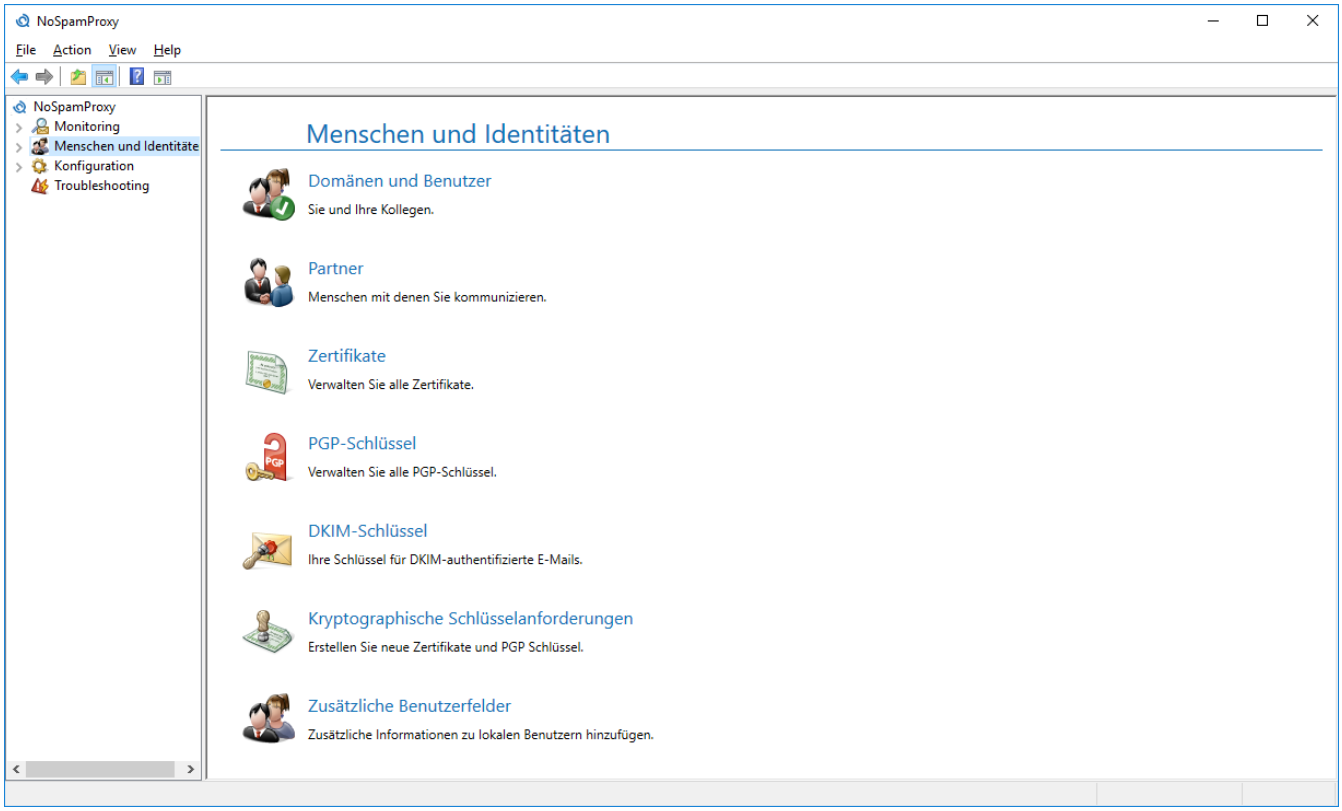


Bild 27: Die Bereiche unter dem Knoten Menschen und Identitäten

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 28). 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.

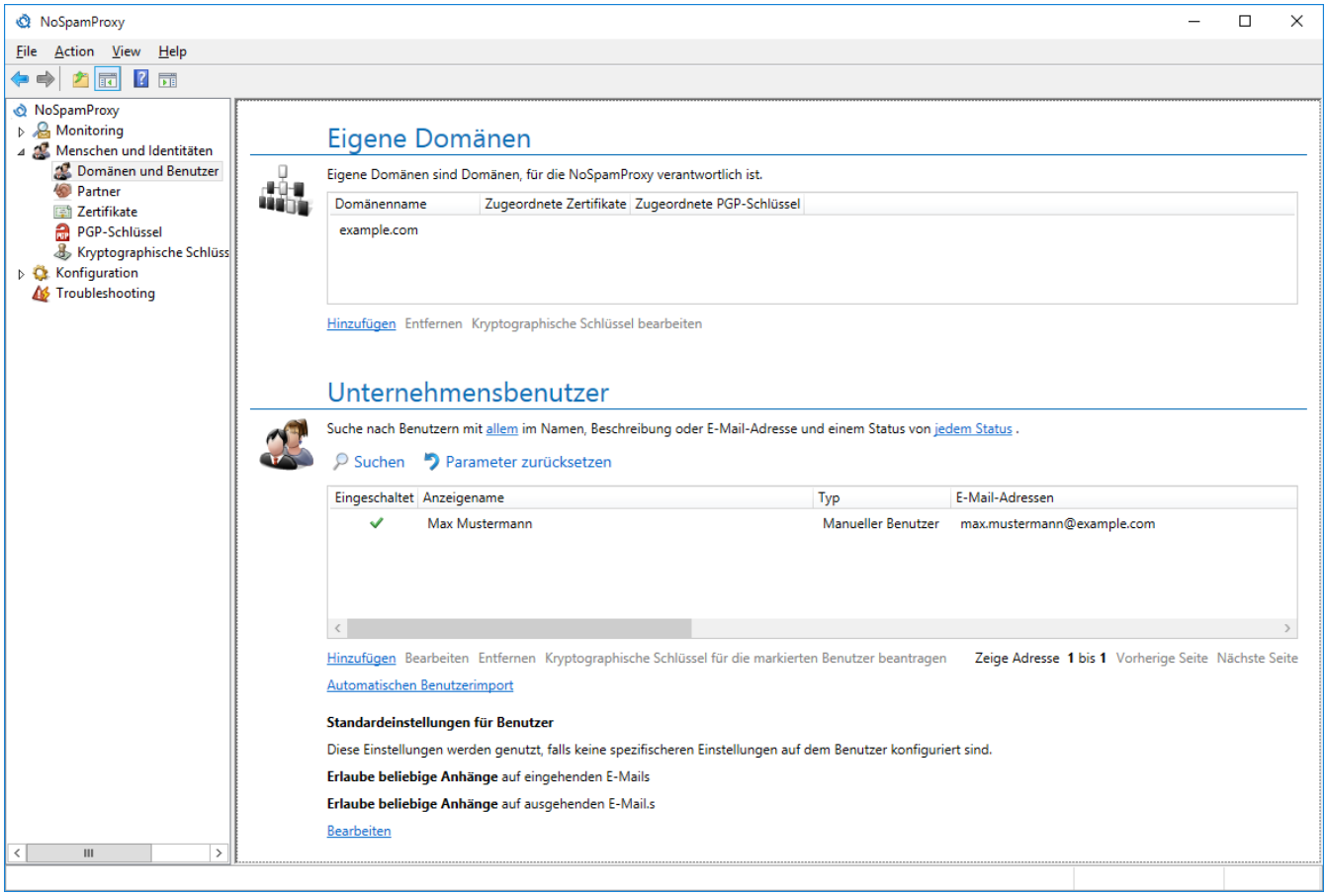


Bild 28: Die Liste der eigenen Domänen und die Unternehmensbenutzer

Kryptographische Schlüssel in den eigenen Domänen und den Unternehmensbenutzern

Die Verwaltung der Domänenzertifikate und Domänen-PGP-Schlüssel unter den eigenen Domänen und die Verwaltung der Zertifikate und PGP-Schlüssel unter den E-Mail-Adressen eines Unternehmensbenutzer läuft in allen Bereichen praktisch identisch ab. Um unnötige Wiederholungen zu vermeiden, wird der Vorgang der Schlüsselauswahl an dieser Stelle zentral beschrieben.

Sie können sowohl für Domänenzertifikate wie auch für E-Mail-Zertifikate oder PGP-Schlüssel einzeln festlegen, welcher der kryptographischen Schlüssel für die Signierung oder Verschlüsselung von E-Mails genutzt werden soll. In dem ausgewählten Bereich werden alle kryptographischen Schlüssel aufgelistet, die der Domäne oder E-Mail-Adresse zugeordnet sind. Für die Auswahl des aktiven Signatur- oder Verschlüsselungszertifikats können Sie in der Spalte **Signatur** bzw. **Verschlüsselung** bei dem betroffenen kryptographischen Schlüssel die Auswahl auf **Signieren/Verschlüsseln unterstützt und ausgewählt** stellen. NoSpamProxy bietet Ihnen für jeden kryptographischen Schlüssel nur die Möglichkeiten an, die dieser auch unterstützt. Beachten Sie, dass nur jeweils ein Schlüssel zur Verschlüsselung bzw. Signatur ausgewählt werden kann. Falls Sie zu einem späteren Zeitpunkt einen anderen Schlüssel auswählen, wird der zuerst ausgewählte nicht mehr für die Verschlüsselung benutzt.

Über die Funktion **Zeige Zertifikatsdetails** bzw. **Zeige PGP-Schlüsseldetails** können Sie alle Eigenschaften des Schlüssels einsehen. Das Löschen von kryptographischen Schlüsseln ist über die Funktion **Lösche ausgewählte Zertifikate** oder **Lösche ausgewählte PGP-Schlüssel** möglich.

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 29).

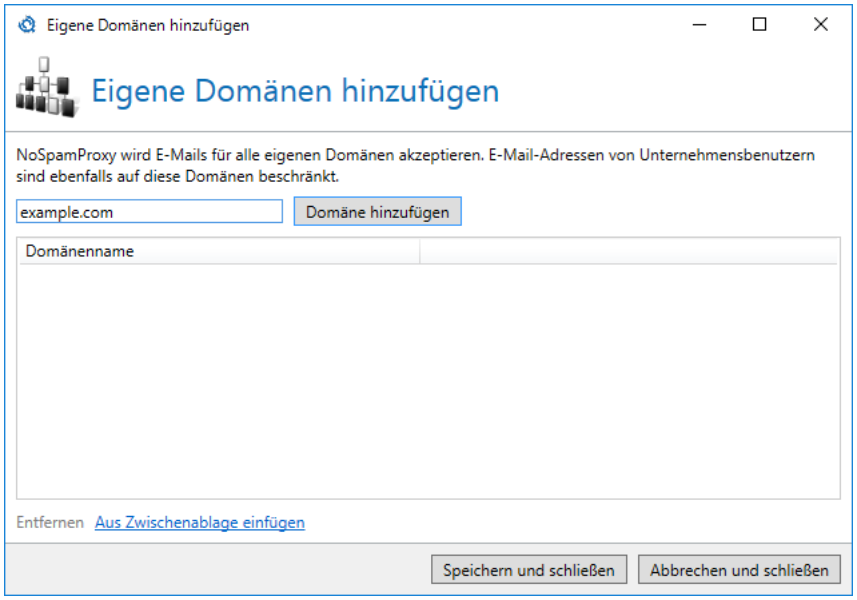


Bild 29: Dialog für neue eigene Domänen

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.

Kryptographische Schlüssel bearbeiten

Über die Funktion **Kryptographische Schlüssel bearbeiten** können Sie die Domänenzertifikate Ihrer eigenen Domänen verwalten (Bild 30).

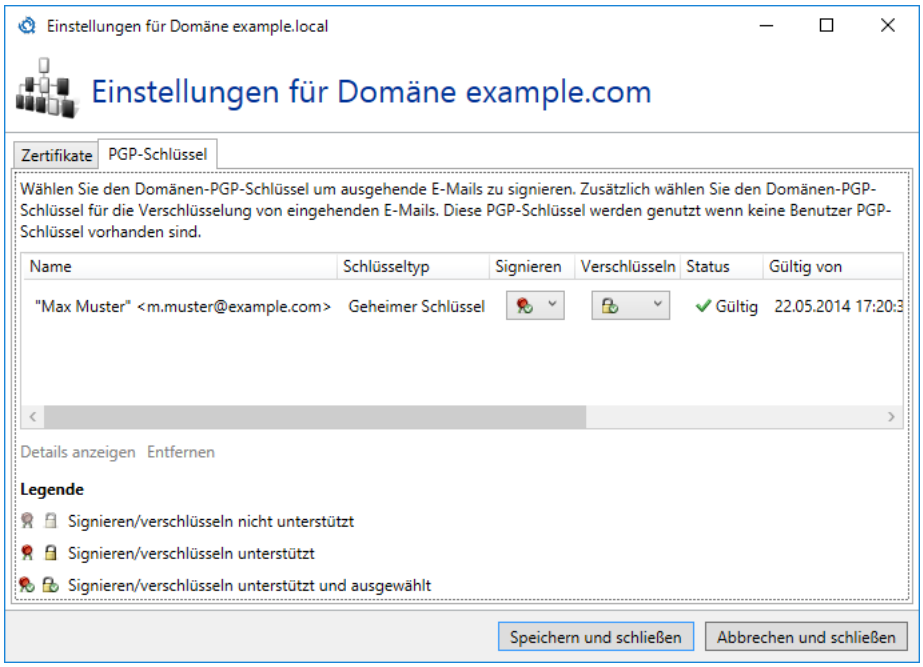


Bild 30: Kryptographische Schlüssel (hier PGP) einer eigenen Domäne

Das Bearbeiten der Zertifikate der eigenen Domäne wird im Abschnitt Kryptographische Schlüssel in den eigenen Domänen und den Unternehmensbenutzern beschrieben.

Um einen kryptographischen Schlüssel für Ihre Domänen zu verwenden, müssen Sie mehrere Schritte durchführen. Importieren Sie zuerst den Schlüssel für Ihre eigene Domäne über die Zertifikats- oder PGP-Schlüsselverwaltung. Stellen Sie sicher, dass sich die Domäne des Schlüssels auch in Ihren eigenen Domänen befindet. Legen Sie nun einen Benutzer in dem Unternehmensbenutzer an, dem die E-Mail-Adresse des Zertifikats zugeordnet wird. Diese E-Mail-Adresse enthält nun automatisch Ihr importiertes Zertifikat. Gehen Sie über die Funktion **Kryptographische Schlüssel bearbeiten** zu den kryptographischen Schlüsseln der E-Mail-Adresse. Wählen Sie dort den importierten Schlüssel aus und dann die Funktion **Zum Domänen-Zertifikaten heraufstufen** oder **Zum Domänen-PGP-Schlüsseln heraufstufen**. Durch das Heraufstufen wird der Schlüssel aus der lokalen E-Mail-Adresse in die eigenen Domänen verschoben. Bitte kontrollieren Sie nach dem Abspeichern in der betroffenen eigenen Domäne die Signatur und Verschlüsselungseinstellungen für Ihr Domänenzertifikat.

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.

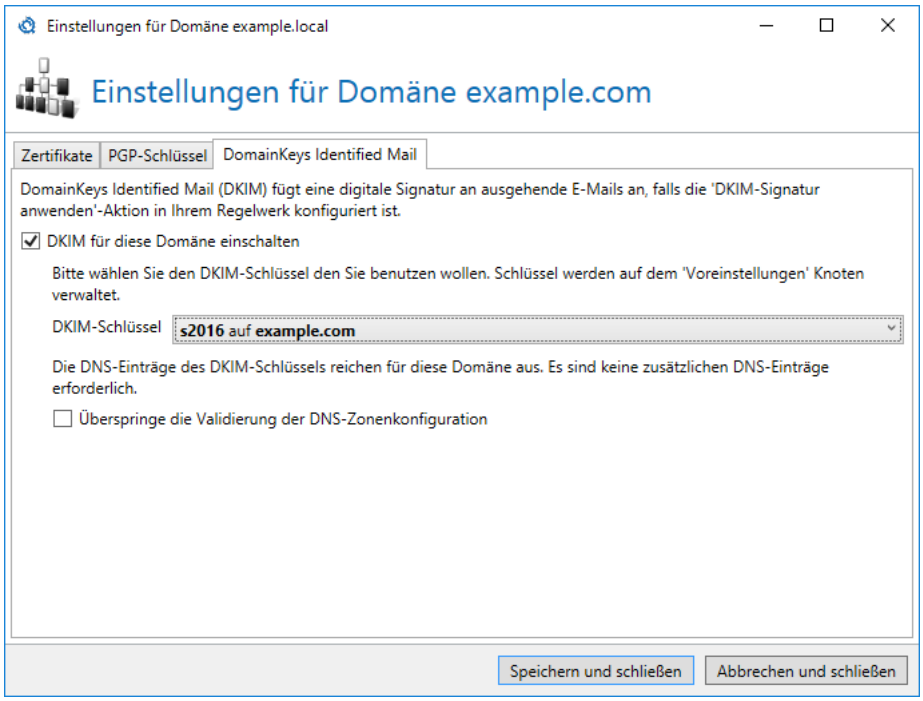


Bild 31: Die Auswahl eines DKIM-Schlüssels für die aktuelle eigene Domäne

Die bereits erstellten Schlüssel können auf der Karteikarte **DomainKeys Identified Mail** der Domäne zugeordnet werden (Bild 31). 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 32). 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.

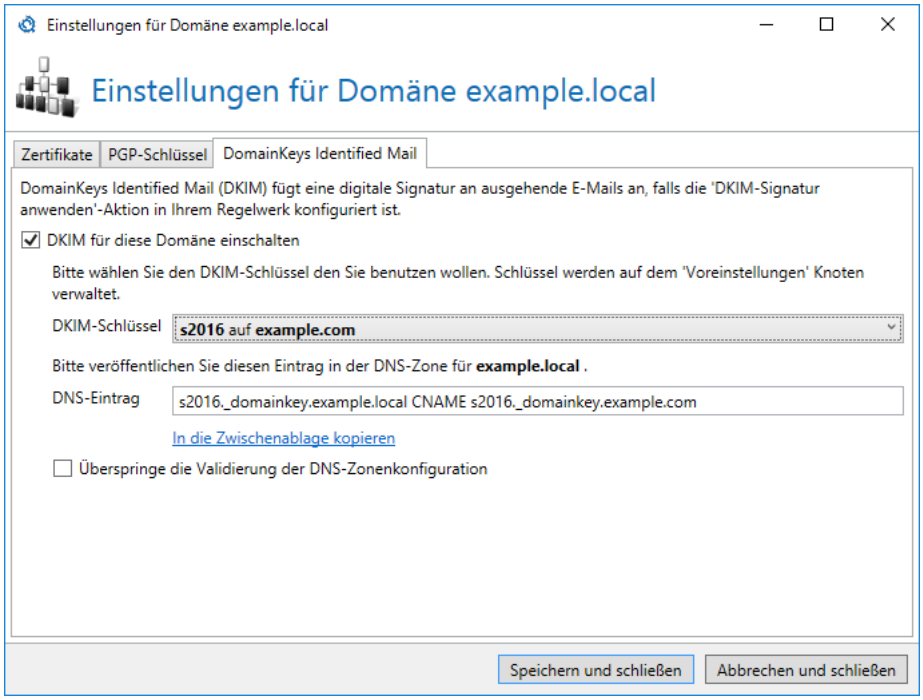


Bild 32: Die Auswahl eines DKIM-Schlüssels von einer anderen Domäne

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 33) den Namen ein. Der Name ist ein Pflichtfeld. Die optionalen Details werden für die Beantragung von Zertifikaten benötigt.

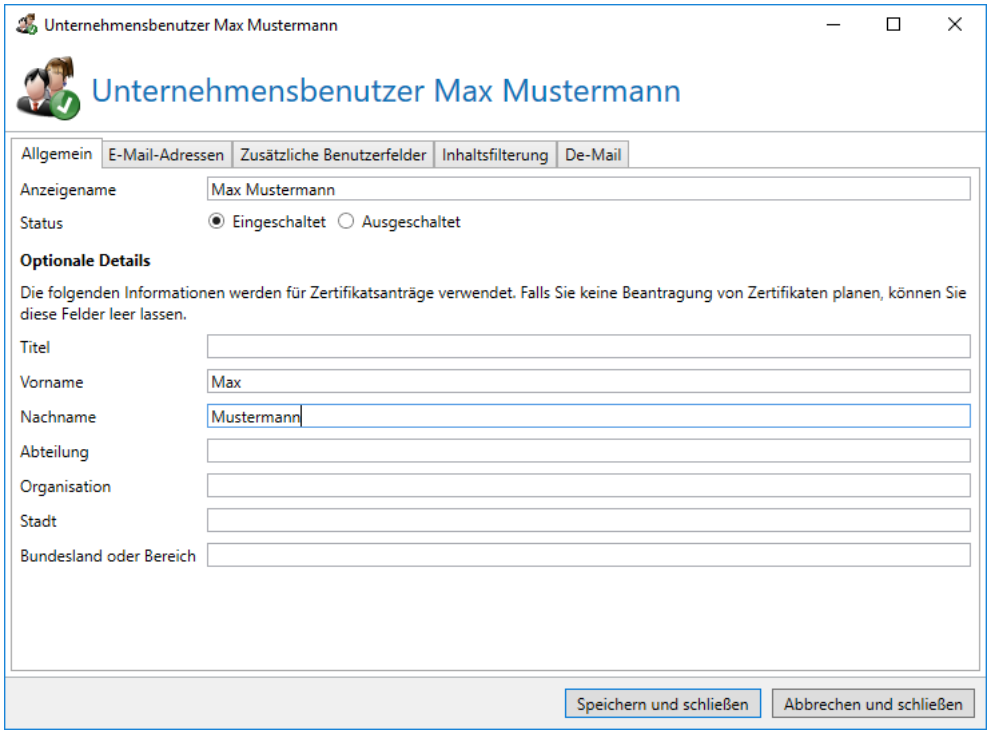


Bild 33: Der Name und die Daten des Benutzers

Geben Sie im nächsten Schritt alle E-Mail-Adressen des Benutzers ein (Bild 34).

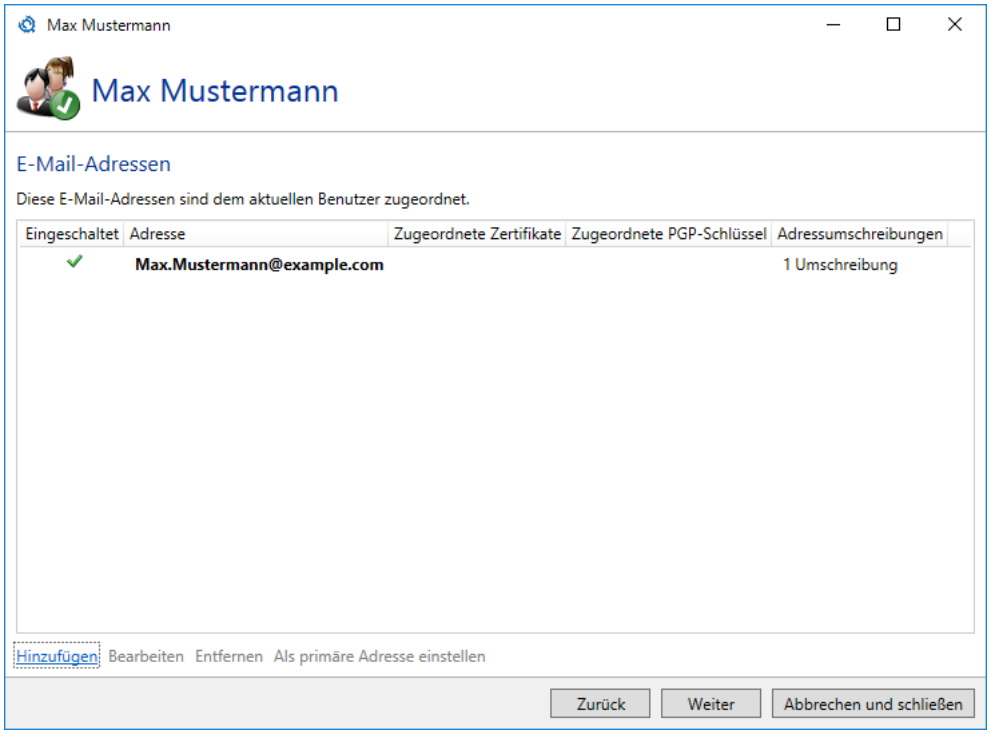


Bild 34: Alle E-Mail-Adressen, die dem Benutzer zugeordnet sind

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 35).

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.

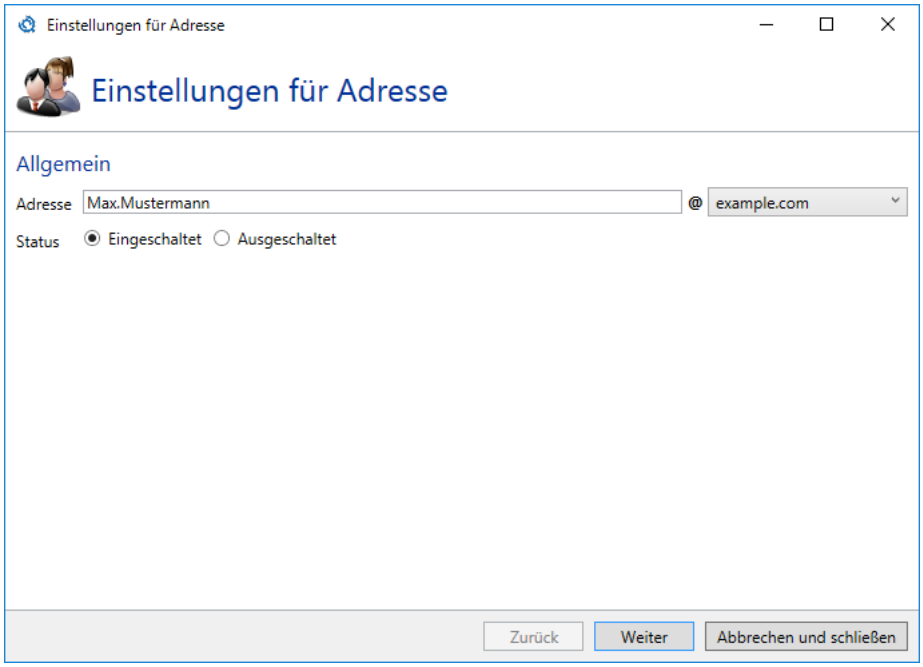


Bild 35: Eingabe einer neuen E-Mail-Adresse

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.

In den nächsten Schritten werden alle Zertifikate und PGP-Schlüssel angezeigt, die ebenfalls die eingegebene E-Mail-Adresse besitzen. Sie können hier Signatur- und Verschlüsselungsschlüssel für die Adresse auswählen. Das Bearbeiten der Zertifikate einer Benutzer E-Mail-Adresse wird im Abschnitt Kryptographische Schlüssel in den eigenen Domänen und den Unternehmensbenutzern beschrieben.

Der letzte Schritt (Bild 36) bestimmt alle Adressumschreibungen für diese E-Mail-Adresse.

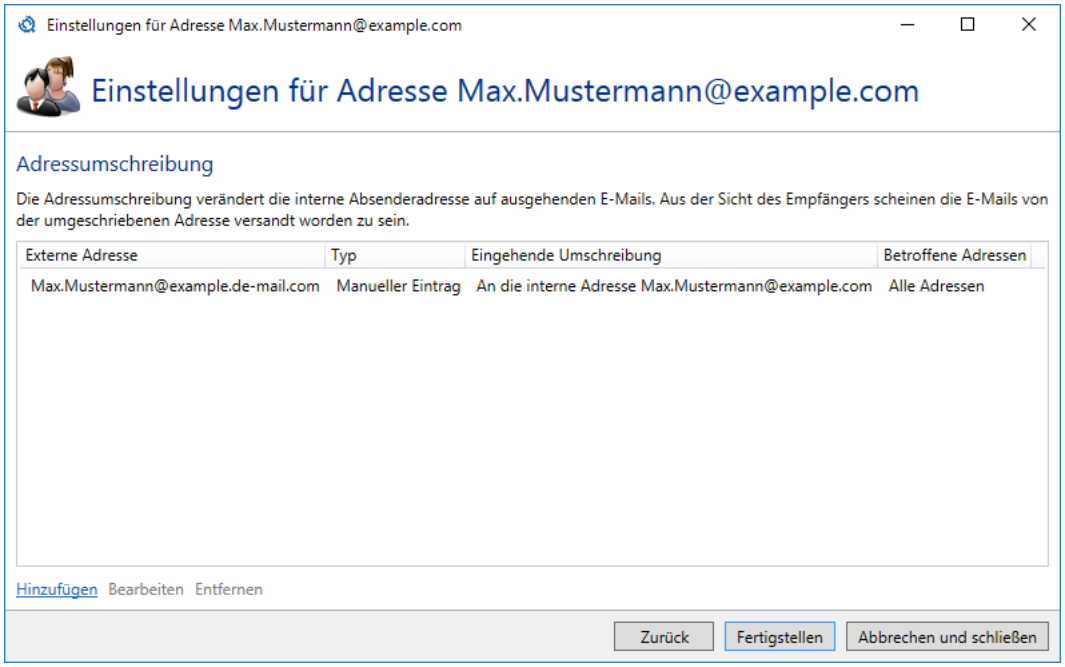


Bild 36: Die Liste aller Adressumschreibungen

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 37). Sie können entweder die übergeordneten Einstellungen verwenden, alle Anhänge zulassen, oder einen auf dem Knoten **Voreinstellungen** konfigurierten Inhaltsfilter auswählen.

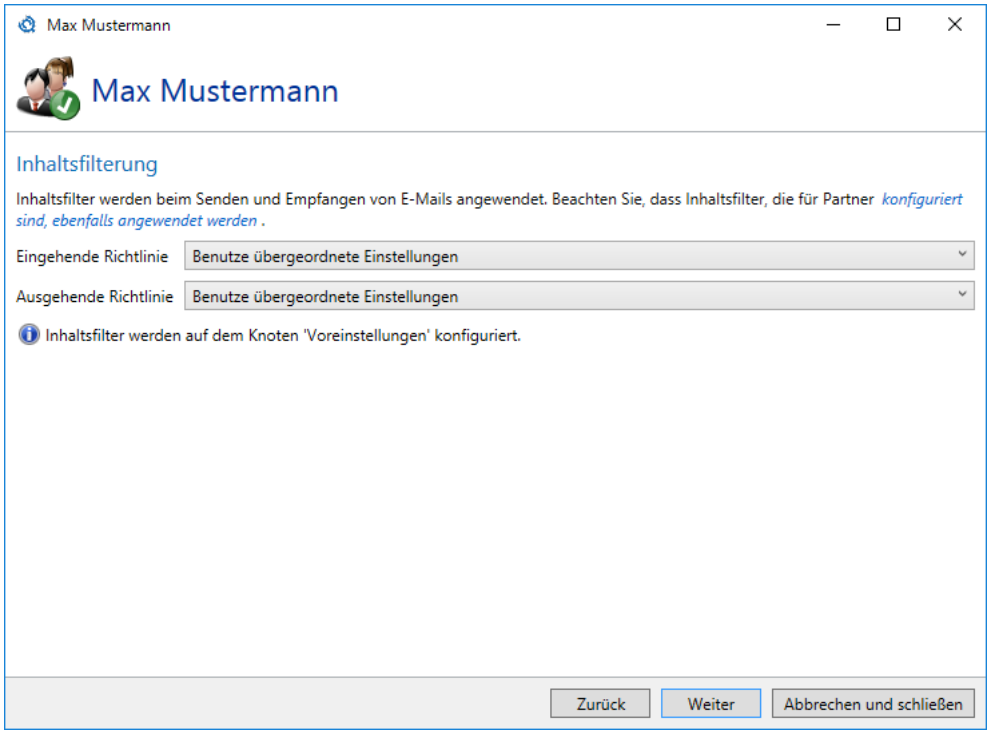


Bild 37: Konfiguration der Inhaltsfilter für den Benutzer

Auf der Seite **De-Mail** (Bild 38) 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.

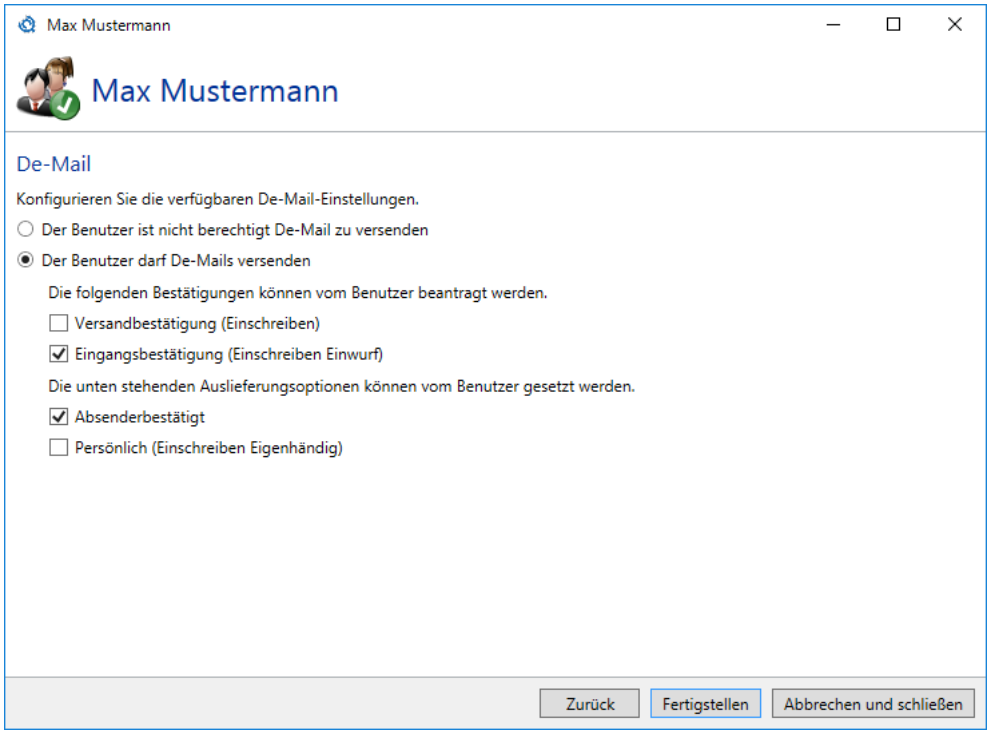


Bild 38: Verfügbare De-Mail-Funktionen für den Benutzer

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 39). Wählen Sie danach, wie E-Mails an lokale Adressen behandelt werden.

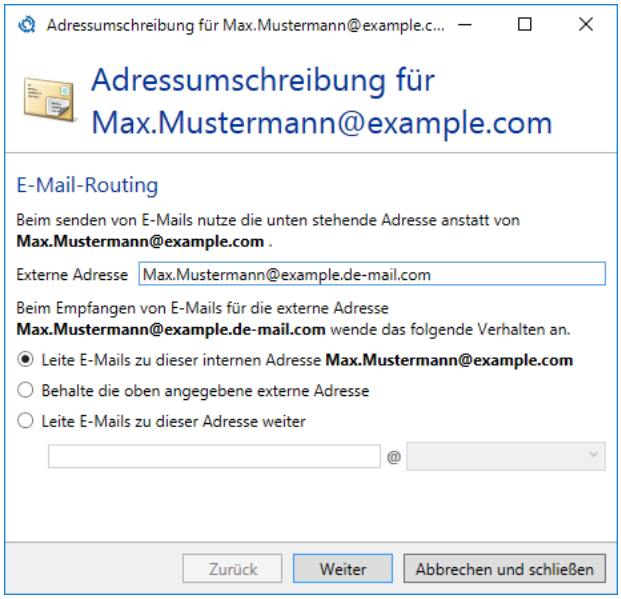


Bild 39: Externe und lokale Adressen

Im nächsten Schritt wird ausgewählt, bei welchen Empfängeradressen diese Umschreibung genutzt wird (Bild 40). Entspricht die Empfängeradresse nicht Ihrer Auswahl, wird die Adressumschreibung nicht ausgeführt. In der Auswahl **Eine Adresse mit dem Muster** können Sie Platzhalter ('*' und '?') nutzen.

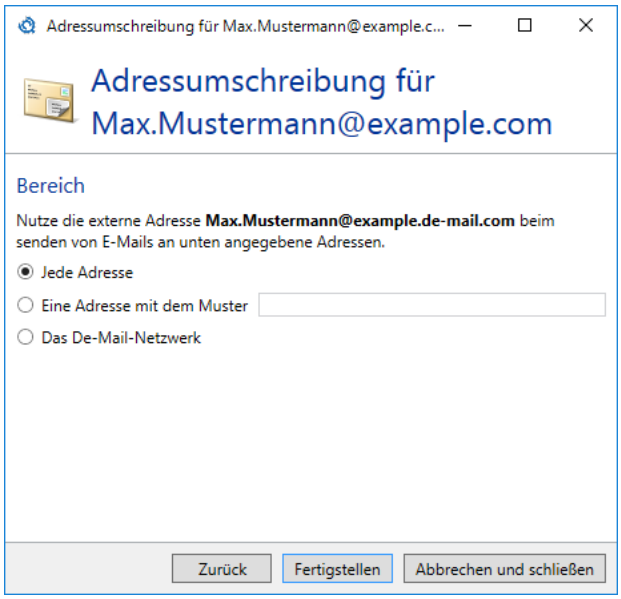


Bild 40: Gewählte Empfängeradressen dieser Umschreibung

Das Löschen von Benutzern ist für replizierte Benutzer nicht verfügbar.

Kryptographische Schlüssel für die markierten Benutzer beantragen

Wenn Sie Anbieter für kryptographische Schlüsselanforderungen konfiguriert haben, können Sie über NoSpamProxy Encryption Zertifikate und PGP-Schlüssel für die E-Mail-Adressen der Unternehmensbenutzer erstellen lassen.

Wählen Sie für die Erstellung der E-Mail-Zertifikate die entsprechenden Benutzer in der Liste der Unternehmensbenutzer aus und danach die Funktion **Kryptographische Schlüssel für die markierten Benutzer beantragen**. Es erscheint der Dialog für Anforderungen von kryptographischen Schlüsseln (Bild 41).

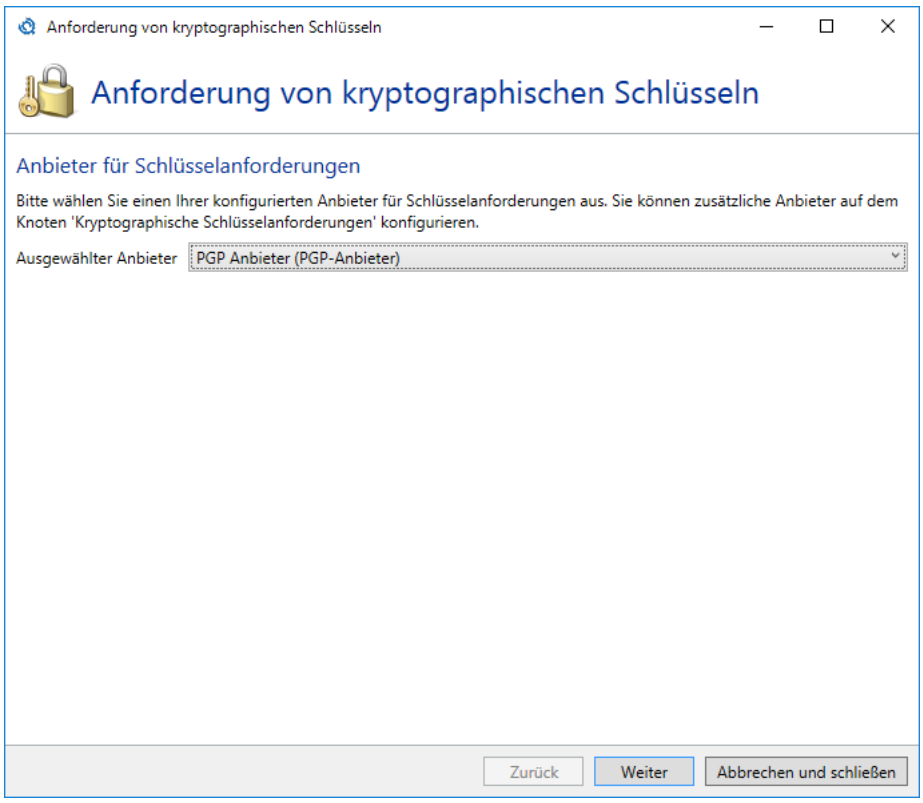


Bild 41: Die Auswahl des Anbietertyps

Wählen Sie einen der konfigurierten Schlüsselanbieter. In der Auswahlliste wird der Name des Anbieters und der Typ der Schlüsselbereitstellung angezeigt. Danach kommen Sie mit **Weiter** zu den ausgewählten Benutzern (Bild 42).

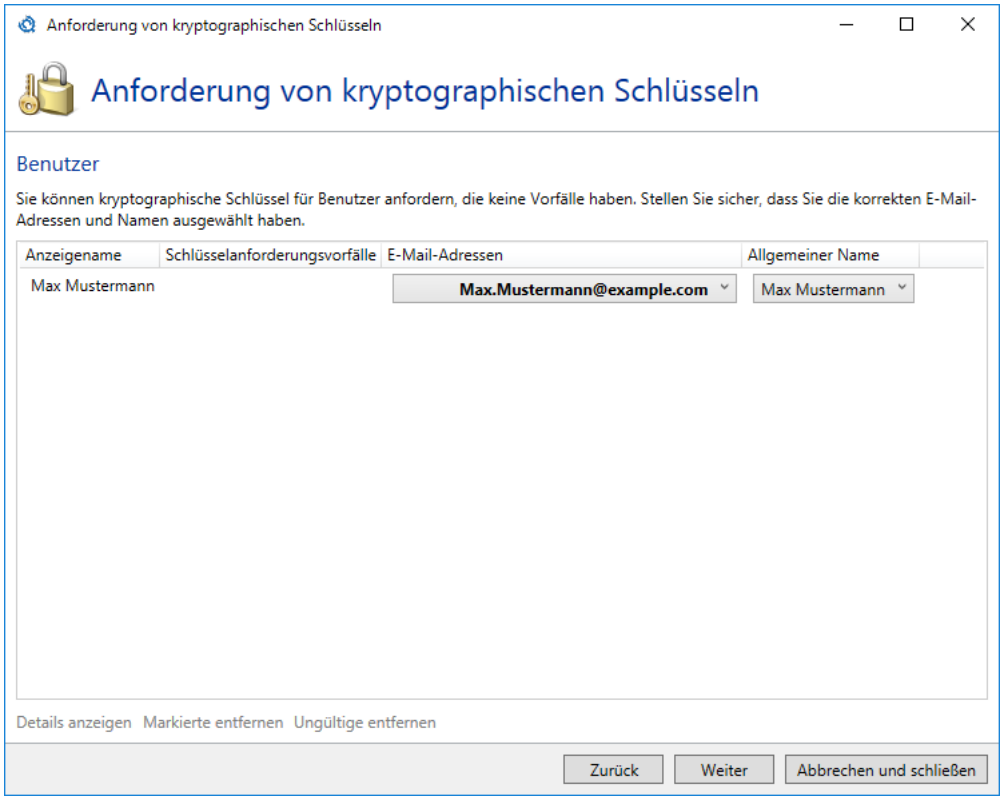


Bild 42: Die Benutzer, die in der Auswahl vorhanden sind

In der Spalte **Schlüsselanforderungsvorfälle** (in der Liste der gewählten Benutzer) werden alle Eigenschaften des Benutzers aufgelistet, die eine erfolgreiche Schlüsselanforderung verhindern würden. Problematische Eigenschaften sind zum Beispiel zu lange Namen oder unüblich lange E-Mail-Adressen. Sind Benutzer mit solchen Eigenschaften in der Auflistung vorhanden, müssen diese vor der Beantragung der Schlüssel aus der Liste entfernt werden. Das kann automatisch mit der Funktion **Entferne ungültige Benutzer aus der Schlüsselanforderung** oder manuell durch die Auswahl der betroffenen Benutzer und die Funktion **Entferne ausgewählte Benutzer aus der Schlüsselanforderung** erfolgen.

In den Spalten **E-Mail-Adresse** und **Allgemeiner Name** sind alle für den ausgewählten Benutzer vorhandenen Einträge aufgelistet. Ist eine Adresse als primäre E-Mail-Adresse markiert, so ist sie hervorgehoben. Vor den jeweiligen E-Mail-Adressen befinden sich ggf. Bilder für die bereits vorhandenen kryptographischen Schlüssel. Das linke Bild zeigt an, ob Zertifikate mit der E-Mail-Adresse verknüpft sind, das rechte Bild zeigt das Vorhandensein von PGP-Schlüsseln. Beide Bilder geben keine Auskunft über den Zustand der Zertifikate oder die derzeitige Art der Verwendung. Überprüfen Sie vor der Schlüsselanforderung ob die für die Zertifikatserstellung richtigen E-Mail-Adressen und allgemeinen Namen ausgewählt sind. Die kryptographischen Schlüssel werden beim Schließen des Dialogs beantragt und erscheinen nach Ihrer Fertigstellung unter den Unternehmensbenutzer.

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 43).

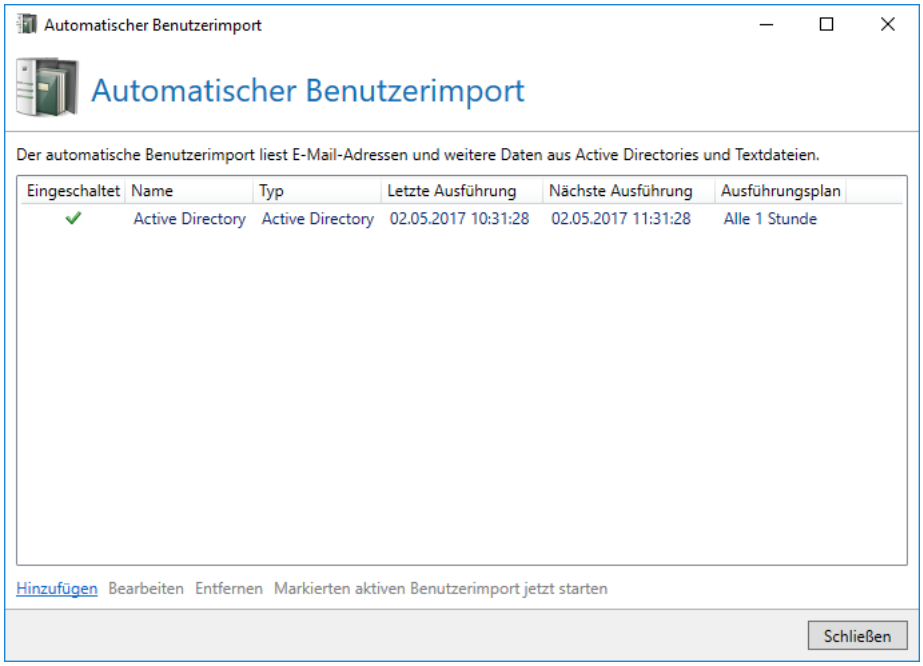


Bild 43: Die Liste aller eingerichteten Benutzerimporte

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 44). Sie können aus dem Active Directory, einer generischen LDAP-Quelle, wie zum Beispiel Lotus Notes, oder einer Textdatei importieren.

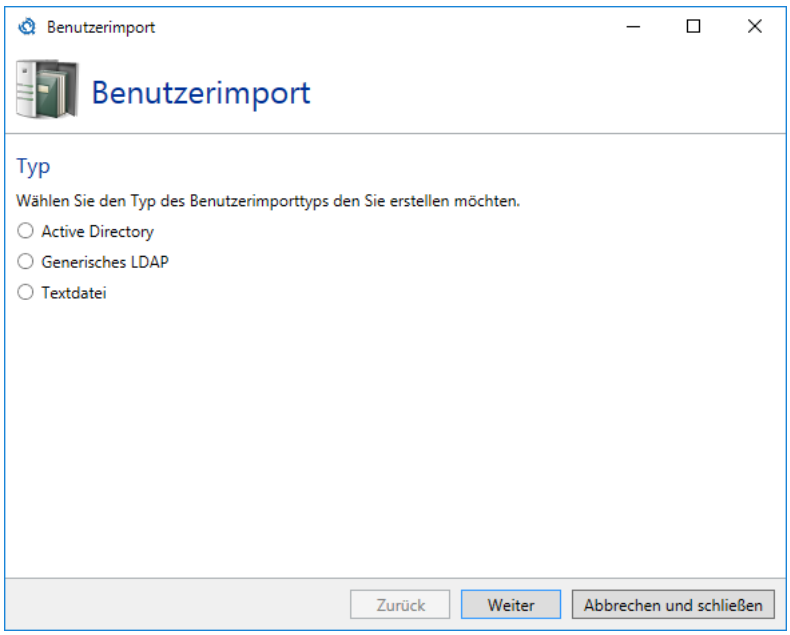


Bild 44: Typ des Benutzerimports

Im Schritt **Allgemein** (Bild 45) 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.

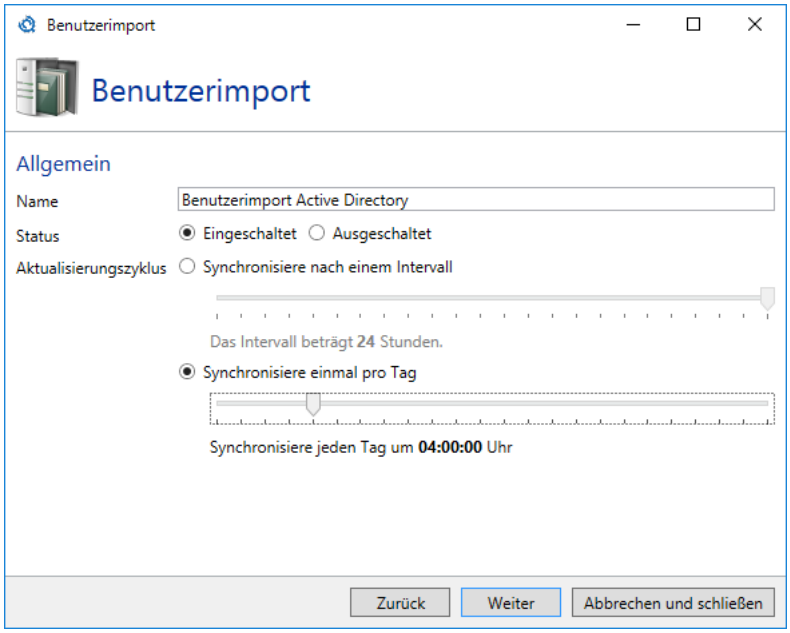


Bild 45: Allgemeine Einstellungen

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 46). 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.

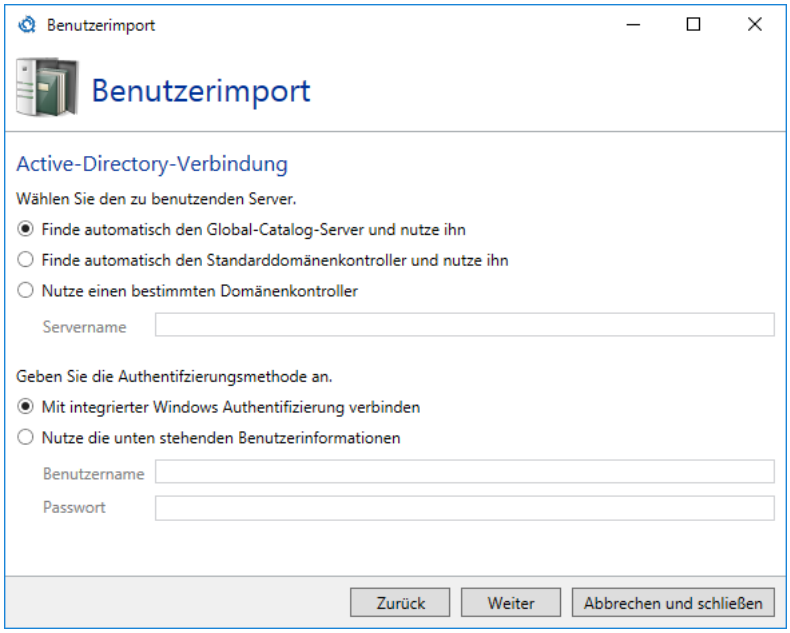


Bild 46: Die Verzeichnisverbindung

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.

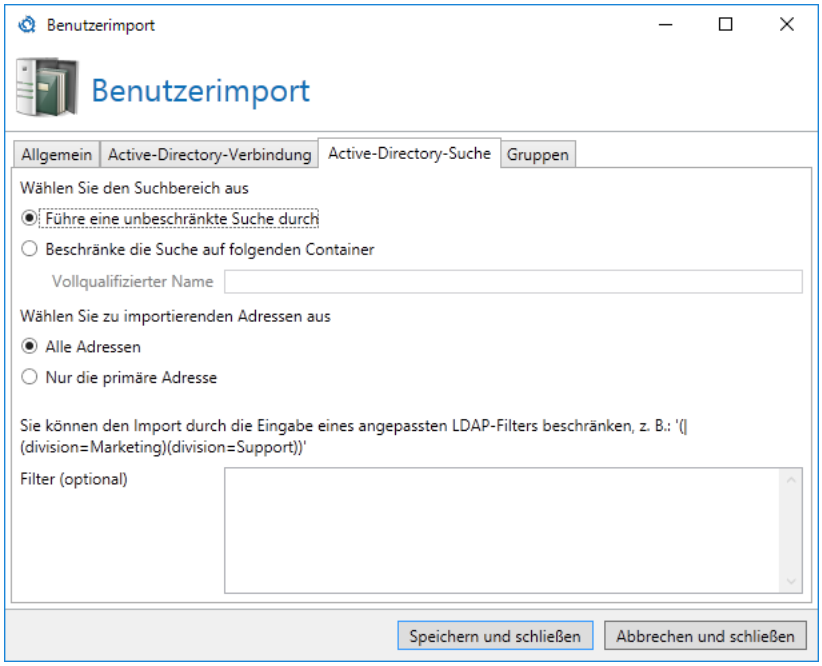


Bild 47: Die Auswahl der zu importierenden Active Directory Benutzer

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 48) geben Sie an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.

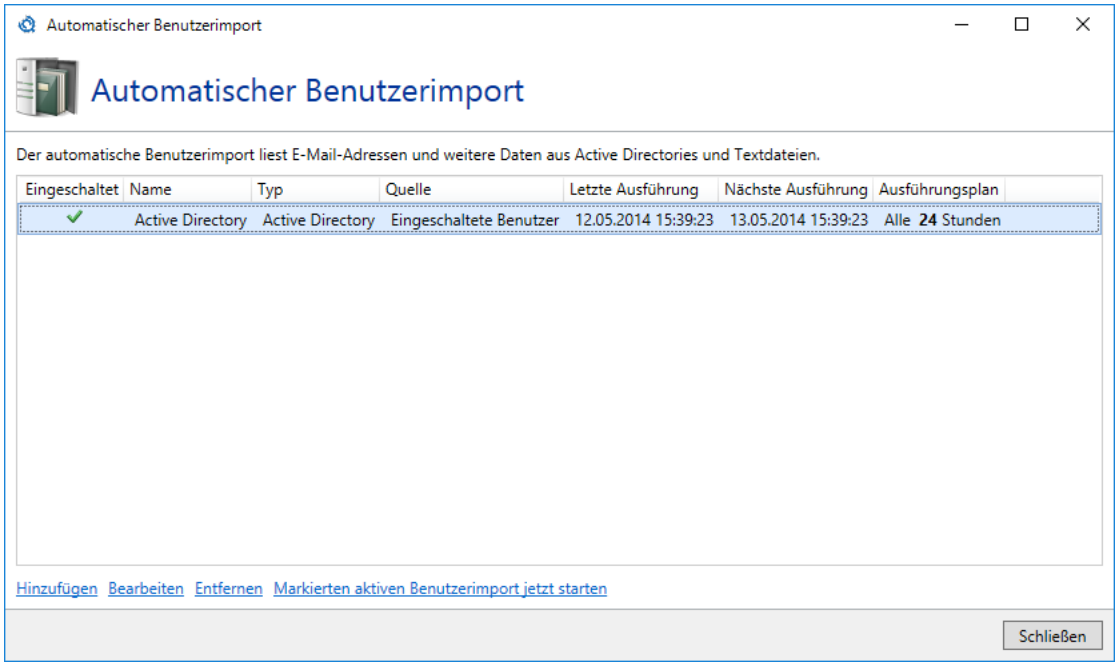


Bild 48: Berechtigte Gruppen für De-Mail

Generisches LDAP

Die **LDAP-Verbindung** (Bild 49) baut die Verbindung zu Ihrem Server auf. Geben Sie den Server und die zu benutzenden Anmeldeinformationen ein.

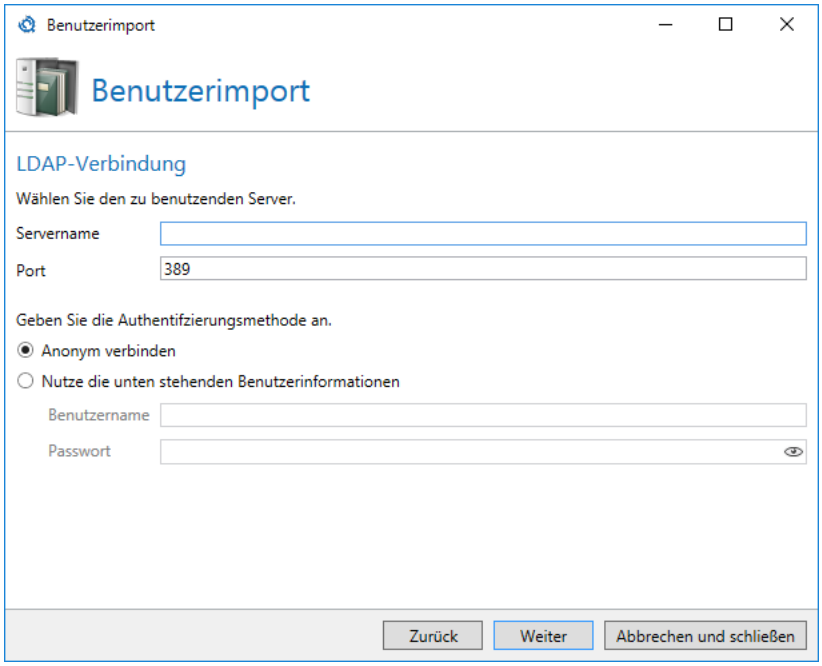


Bild 49: Verbindung zum LDAP-Server

In der **LDAP-Suche** (Bild 50) 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.

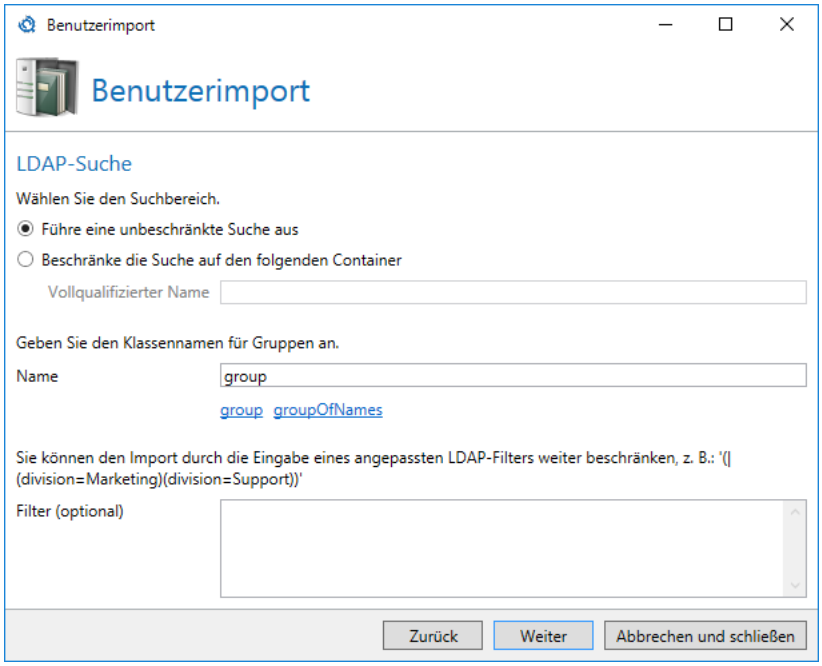


Bild 50: Anpassen der LDAP-Suche

Auf der Seite der **LDAP-Adressfelder** können Sie zusätzliche LDAP-Felder angeben, in denen nach E-Mail-Adressen gesucht werden soll (Bild 51). Dies ist notwendig, falls Ihr System die E-Mail-Adressen nicht in den Standardfeldern 'mail' bzw. 'otherMailBox' speichert.

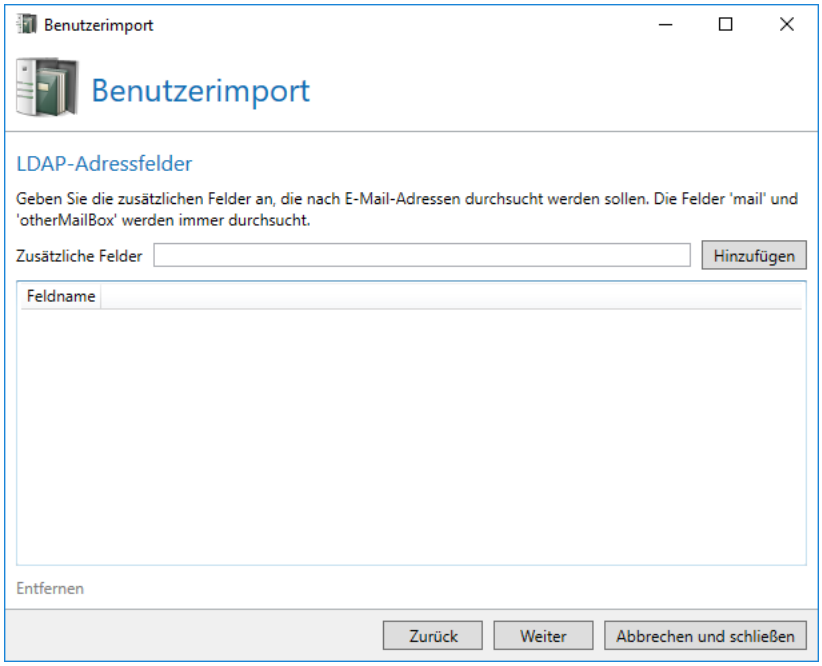


Bild 51: Konfiguration zusätzlicher Adressfelder

In den **Gruppen** geben Sie an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf (Bild 52). Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.

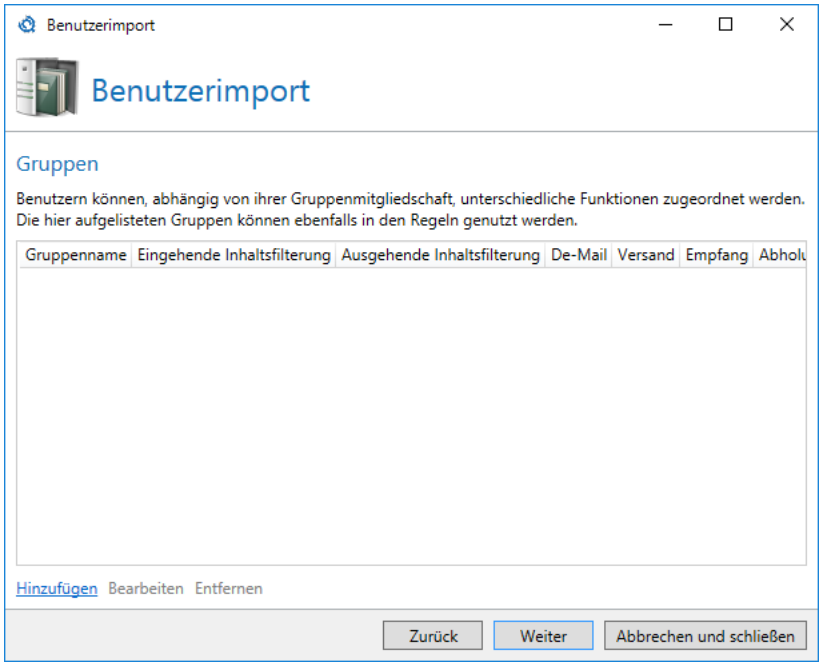


Bild 52: Berechtigte Gruppen für De-Mail

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 53).

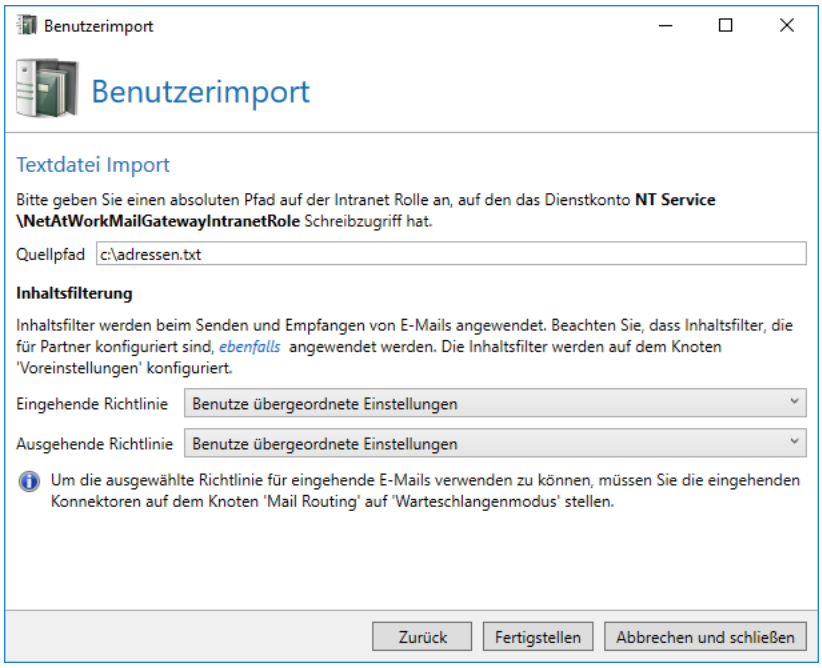


Bild 53: Die Angabe des Pfads zur Textdatei

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.

Neue Gruppe im Benutzerimport

Um Funktionen von NoSpamProxy für Benutzergruppen freizugeben, muss die Active-Directory-Verbindung oder die LDAP-Verbindung konfiguriert sein. Suchen Sie nach der Gruppe, die Sie berechtigen wollen und wählen Sie diese dann aus (Bild 54).

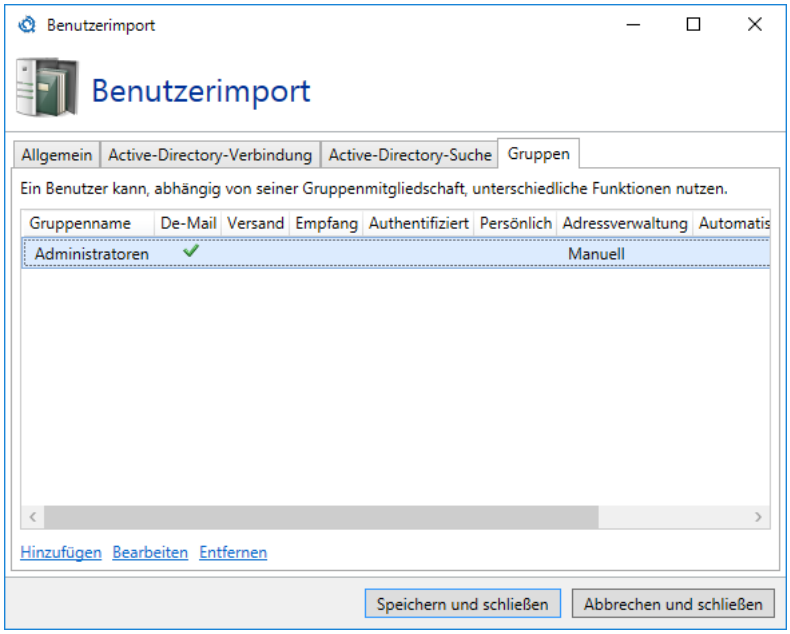


Bild 54: Die Auswahl der Benutzergruppen

Bei lizenziertem NoSpamProxy Large Files oder NoSpamProxy Protection können Sie für jede Gruppe die verwendeten Inhaltsfilter auswählen. Diese werden auf dem Knoten Inhaltsfilter definiert.

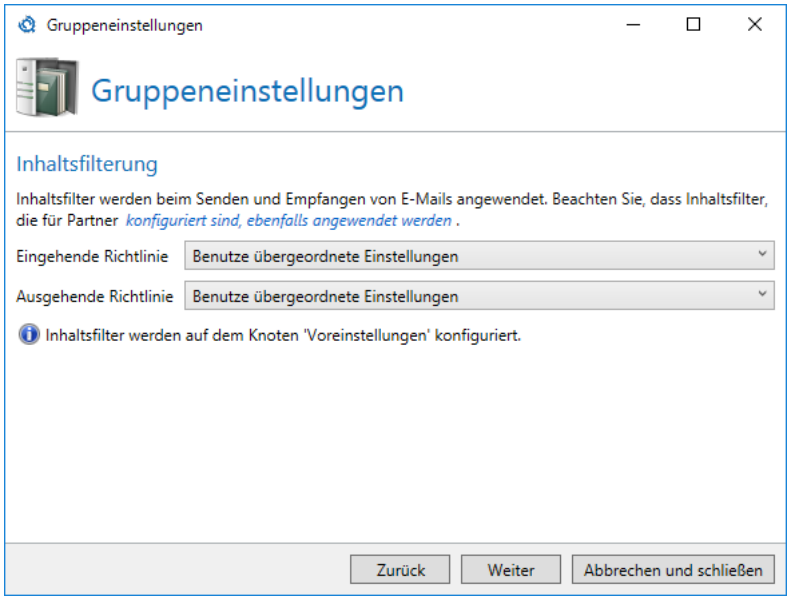


Bild 55: Die Auswahl der Inhaltsfilter

In den De-Mail Berechtigungen (Bild 56) legen Sie fest, welche De-Mail Funktionen den Mitgliedern dieser Gruppe zu Verfügung gestellt werden.

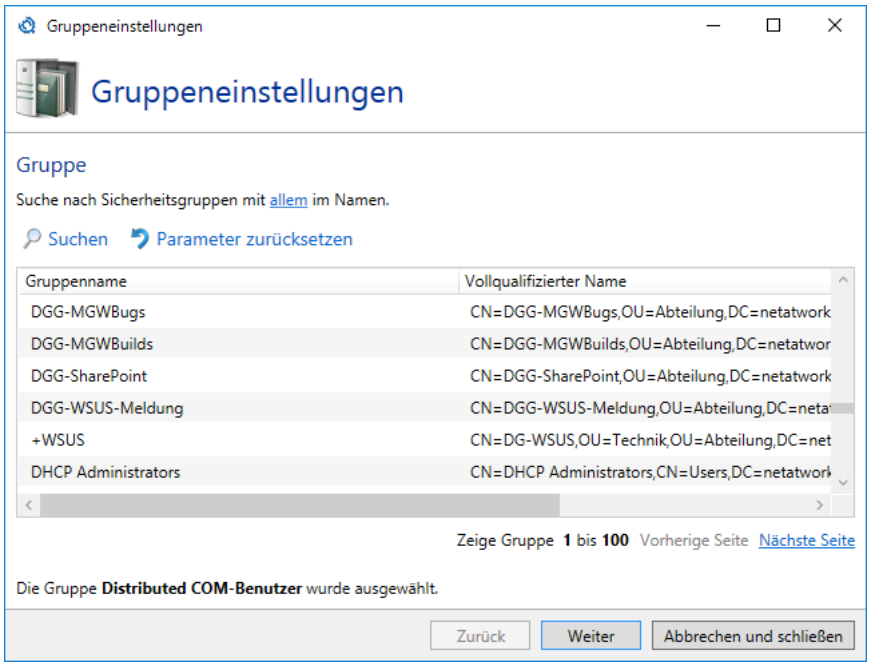


Bild 56: Berechtigungen der gewählten Gruppe auf De-Mail-Funktionen

Alle Benutzer, die De-Mail nutzen wollen, benötigen eine De-Mail-Adresse. Diese können Sie über die **Adressverwaltung** (Bild 57) nach einem Ersetzungsmuster erstellen lassen oder auch manuell über den Knoten Adressumschreibung. Für Benutzer, die keine gültige De-Mail-Adresse besitzen, wird im Ereignisprotokoll eine Warnung angezeigt.

Ist es den Mitgliedern der Gruppe nicht erlaubt De-Mails zu versenden, dann ist dieser Dialog nicht benutzbar.

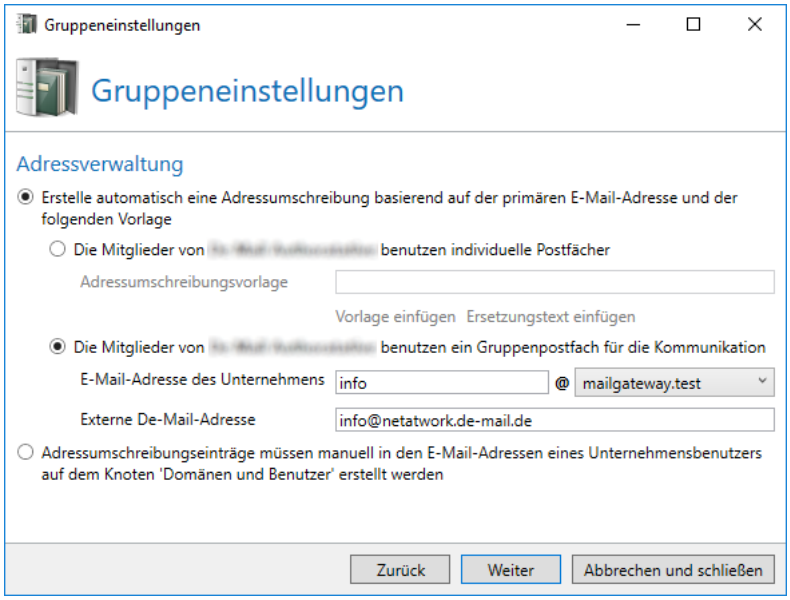


Bild 57: Die Verwaltung der De-Mail-Adressumschreibungen

Wählen Sie zunächst aus, ob die Adressumschreibung automatisch nach dem hinterlegten Muster oder manuell über den Adressumschreibungsknoten erstellt werden soll. Möchten Sie die Adressumschreibungen automatisch erstellen lassen, können Sie entweder individuelle Einträge erstellen lassen oder die Gruppen-Mailbox-Funktionalität nutzen. Bei individuellen Einträgen wird für jeden Benutzer für dessen primäre E-Mail-Adresse eine eindeutige De-Mail-Adresse generiert. Hierfür hinterlegen Sie in dem Dialog eine Vorlage, nach der die Adresse erstellt werden soll. Es stehen Ihnen die folgenden Ersetzungseinträge zur Verfügung.

- **Vorname %g**
  Bei der Benutzung von '%g' wird der Vorname des Benutzers eingesetzt. Beispielsweise wird für den Benutzer 'Eva Musterfrau' der Vorname 'Eva' eingefügt.
- **Erster Buchstabe des Vornamen %1g**
  Bei der Benutzung von '%1g' wird der erste Buchstabe des Vornamens des Benutzers eingesetzt. Sie können statt '1' auch andere Zahlen einsetzen um mehrere Buchstaben des Nachnamen zu benutzen. Beispielsweise wird für den Benutzer 'Eva Musterfrau' bei Benutzung von '%2g' der Teil 'Ev' des Vornamen eingefügt.

- **Nachname %s**
  Bei der Benutzung von '%s' wird Nachname des Benutzers eingesetzt. Beispielsweise wird für den Benutzer 'Eva Musterfrau' der Nachname 'Musterfrau' eingefügt.
- **Erster Buchstabe des Nachnamen %1s**
  Bei der Benutzung von '%1s' wird der erste Buchstabe des Nachnamens des Benutzers eingesetzt. Sie können statt '1' auch andere Zahlen einsetzen um mehrere Buchstaben des Nachnamen zu benutzen. Beispielsweise wird für den Benutzer 'Eva Musterfrau' bei Benutzung von '%7s' der Teil 'Musterf' des Nachnamen eingefügt.
- **Lokaler Teil %p**
  Bei der Benutzung von '%p' wird der lokale Teil der primären E-Mail-Adresse eingesetzt. Beispielsweise wird für die Adresse 'max.mustermann@example.com' der lokale Teil 'max.mustermann' eingefügt.
- **Domäne ohne TLD %c**
  Bei der Benutzung von '%c' wird die Domäne der primären E-Mail-Adresse ohne die Top-Level-Domain wie '.de', '.net', '.com' usw. eingesetzt. Beispielsweise wird für die Domäne 'example.com' der Domänenname 'example' eingefügt.

Nutzen Sie eine der vordefinierten Ersetzungsvorlagen und passen Sie sie ggf. an falls Sie den Ersetzungseintrag nicht vollständig manuell erstellen möchten. Alternativ kann die Gruppen-Mailbox-Funktionalität verwendet werden. In diesem Fall verwenden alle Mitglieder der Gruppe die gleiche De-Mail-Adresse. Empfangene De-Mails werden dann an eine bestimmte lokale E-Mail-Adresse geleitet.

Im Schritt **Automatische Schlüsselanforderung** (Bild 56) können Sie einen bereits konfigurierten Anbieter für kryptographische Schlüssel wie Zertifikate und PGP-Schlüssel auswählen. Die Intranet Rolle wird mit dem Anbieter einen Schlüssel erstellen, falls nicht bereits ein gültiger Schlüssel vorhanden ist.

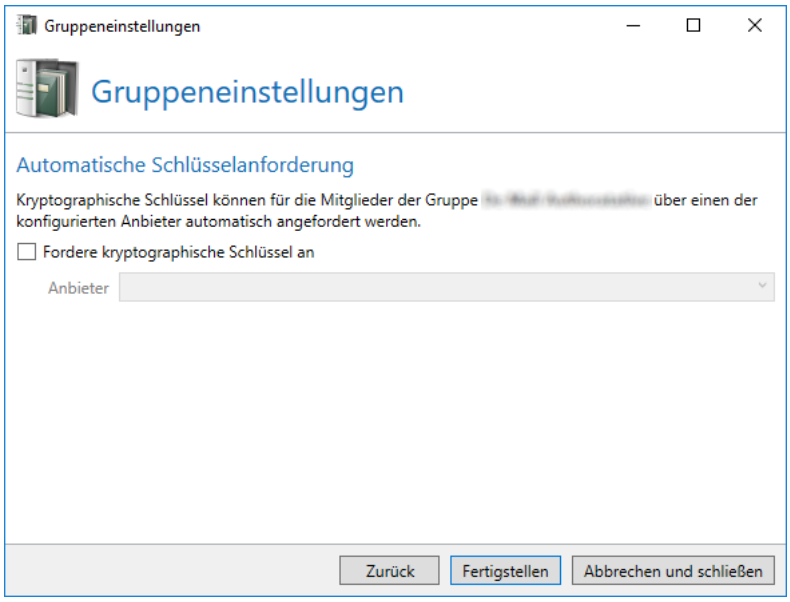


Bild 58: Auswahl des Anbieters für automatische Schlüsselanforderung

Wird ein Benutzer aus der Gruppen entfernt, werden automatisch angeforderte Zertifikate und PGP-Schlüssel nicht zurückgezogen. Dies muss der Administrator des System manuell tun.

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 59) für E-Mail-Anhänge gewählt werden. Inhaltsfilter werden auf dem Knoten Inhaltsfilter definiert.

Des Weiteren kann die bevorzugte Ende-zu-Ende-Verschlüsselung gewählt werden.

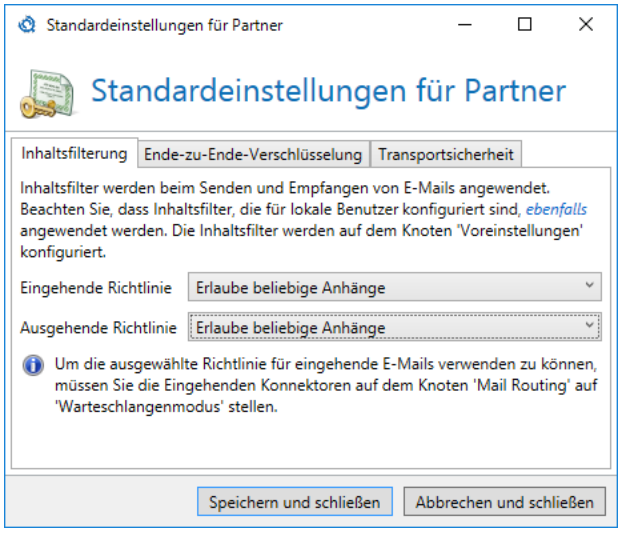


Bild 59: Standardeinstellung der Inhaltsfilter

Für die Ende-zu-Ende-Verschlüsselung (Bild 60) wird NoSpamProxy Encryption benötigt.

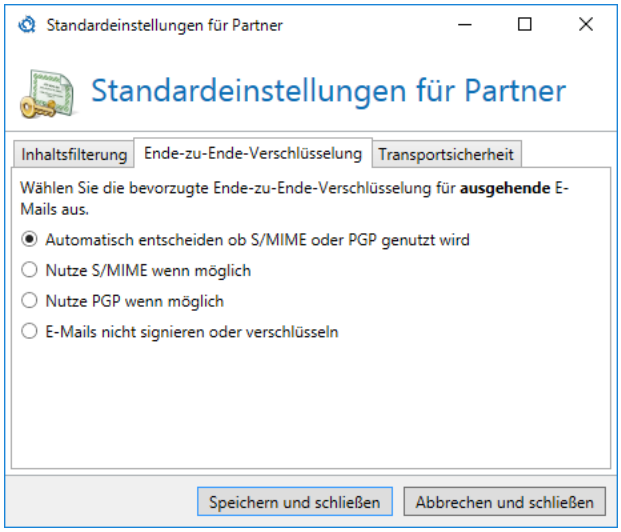


Bild 60: Standardeinstellung für die Ende-zu-Ende-Verschlüsselung

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 61). 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.

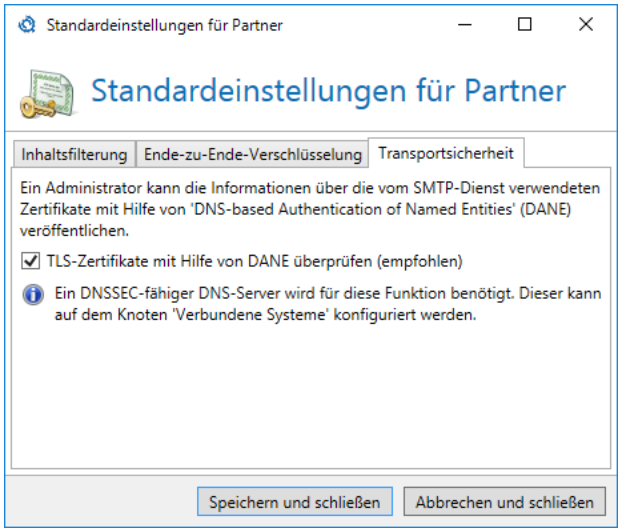


Bild 61: Einstellung für DANE mit TLS-Zertifikaten

Partnerdomänen

Die Liste der Partner ist nach den Domänen gruppiert (Bild 62). Jede Domäne beinhaltet einerseits Einstellungen für Inhaltsfilter und Ende-zu-Ende-Verschlüsselung sowie die notwendige Transportsicherheit.

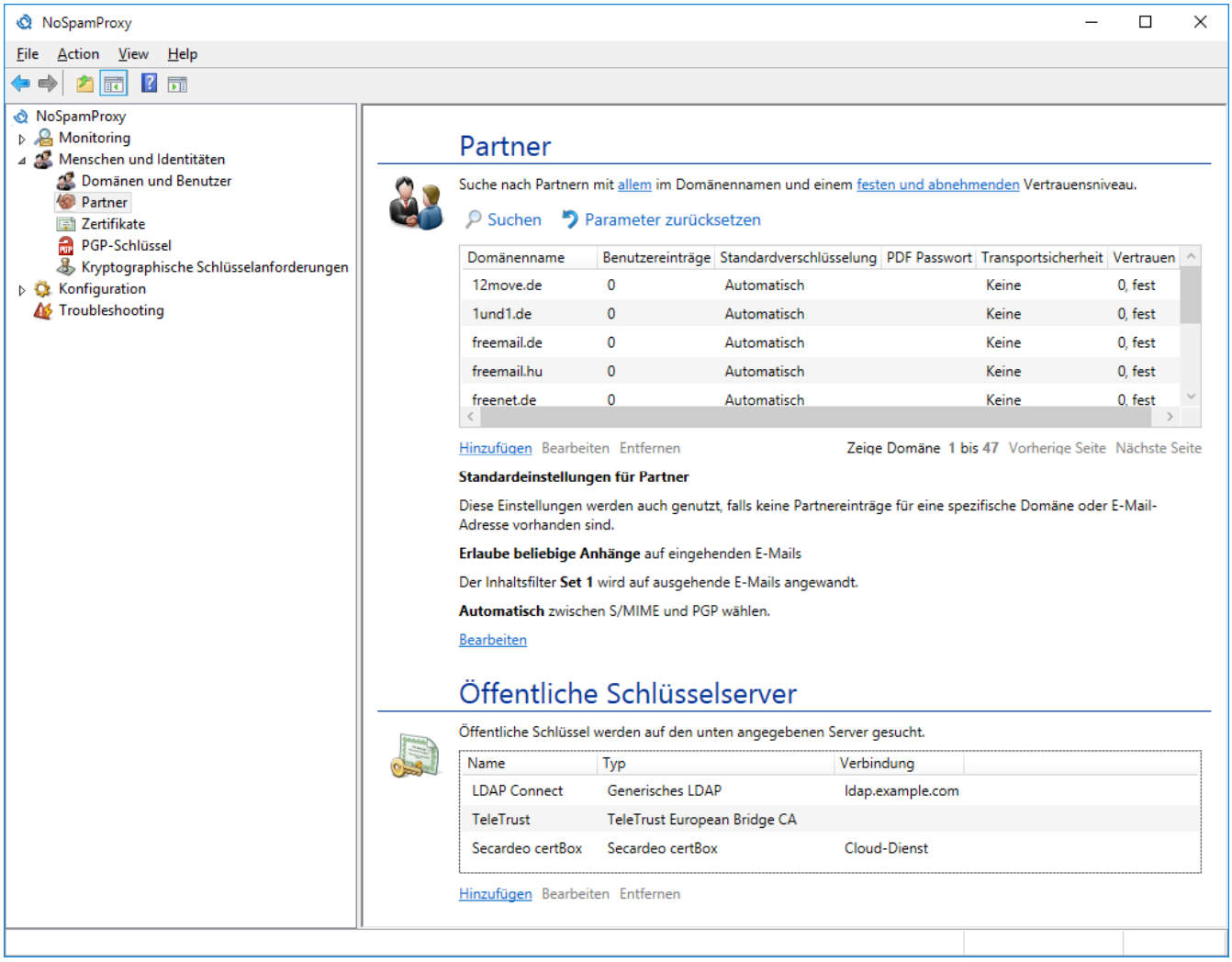


Bild 62: Die Übersicht über alle Partner

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.

In den Benutzereinträgen stehen Einstellungen für den anzuwendenden Inhaltsfilter, die erforderliche Ende-zu-Ende-Verschlüsselung und die der E-Mail-Adresse zugeordneten Zertifikate und PGP-Schlüssel. Die tatsächlich verfügbaren Funktionen sind abhängig von Ihrer Lizenz.

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.

In der **Ende-zu-Ende-Verschlüsselung** einer Domäne legen Sie die Anforderungen für die Verschlüsselung und Signatur der Nachricht fest. Hier können Sie auch die zur Verschlüsselung sowie

Signatur genutzten Zertifikate und PGP-Schlüssel auswählen. Zusätzlich kann hier ein Passwort für den Schutz von PDF-Nachrichten hinterlegt werden.

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.

Neue Partnerdomäne

Beim Hinzufügen einer Partnerdomäne geben Sie zuerst den Domänennamen an (Bild 63). Der Domänenname muss hier mit US-ASCII-Zeichen geschrieben werden.

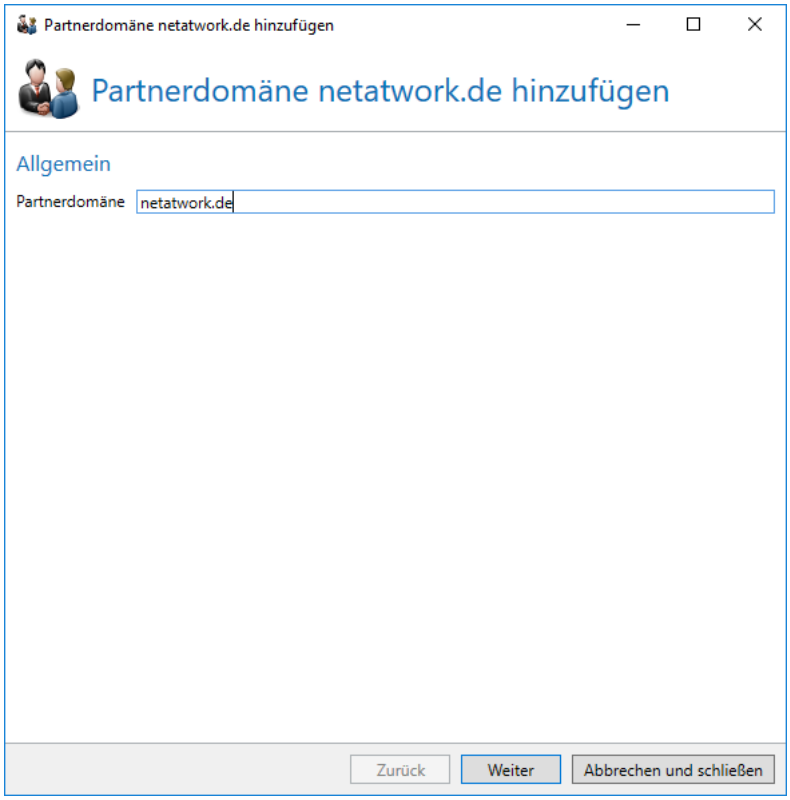


Bild 63: Der Domänenname

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.

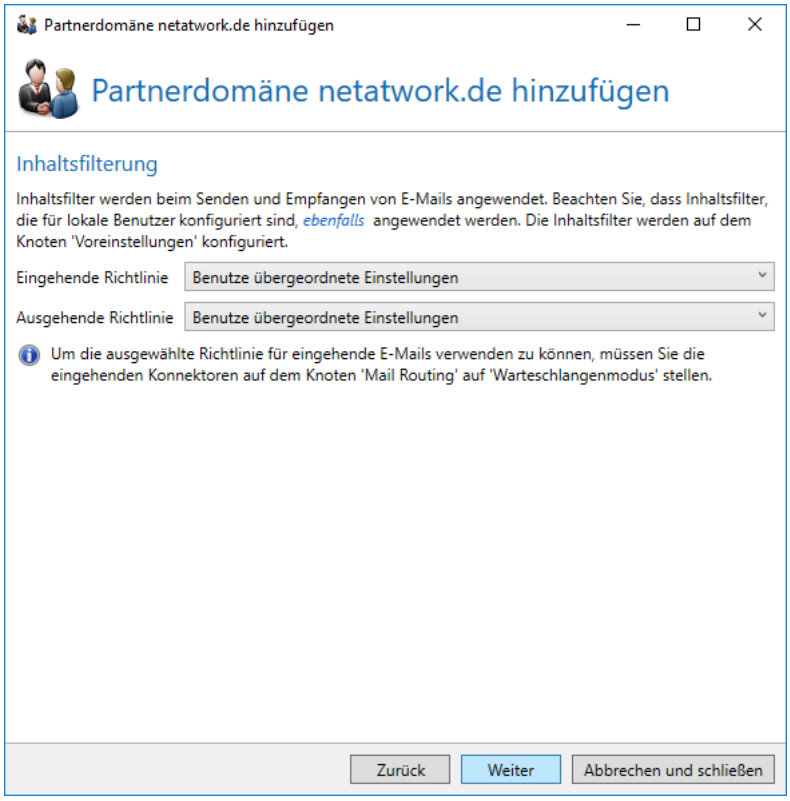


Bild 64: Konfiguration der Inhaltsfilter

Legen Sie danach die bevorzugte **Ende-zu-Ende-Verschlüsselung** fest (Bild 65). Sie können hier auch die genutzten S-MIME-Algorithmen auf bestimmte Wert festlegen. Diese Funktion wird zum Beispiel eingesetzt, wenn der E-Mail-Server des Partners einen Algorithmus vorschlägt, den er selbst nicht einwandfrei verarbeiten kann.

Wenn für den Partner sowohl S/MIME-Zertifikate als auch PGP-Schlüssel verfügbar sind, werden S/MIME Zertifikate beim Versand und Empfang von E-Mails bevorzugt.

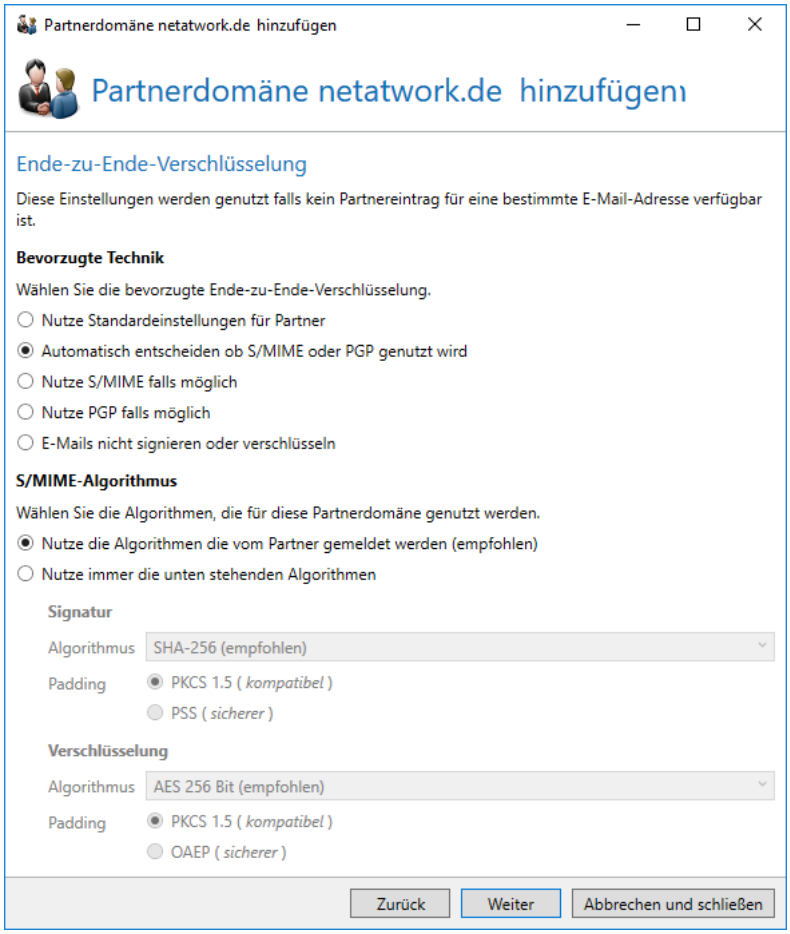


Bild 65: Ende-zu-Ende-Verschlüsselung

Auf der Seite **PDF Mail** kann ein Passwort festgelegt, geändert oder gelöscht werden (Bild 66). Falls bereits ein Passwort über ein Web Portal durch den Benutzer hinterlegt wurde, wird es hier als hinterlegt angezeigt.

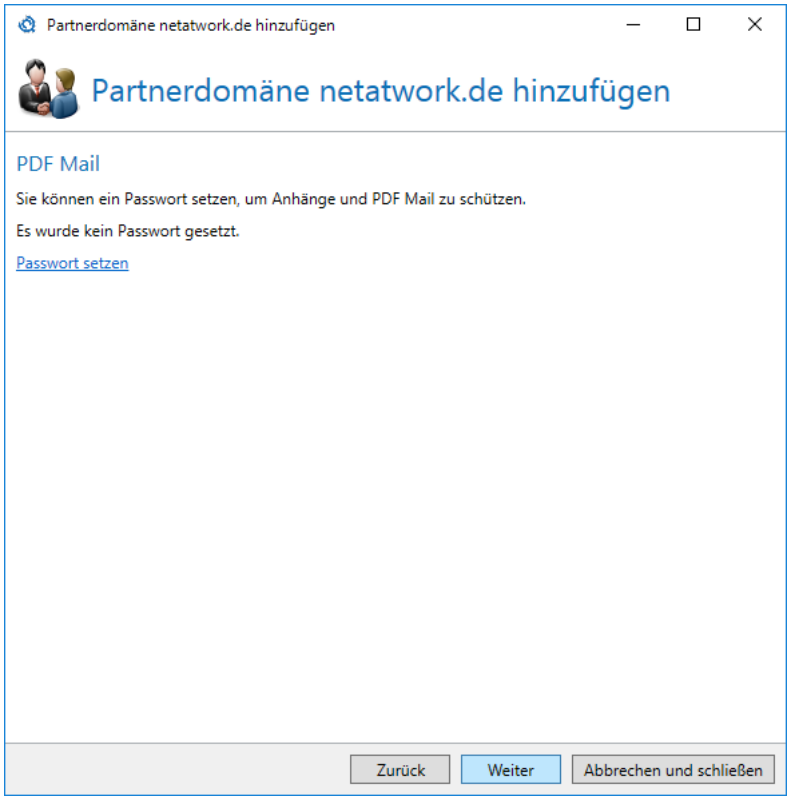


Bild 66: PDF-Passwort

Die Transportsicherheit legt fest, ob die Kommunikation zu den Server der Partnerdomäne verschlüsselt erfolgen muss und welchen Zertifikaten gegebenenfalls vertraut wird (Bild 67). Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielserver eingesetzt werden können. Zum Deaktivieren der Transportsicherheit müssen Sie die Häkchen aus allen Kontrollkästchen entfernen.

Der Begriff **Transportsicherheit** beschreibt den Schutz einer E-Mail vor dem Abhören Dritter während des Transports vom sendenden E-Mail-Server zum empfangenden. Im Gegensatz dazu definiert **Ende-zu-Ende-Verschlüsselung** die Absicherung einer E-Mail durch S/MIME-Zertifikate oder PGP-Schlüssel beim Versand vom Absender bis zum Empfänger. Beide Verschlüsselungen können beliebig kombiniert werden.

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.

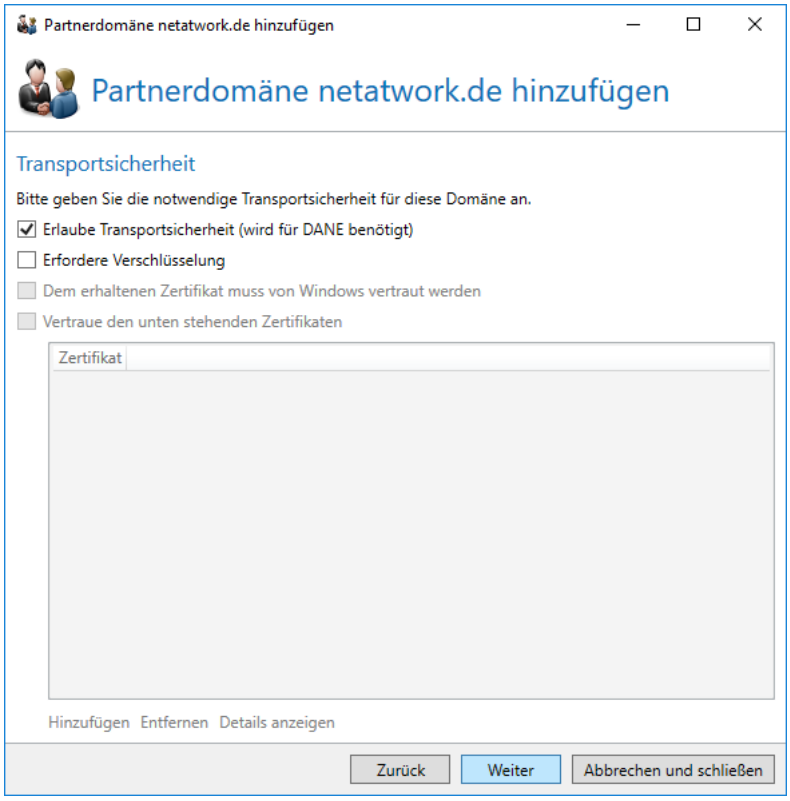


Bild 67: Transportsicherheit

Partnerdomäne bearbeiten

Beim Bearbeiten eines Partners können die Einstellungen aus der Domäne angepasst werden. Beim Bearbeiten eines Partners sind zusätzliche Bereiche verfügbar.

Die Ende-zu-Ende-Verschlüsselung bietet die Konfiguration der Domänenzertifikate und PGP-Schlüssel. Diese Schlüssel gelten für alle Partner-E-Mail-Adressen, die keine eigenen Schlüssel haben.

In Einzelfällen kann es vorkommen, das sich die verwendeten Verschlüsselungs- und Signaturalgorithmen innerhalb einer Domäne durch unterschiedliche eingesammelte oder importierte Zertifikate unterscheiden. Um diese auf denselben Stand zu setzen, nutzen Sie den Link **S/MIME Algorithmen zurücksetzen** auf der Karteikarte **Domäneneintrag**.

Zertifikate werden über die Zertifikats- oder PGP-Schlüsselverwaltung importiert. Alle öffentlichen End-Zertifikate werden in den Partnern angezeigt.

Falls Sie ein Zertifikat oder PGP-Schlüssel zu einem Domänen-Schlüssel heraufstufen wollen, gehen Sie bitte zu der Partner-E-Mail-Adresse, die diesen Schlüssel besitzt und wählen dort die Funktion **Zum**

Domänenzertifikat/PGP-Schlüssel heraufstufen. Dadurch verschiebt NoSpamProxy Encryption das heraufgestufte Zertifikat vom Eintrag für die E-Mail-Adresse in den Domäneneintrag.

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.

Sobald ein kryptographischer Schlüssel oder ein Web Portal Passwort für einen bisher unbekannten Partner hinterlegt wird, wird automatisch ein neuer Eintrag für diesen Partner angelegt.

Zuerst wird die E-Mail-Adresse eingegeben (Bild 68). 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.

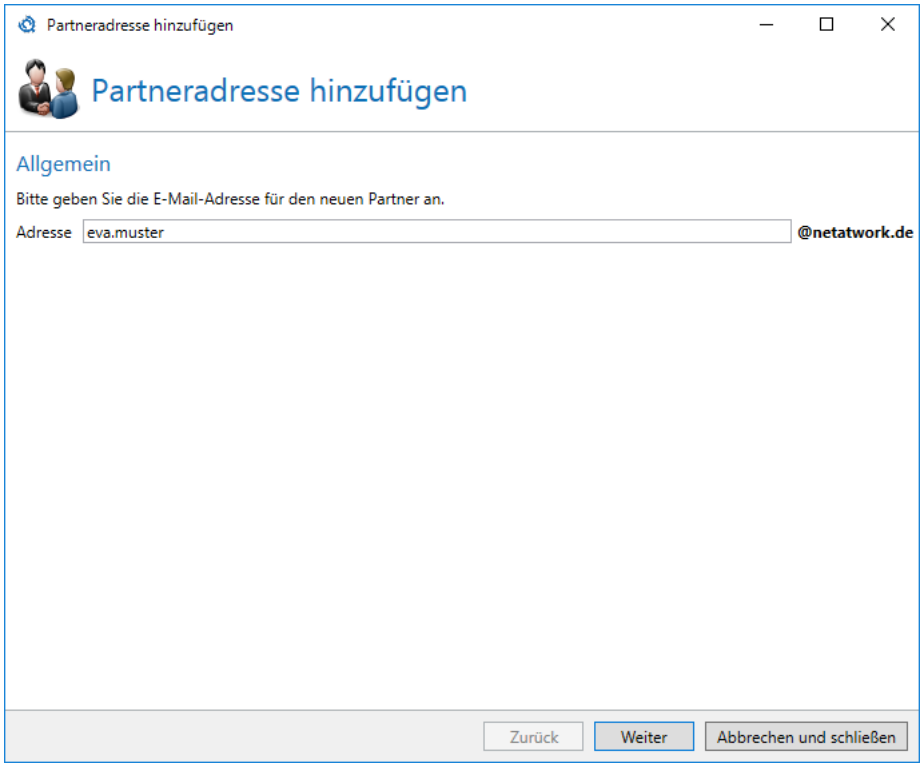


Bild 68: Hinzufügen einer E-Mail-Adresse eines Partners

Im nächsten Schritt legen Sie einen Inhaltsfilter fest.

Die Ende-zu-Ende-Verschlüsselung definiert Einstellungen, die für diese E-Mail-Adresse gelten. Diese Einstellungen überstimmen Einstellungen auf Domänenebene.

Beim **Bearbeiten** eines Benutzereintrags erscheinen analog zum Bearbeiten einer Partnerdomäne die Karteikarten mit den zugeordneten **Zertifikaten** und den **PGP-Schlüsseln**. Die Einstellungen für eine E-Mail-Adresse haben Vorrang vor den Einstellungen der Domäne.

Das Löschen von kryptographischen Schlüsseln aus einem Partner löscht diese Schlüssel endgültig aus NoSpamProxy. Falls Sie die Schlüssel zu einem späteren Zeitpunkt erneut verwenden wollen, sollten Sie sie vorher unter der Zertifikats- oder PGP-Schlüsselverwaltung exportieren.

Das Löschen einer Partnerdomäne oder eines E-Mail-Adresse eines Partners löscht ebenfalls alle dort zugeordneten Schlüssel. Falls Sie diese Schlüssel zu einem späteren Zeitpunkt erneut benötigen, sollten Sie diese exportieren.

Öffentliche Schlüsselserver

Ist bei einer E-Mail an externe Adressen kein Zertifikat oder PGP-Schlüssel für diese vorhanden, so kann NoSpamProxy Encryption einen Schlüssel suchen. Hierfür werden öffentliche Schlüsselserver befragt.

Um Zertifikate und PGP-Schlüssel über Secardeo certBox suchen zu lassen, müssen Sie einen Vertrag mit der Firma Secardeo abschließen. Ohne eine Freischaltung ist kein Zugriff auf die Dienste möglich.

Beim Erstellen eines neuen Anbieters wählen Sie zunächst den Typ aus.

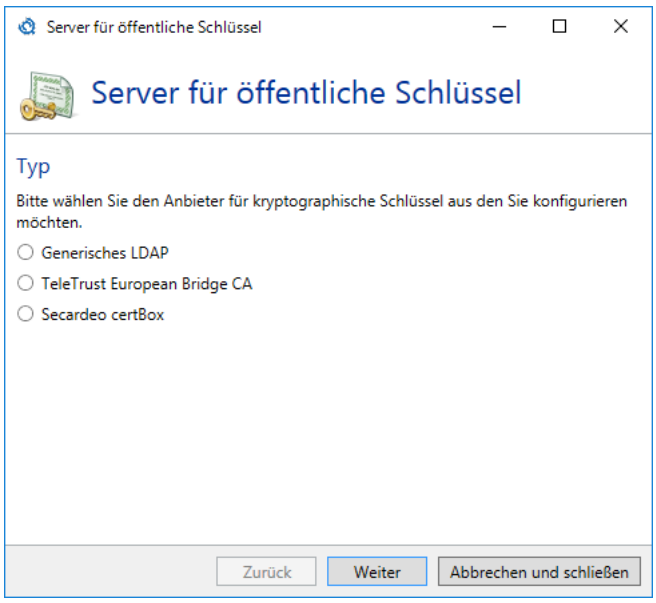


Bild 69: Anbieterauswahl

Bei der Auswahl eines generischen LDAP Anbieters konfigurieren Sie zunächst den Namen und die Serveranbindung (Bild 70). Der Name ist nur für Sie relevant und wird von der Software nicht weiter verwendet. In den Feldern Hostname und Port konfigurieren Sie die Verbindung zum LDAP-Server des Anbieters. Der Standard-Port für LDAP-Abfragen ist 389.

Verlangt der Anbieter eine Authentifizierung, so können Sie die im unteren Abschnitt angeben.

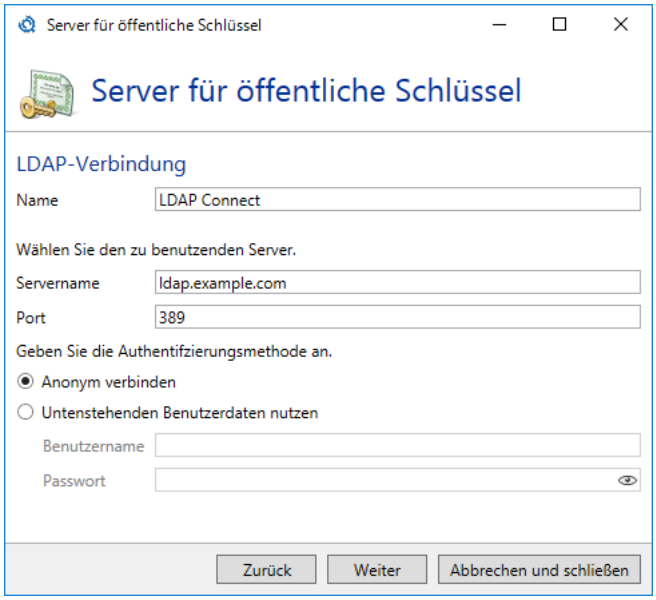


Bild 70: Verbindungsparameter für einen generischen LDAP-Anbieter

Geben Sie im nächsten Schritt die Suchparameter ein (Bild 71). Sie können die Suche entweder unbeschränkt durchführen oder auf einen bestimmten LDAP-Container beschränken. Im letzteren Fall geben Sie im Feld **Vollqualifizierter Name** den LDAP-Pfad (Distinguished Name) des Containers an.

Der **Filter** gibt den Suchfilter an, mit dessen Hilfe Zertifikate gesucht werden. Dies muss ein gültiger LDAP-Suchstring sein. Ein einfaches Beispiel ist '(|(rfc822mailbox=%e)(pGPUserID=*%e*))'. Dabei wird %e bei der Ausführung der Suche durch die gesuchte E-Mail-Adresse ersetzt. Im angegebenen Beispiel wird nach Elementen gesucht, wo entweder das Feld 'rfc822mailbox' gleich der E-Mail-Adresse ist oder das Feld 'pGPUserID' die E-Mail-Adresse enthält.

Der Suchfilter muss mindestens einmal den Platzhalter für E-Mail-Adresse (%e) enthalten.

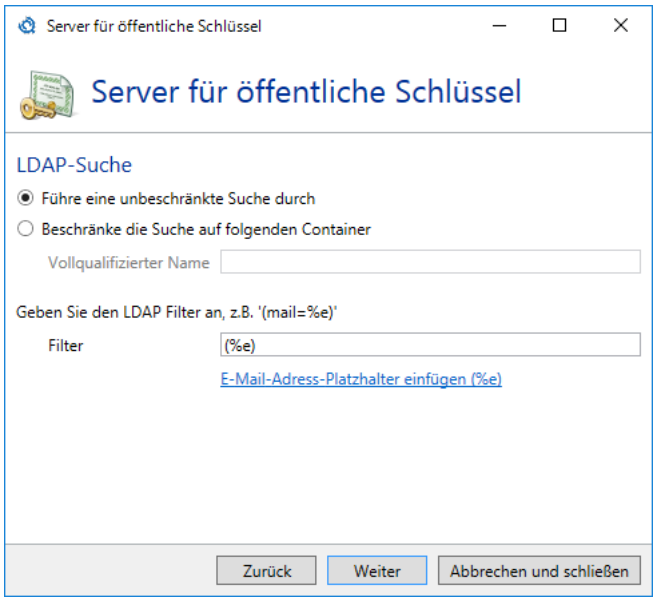


Bild 71: Suchparameter für einen generischen LDAP-Anbieter

Im folgenden Schritt wählen Sie aus, ob Sie X509 Zertifikate, PGP-Schlüssel oder beides von dem Anbieter abrufen möchten (Bild 71).

Mindestens eine Art von Schlüsseln muss ausgewählt werden; andernfalls kann der Anbieter nicht hinzugefügt werden. Für den Typ müssen Sie außerdem festlegen, aus welchen LDAP-Feld der Schlüssel geladen werden soll.

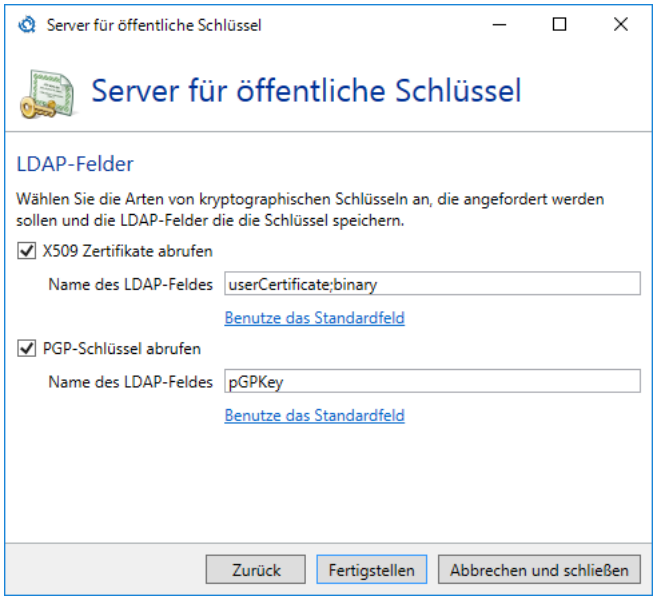


Bild 72: Verbindungsparameter für einen generischen LDAP-Anbieter

Im letzten Schritt können Sie konfigurieren, ob der Server Schlüssel für beliebige Domänen bereithält oder nur für bestimmte. Falls letzteres der Fall ist, tragen Sie die Domänen in die Liste ein.

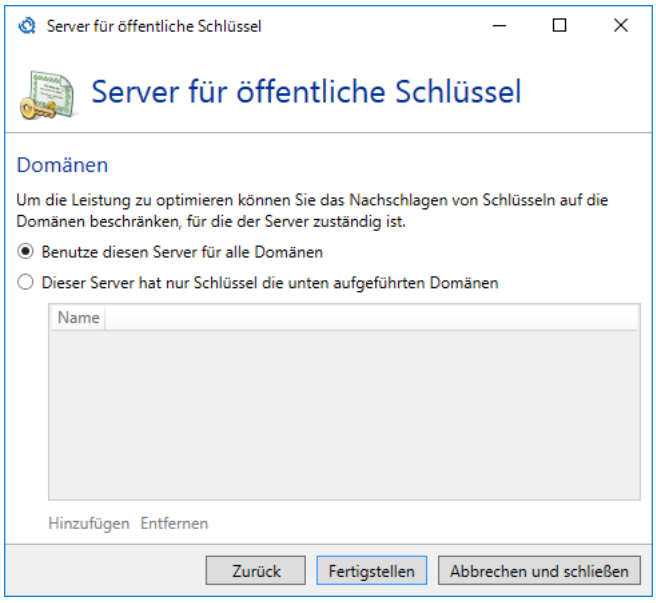


Bild 73: Einschränkung des Servers auf bestimmte Domänen.

Bei Benutzung der TeleTrusT European Bridge CA geben Sie nur den Namen an, unter dem Sie diesen Schlüsselanbieter speichern möchten. Alle weiteren Einstellungen werden automatisch von NoSpamProxy vorgenommen.

Haben Sie als Anbieter die Secardeo certBox ausgewählt, dann können Sie im Folgenden die Anbindung konfigurieren (Bild 74). Zunächst geben Sie dem Anbieter einen Namen. Dieser ist nur für Sie relevant und wird von der Software nicht weiter verwendet.

Um Secardeo certBox zu nutzen müssen Sie einen Vertrag mit dem Schlüsselanbieter abgeschlossen haben.

- Sie können den Secardeo Cloud-Dienst verwenden. In diesem Fall muss Ihre Firewall so konfiguriert werden, dass Sie ausgehende Verbindungen auf Port 389 (LDAP) zulässt.
- Sie können eine lokale certBox ansprechen. Geben hierzu die Adresse und den Port an.

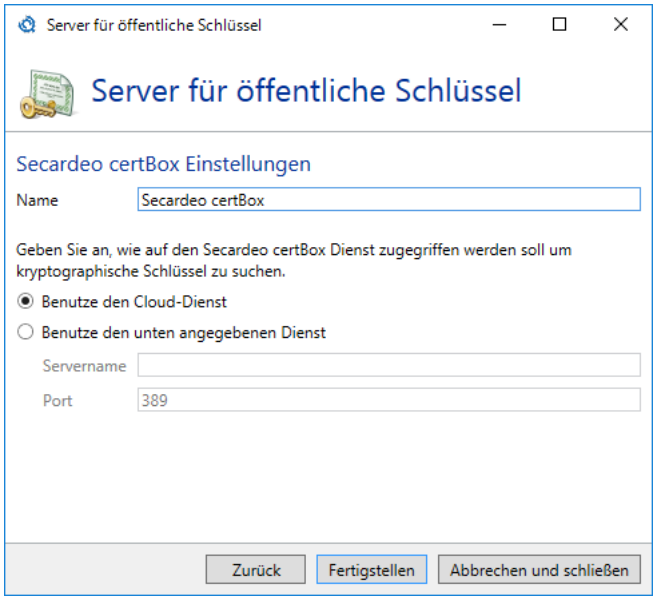


Bild 74: Anbindung an die Secardeo certBox

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 75: Den Open Keys Web Service nutzen

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

Zertifikate und PGP-Schlüssel

Die Knoten **Zertifikate** und **PGP-Schlüssel** für die Verwaltung der kryptographischen Schlüssel sind analog aufgebaut, deshalb werden Sie hier nur einmal beschrieben. Signifikante Unterschiede werden an den passenden Stellen erläutert.

NoSpamProxy Encryption benötigt für den vollständigen Einsatz der Aktionen für E-Mail-Signatur und Verschlüsselung die kryptographischen Schlüssel der Benutzer, die signierte E-Mails an externe E-Mail-Empfänger versenden wollen und dadurch verschlüsselte E-Mail-Antworten empfangen wollen. Über die Schlüsselverwaltung haben Sie Zugriff auf alle kryptographischen Schlüssel, die derzeit in NoSpamProxy Encryption gespeichert sind. Dies umfasst sowohl eigene als auch öffentliche Zertifikate, Stamm- und Zwischenzertifikate sowie PGP-Schlüssel (Bild 76).

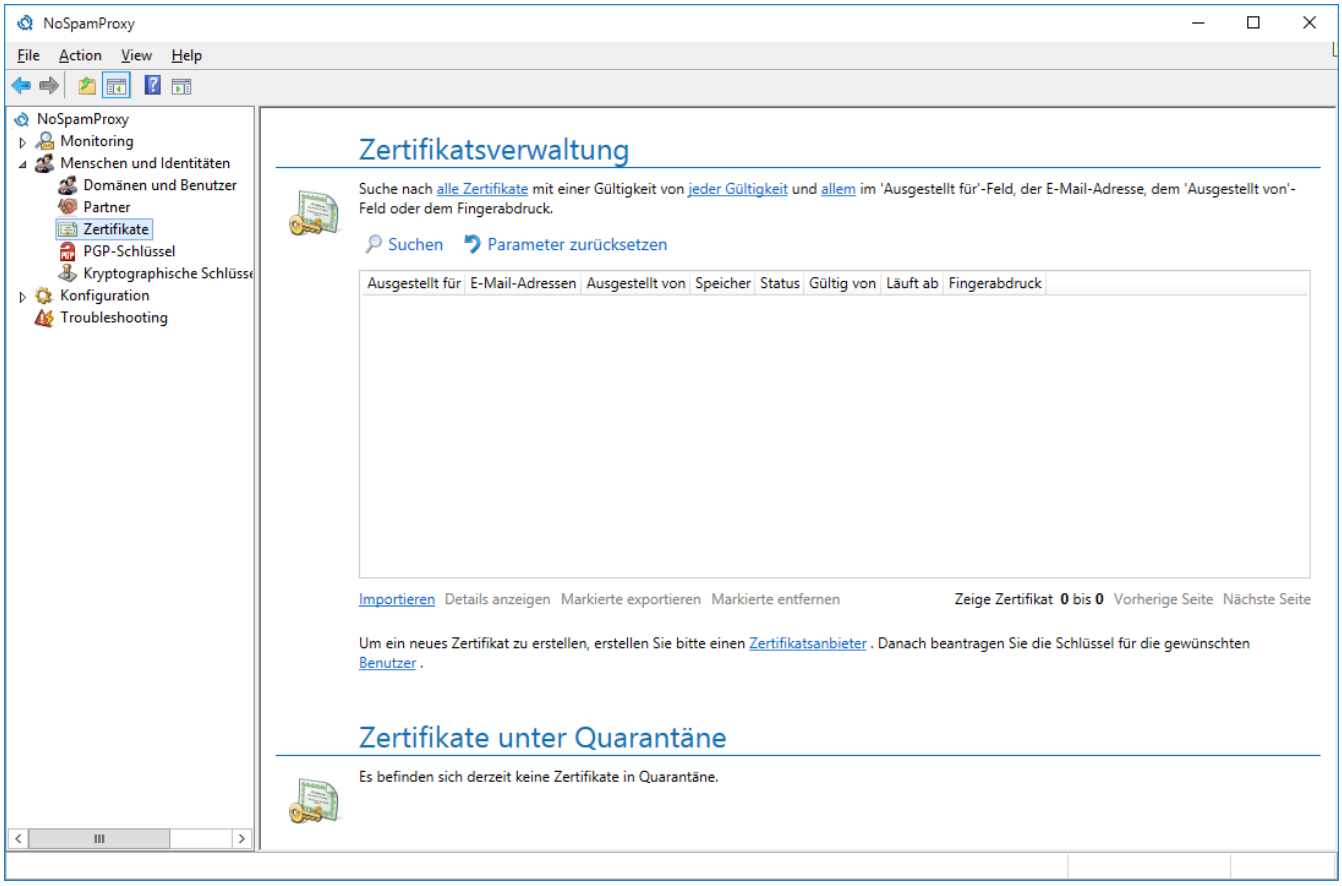


Bild 76: Zertifikatsübersicht

Neue Zertifikate können Sie über den Link Importieren hinzufügen. Zusätzlich sammelt die Gateway Rolle automatisch öffentliche Zertifikate von E-Mails an lokale Adressen ein.

Zwischen- und Stammzertifikate, sowie PGP-Schlüssel werden zwar auch von E-Mails an lokale Adressen eingesammelt. Da bei diesen Schlüsseln aber keine Vertrauenskette aufgebaut werden kann, werden sie zunächst unter Quarantäne gestellt und müssen vom Administrator genehmigt werden.

Sie können hier auch weitere Zertifikate aus Dateien im Dateiformat "CER", "DER", "P12" und "PFX" in NoSpamProxy Encryption importieren. Die gesammelten Zertifikate werden von den Aktionen für S/MIME Verschlüsselung und S/MIME Signatur verwendet bzw. durch diese Aktion gesammelt. Genauere Erklärungen stehen im Kapitel Verschlüsselung.

Schlüsselverwaltung

Import

Sie können sowohl öffentliche wie auch private oder geheime kryptographische Schlüssel manuell importieren. Wählen Sie die Funktion **Importieren**, um den Importassistenten (Bild 77) zu starten.

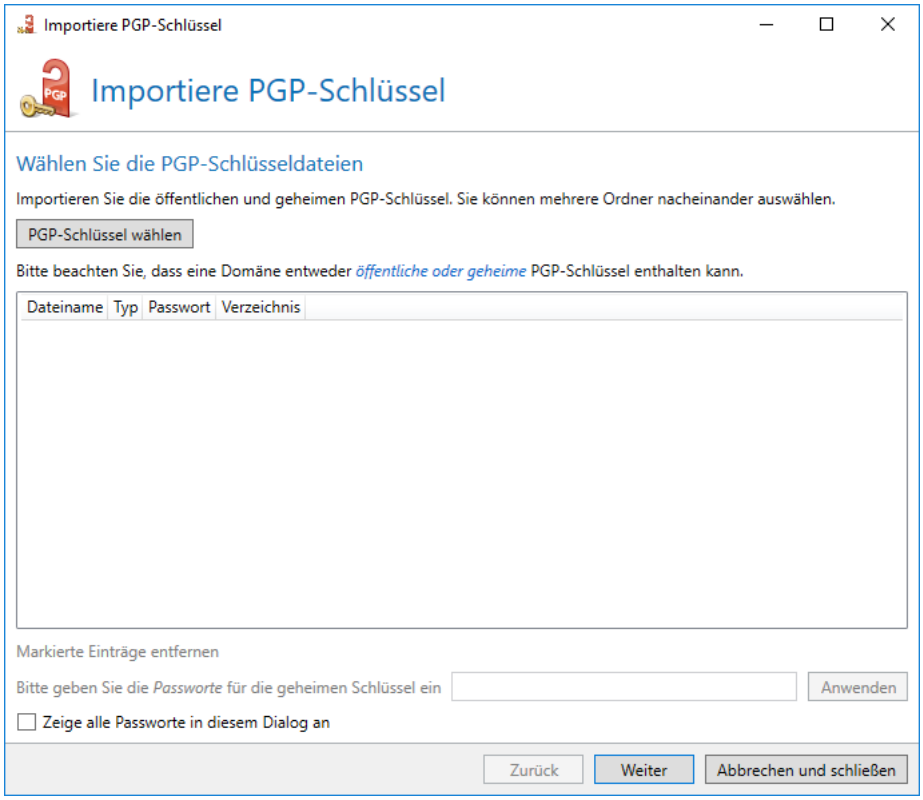


Bild 77: Import von kryptographischen Schlüsseln

Wählen Sie über die Schaltfläche **Zertifikate wählen** oder **PGP-Schlüssel wählen** Dateien aus einem Verzeichnis aus. Die Dateien fügen Sie nach der Auswahl mit **Öffnen** Ihrer Auswahl hinzu. Wenn Sie kryptographische Schlüssel aus mehreren Verzeichnissen importieren möchten, können Sie diesen Vorgang auch mehrmals wiederholen. Die weiteren ausgewählten Dateien werden ebenfalls der Liste hinzugefügt. Ungewollte Dateien können Sie aus der Liste löschen.

Für Zertifikate im PFX und P12 Dateiformat ist üblicherweise ein Passwort für den Import notwendig. PGP-Schlüsseldateien können ebenfalls durch Passworte geschützt sein; bei diesen ist durch die Dateiendung nicht klar ersichtlich, welche Dateien Passworte benötigen. Sie können Passwörter für den Import bereitstellen, indem Sie ein oder mehrere Schlüsseldateien mit gleichem Passwort markieren, danach das Passwort in das Eingabefeld eintragen und mit **Anwenden** bestätigen (Bild 78).

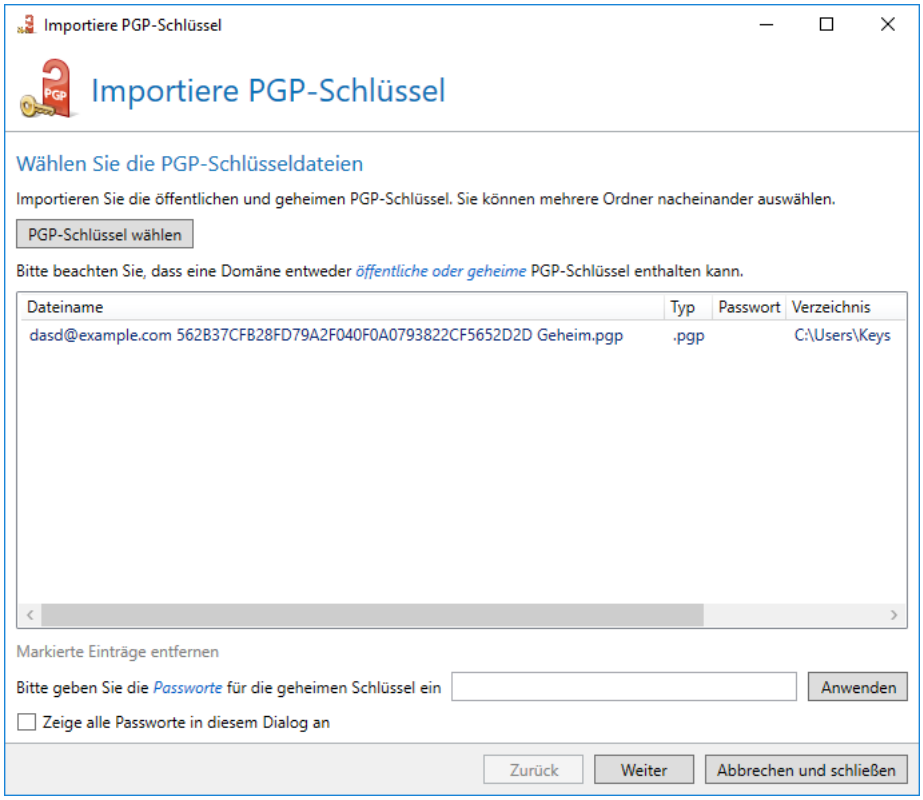


Bild 78: Zu importierende Schlüsseldateien mit Passworten

Die Passwörter können durch das Setzen des Häkchens neben **Zeige alle Passworte in diesem Dialog an** angezeigt werden. Wenn Sie die Auswahl der Dateien und das Anwenden von Passwörtern beendet haben, können Sie über die Schaltfläche **Weiter** das Laden der Schlüsseldateien starten.

Nach dem Validieren werden alle erfolgreich validierten Schlüsseldateien in der oberen Liste, alle nicht erfolgreich validierten Schlüssel in der unteren Liste angezeigt (Bild 79).

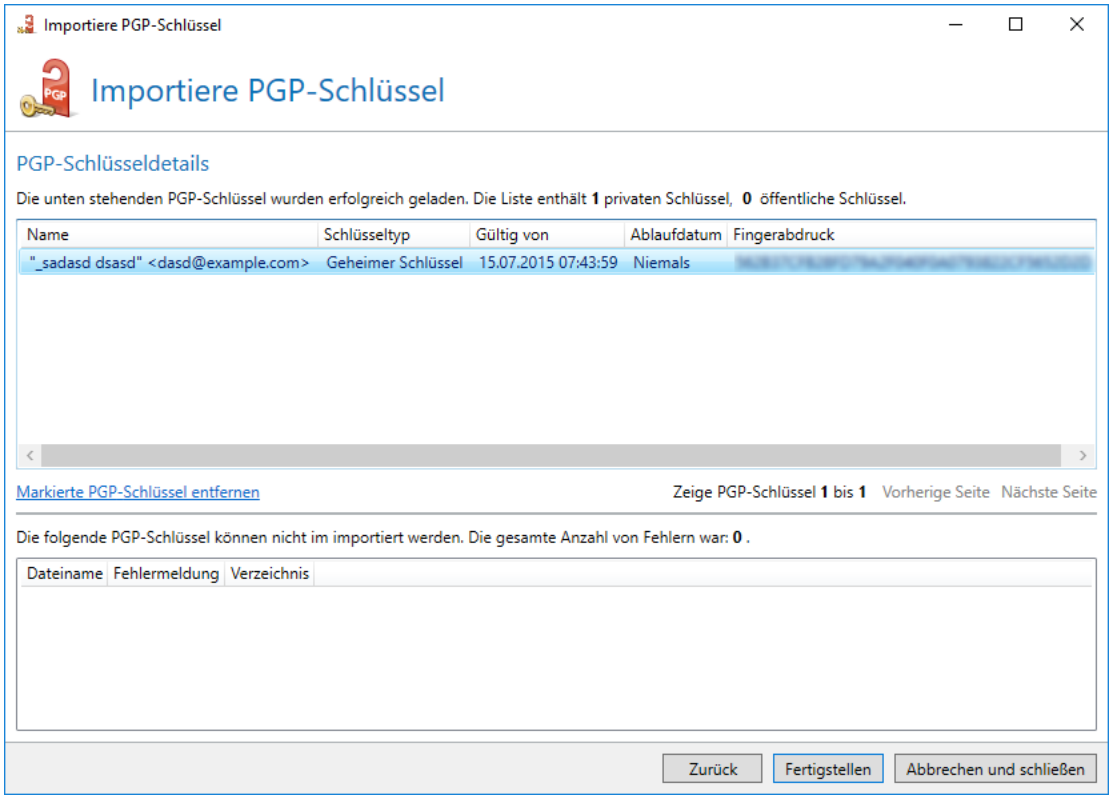


Bild 79: Auswertung der zu importierenden kryptographischen Schlüssel

Sie können mit **Zurück** die Liste für den Import anpassen oder Passwörter korrigieren und danach mit **Weiter** den Validierungsvorgang erneut durchführen. Die erfolgreich ausgewerteten kryptographischen Schlüssel werden durch die Schaltfläche **Fertigstellen** in den Server importiert.

Wenn private kryptographische Schlüssel für eine Domäne importiert werden, die bereits öffentliche Schlüssel enthält, werden die öffentlichen Schlüssel gelöscht. Sollten zeitgleich private und öffentliche Schlüssel derselben Domäne importiert werden, speichert der Server nur die privaten Schlüssel.

Beim Import eines kryptographischen Schlüssels mit mehreren E-Mail-Adressen ist es möglich, dass die Domänen der unterschiedlichen E-Mail-Adressen dieses Schlüssels sich sowohl in der Liste der eigenen Domänen befinden, als auch in den Partnern. Beim Import eines solchen Schlüssels ist seine Art von Bedeutung: Beim Import eines privaten Schlüssels werden die E-Mail-Adressen beachtet, deren Domänen sich in der Liste der eigenen Domänen befinden, die anderen E-Mail-Adressen werden ignoriert. Beim Import eines öffentlichen Schlüssels werden für alle E-Mail-Adressen, deren Domäne nicht zu den lokalen Domänen gehört, neue Partner erstellt oder ein bestehender ergänzt. Die übrigen E-Mail-Adressen werden ignoriert.

Wenn Sie Stammzertifikate oder Zwischenzertifikate als eigene Dateien oder auch eingebettet in Endzertifikate importieren, werden diese automatisch im Zertifikatsspeicher des Servers hinterlegt. Stammzertifikate befinden sich dann in der Liste der **Vertrauenswürdigen Stammzertifizierungsstellen** und Zwischenzertifikate in der Liste der **Zwischenzertifizierungsstellen** des lokalen Computers.

Export

Auch der Export von kryptographischen Schlüsseln läuft bei Zertifikaten und PGP-Schlüsseln fast identisch ab. Die Unterschiede werden auch hier wieder an den entsprechenden Stellen erläutert.

Wählen Sie die in der Übersicht die Export-Funktion um die ausgewählten kryptographischen Schlüssel zu exportieren.

Wählen Sie zuerst aus, ob alle ausgewählten Schlüssel in dieselbe oder in unterschiedliche Dateien exportiert werden sollen. Sie können auch entscheiden, ob Sie nur die öffentlichen Schlüssel oder auch gegebenenfalls vorhandene private bzw. geheime Schlüssel exportieren möchten (Bild 80).

Bild 80: Exportoptionen (hier für Zertifikate)

Sie sehen auf der Seite für die **Exporteinstellungen**, in Abhängigkeit zum letzten Schritt, unterschiedliche Elemente. (Bild 81)

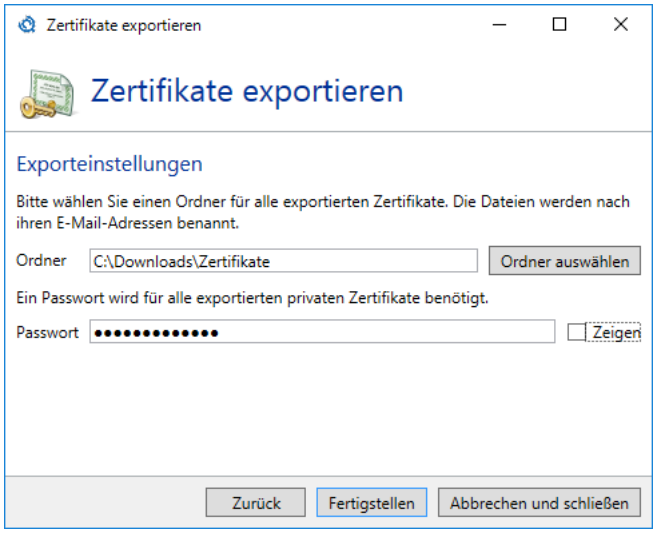


Bild 81: Exporteinstellungen (hier für Zertifikate)

Zertifikate auf Open Keys veröffentlichen

Sie haben die Möglichkeit, öffentliche Schlüssel über den Open Keys Web Service anderen Personen und Organisationen zur Verfügung zu stellen. Der hier bereitgestellte öffentliche Schlüssel wird zur Verschlüsselung, ihr privater Schlüssel für die Entschlüsselung von E-Mails an Sie genutzt.

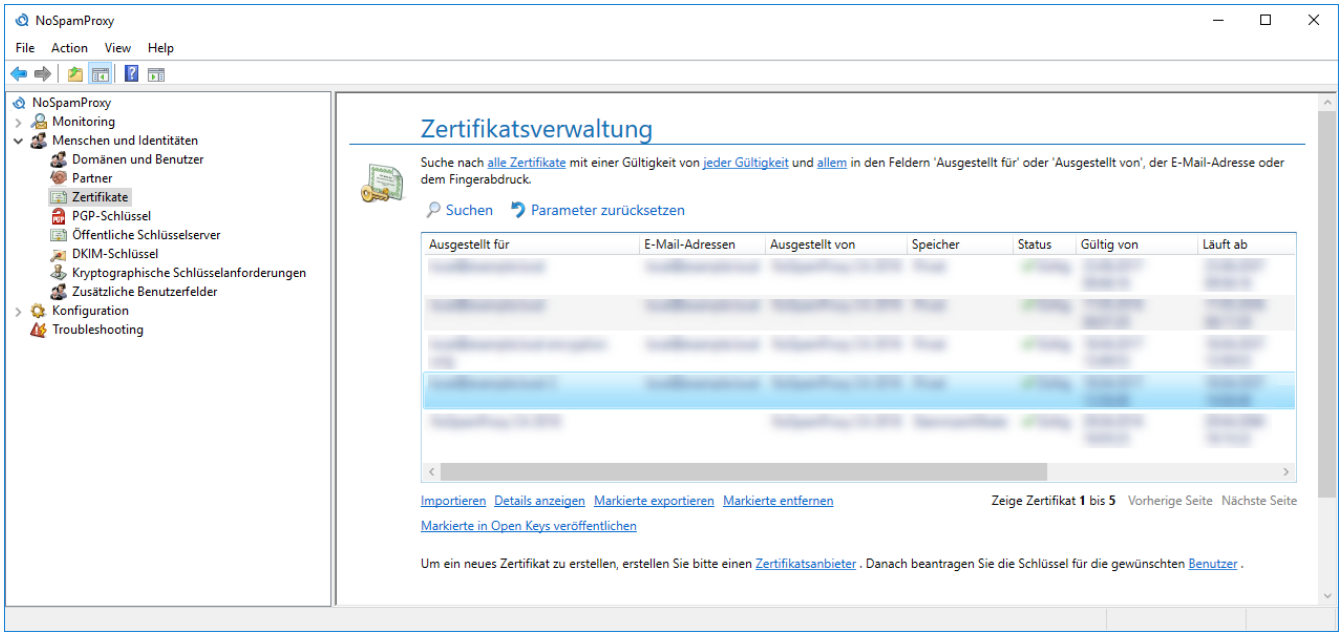


Bild 82: Zertifikate in Open Keys veröffentlichen

Um ein Zertifikat zu veröffentlichen, gehen Sie zu **Zertifikate/Zertifikatsverwaltung** und markieren Sie ein oder mehrere Zertifikate. Klicken Sie dann **Markierte in Open Keys veröffentlichen**.

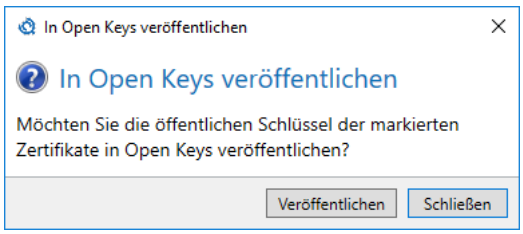


Bild 83: Die ausgewählten Zertifikate werden automatisch nach Open Keys hochgeladen

Klicken Sie im dann folgenden Dialog auf **Veröffentlichen**.

Quarantäne für kryptographische Schlüssel

PGP-Schlüssel sowie Zwischen- und Stammzertifikate, die von E-Mails an lokale Adressen eingesammelt werden, werden unter Quarantäne gestellt und müssen vom Administrator genehmigt werden, bevor sie von NoSpamProxy verwendet werden können. Sofern Schlüssel auf Genehmigung warten, können Sie sie über den Link **Genehmigungen verwalten** entweder genehmigen oder entfernen (Bild 84).

Werden Zwischen- und Stammzertifikate genehmigt, dann werden sie in den Zertifikatsspeicher des Servers installiert.

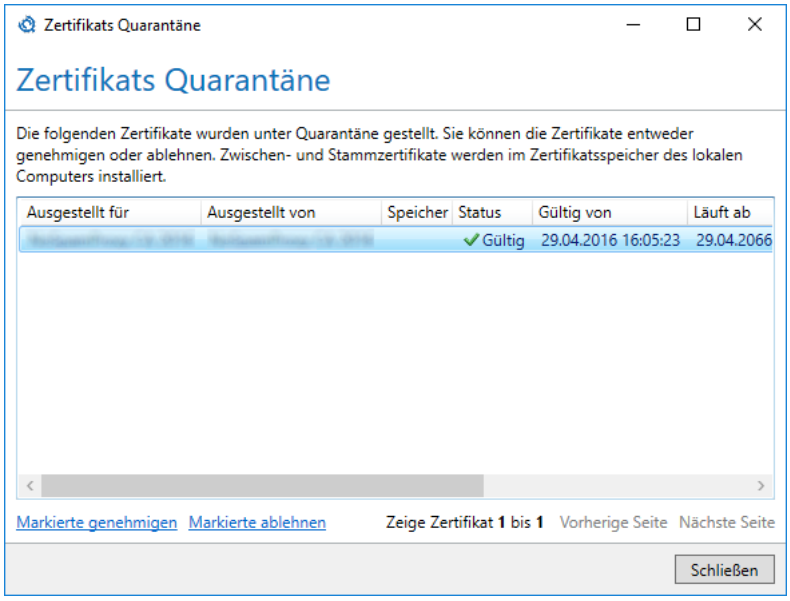


Bild 84: Zertifikate, die unter Quarantäne gestellt wurden

Im Dialog **Zertifikats Quarantäne** bzw. **PGP-Schlüssel Quarantäne** sehen Sie die kryptographischen Schlüssel, die derzeit unter Quarantäne gestellt sind. Über den Link **Markierte genehmigen** bestätigen Sie die markierten Schlüssel und aktivieren sie damit für die weitere Nutzung im Gateway. Wenn Sie den Schlüsseln nicht vertrauen wollen, markieren Sie sie und klicken auf den Link **Markierte ablehnen**. Diese Schlüssel werden dann gelöscht.

Kryptographische Schlüsselanforderung

Unter dem Knoten **Kryptographische Schlüsselanforderung** können Sie Anbieter konfigurieren, die Zertifikate oder PGP-Schlüssel für die Unternehmensbenutzer von NoSpamProxy Encryption bereitstellen und alle gestellten Zertifikatsanforderungsanfragen einsehen und verwalten. (Bild 85)

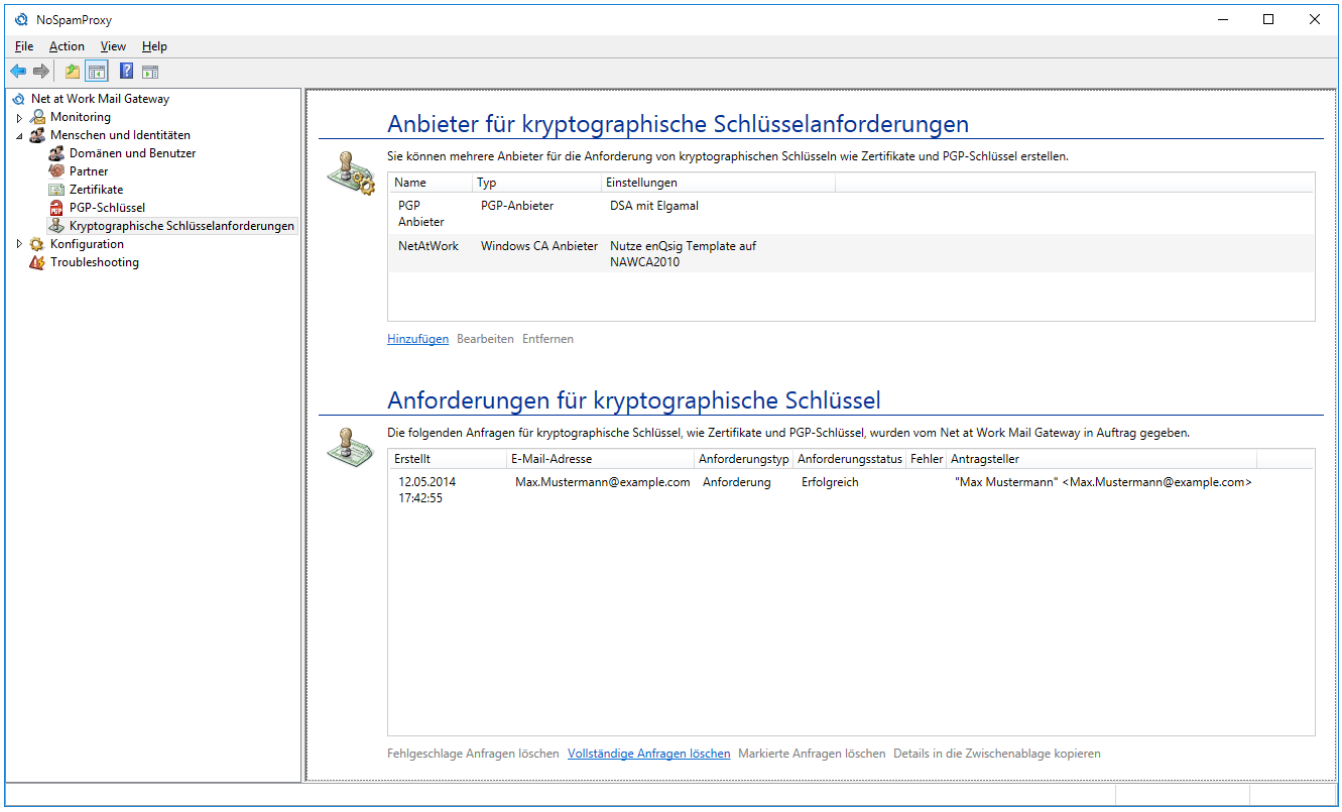


Bild 85: Verwalten Sie Ihre Schlüsselanforderungen

Anbieter für kryptographische Schlüsselanforderungen

Sie können hier unterschiedliche Schlüsselanbieter konfigurieren und abspeichern. Diese abgespeicherten Profile stehen bei zukünftigen Schlüsselanforderungen für Unternehmensbenutzer zur Verfügung, ohne die im Profil gespeicherten Einstellungen mehrmals durchführen zu müssen.

Der Anbieter Active-Directory-Zertifikatdienste erfordert eine in Ihr Active Directory integrierte Enterprise-Zertifizierungsstelle (CA). Der D-Trust-, SwissSign- und GlobalSign-Anbieter erfordert einen Vertrag mit der jeweiligen Firma. Die PGP-Schlüssel können vom NoSpamProxy Encryption selbst erstellt werden.

Der Anbieter Active-Directory-Zertifikatdienste erfordert eine in Ihr Active Directory integrierte Enterprise-Zertifizierungsstelle (CA). Der SwissSign-Anbieter erfordert einen Vertrag mit SwissSign. Die PGP-Schlüssel können vom NoSpamProxy Encryption selbst erstellt werden.

Neuen Anbieter hinzufügen

Wählen Sie auf der ersten Seite des Dialogs den Typ des Schlüsselanbieters. Die verfügbaren Typen werden in den folgenden Kapiteln beschrieben (Bild 86).

Bild 86: Auswahl des Providertyps

SwissSign

Für die automatische Anfrage von Benutzerzertifikaten steht Ihnen SwissSign als Anbieter zur Verfügung (Bild 87).

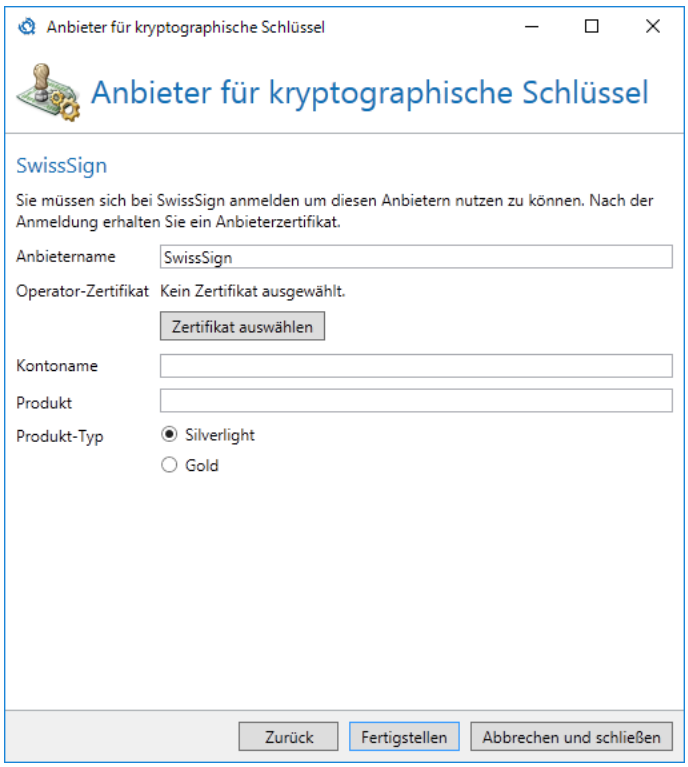


Bild 87: Einstellungen für den SwissSign Anbieter

Um SwissSign zu benutzen, müssen Sie mit der Firma SwissSign einen gültigen Vertrag abgeschlossen und das Zertifikat von SwissSign in der Zertifikatsverwaltung importiert haben.

Neben dem Zertifikat haben Sie von SwissSign auch noch einen Kontonamen bekommen. Tragen Sie diesen hier ebenfalls ein. Abschließend wählen Sie noch aus, welche Zertifikatstypen Sie anfordern möchten. Dabei können Sie zwischen 'Silver Light'- und 'Gold'-Zertifikaten mit einer Laufzeit von 1, 3 oder 5 Jahren wählen. Nähere Informationen finden Sie bei SwissSign.

Für Informationen zum Open Keys Web Service lesen Sie bitte den Abschnitt Schlüssel über den Open Keys Web Service bereitstellen.

D-Trust

Für die automatische Anfrage von Benutzerzertifikaten steht Ihnen D-Trust als Anbieter zur Verfügung (Bild 88).

Bild 88: Einstellungen für den D-Trust-Anbieter

Um D-Trust zu benutzen, müssen Sie mit der Deutschen Bundesdruckerei einen gültigen Vertrag abgeschlossen und das Zertifikat von D-Trust in der Zertifikatsverwaltung importiert haben.

Neben dem Zertifikat wurde Ihnen von D-Trust zusätzlich eine **Zertifikatsvorlage** ausgehändigt. Tragen Sie diese hier ebenfalls ein. Die Abwicklung von Anfragen wird bei diesem Anbieter über E-Mails durchgeführt. Daher müssen Sie im Feld **Operator Email-Adresse** eine interne E-Mail-Adresse auswählen. Diese wird als Absende-Adresse für alle Anfragen verwendet und muss erreichbar sein.

Für Informationen zum Open Keys Web Service lesen Sie bitte den Abschnitt Schlüssel über den Open Keys Web Service bereitstellen.

GlobalSign

Für die automatische Anfrage von Benutzerzertifikaten steht Ihnen darüber hinaus noch GlobalSign als Anbieter zur Verfügung (Bild 89).

Bild 89: Einstellungen für den GlobalSign Anbieter

Um GlobalSign zu benutzen, müssen Sie mit der Firma GlobalSign einen gültigen Vertrag abgeschlossen haben.

Nach der Anmeldung bei GlobalSign erhalten Sie die Zugangsdaten für das GlobalSign Management-Portal. Diese tragen Sie bitte im GlobalSign Konfigurations-Dialog ein. In dem Portal können Sie auch Profile konfigurieren und Zertifikats-Pakete kaufen. Diese Daten tragen Sie hier ebenfalls ein.

Sie müssen im Profil einen IP-Adressbereich für die API freischalten. Nur dann können über die Oberfläche Zertifikate angefordert werden.

Für Informationen zum Open Keys Web Service lesen Sie bitte den Abschnitt Schlüssel über den Open Keys Web Service bereitstellen.

Active-Directory-Zertifikatdienste

Über diesen Anbieter können Sie Benutzerzertifikate von einer Zertifizierungsstelle (CA) anfordern, die sich in Ihrem Active Directory befindet.

Um diesen Anbieter zu nutzen müssen die folgenden Voraussetzungen erfüllt sein:

- Das Betriebssystem des Rechners der Intranet Rolle ist Windows 2008 R2 oder neuer.
- Ihre Intranet Rolle ist in einem Active Directory installiert.
- In Ihrem Active Directory ist eine Enterprise CA installiert.
- Auf der Enterprise CA sind passende Zertifikatsvorlagen freigegeben.

Nutzbare Zertifikatsvorlagen benötigen die folgenden Eigenschaften:

- Die Schlüsselausstellung erfolgt ohne Benutzerinteraktion.
- Die S/MIME-Zertifikatserweiterungen werden unterstützt.
- Der Name des Antragstellers wird an die Vorlage übergeben.
- Der Export des privaten Schlüssels ist erlaubt.
- Das Zertifikat ist für den Schutz von E-Mail-Nachrichten nutzbar.

Nach der Auswahl des Anbieters für eine **Active-Directory-Zertifikatdienste** können Sie die notwendigen Einstellungen vornehmen (Bild 90).

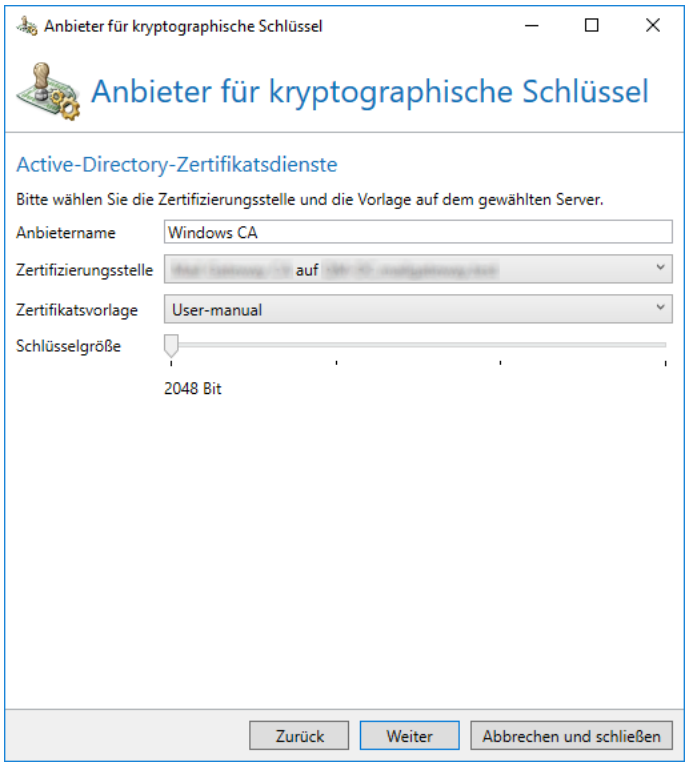


Bild 90: Konfigurieren Sie den Anbieter Active-Directory-Zertifikatdienste

Tragen Sie für die Konfiguration einen eindeutigen Anbieternamen ein und wählen Sie dann eine Ihrer Zertifizierungsstellen aus. Nach der Auswahl werden alle freigegebenen Zertifikatsvorlagen dieser Stelle angezeigt.

Wählen Sie jetzt eine Vorlage aus. Die Vorlage muss die in der obigen Liste aufgeführten Eigenschaften erfüllen, um benutzt werden zu können. Sollten Eigenschaften fehlen, werden Hinweise unter der Auswahlliste angezeigt.

Nach der Auswahl der Zertifikatsvorlage wird der Schieberegler für die Schlüsselgröße auf die erlaubten Werte der Zertifikatsvorlage eingestellt. Zum Schluss tragen Sie bitte die Länderkennung in Form eines ISO 3166-1 Alpha-2 Kürzels an. Unter dem Eingabefeld können Sie über die Auswahl der Ländernamen das dazugehörige Alpha-2-Kürzel in das Eingabefeld eintragen lassen.

Für Informationen zum Open Keys Web Service lesen Sie bitte den Abschnitt Schlüssel über den Open Keys Web Service bereitstellen.

PGP-Schlüsselanbieter

Sie können PGP-Schlüssel mit unterschiedlichen Verschlüsselungsalgorithmen und Schlüssellängen erstellen (Bild 91).

Bild 91: Einstellungen des PGP-Anbieters

Geben Sie als **Anbietername** einen eindeutigen Namen ein. Wählen Sie danach den **PGP-Schlüsseltyp**. Hier steht Ihnen RSA und DSA mit ElGamal zur Verfügung. Die für Sie passende

Konfiguration ist abhängig von den Kommunikationspartnern mit denen Sie später signierte und verschlüsselte E-Mails austauschen wollen. Erfragen Sie bitte bei diesen, welche Schlüsselalgorithmen und Schlüssellängen von Ihrer Infrastruktur unterstützt wird.

Auf der zweiten Seite können Sie die Gültigkeit für den Schlüssel einschränken. Dies ist sinnvoll, da aufgrund von steigender Rechenkapazität Schlüssel mit höherer Schlüssellänge notwendig werden können. Abschließend können Sie die neuen Schlüssel mit einem bestehenden Schlüssel signieren. Dies kann in bestimmten Situationen den Schlüsselaustausch vereinfachen, da dann nur noch der Übergeordnete Schlüssel (z.B. Firmenschlüssel) ausgetauscht werden muss. Alle mit diesem Schlüssel signierten PGP-Schlüssel gelten dann automatisch als vertrauenswürdig (Bild 92)

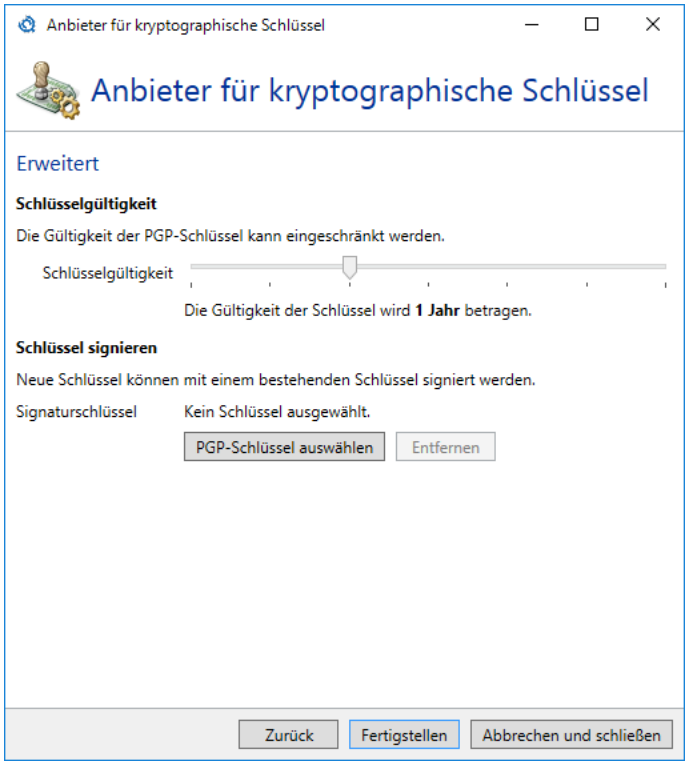


Bild 92: Weitere Einstellungen des PGP-Anbieters

Standardeinstellungen

Für die Anbieter 'D-Trust', 'SwissSign' und die Active-Directory-Zertifikatdienste können unterschiedliche Werte fest vorgegeben werden. Wenn dies geschieht, werden nicht mehr die Werte aus dem Unternehmensbenutzer für den Zertifikatsantrag verwendet, sondern die hier hinterlegten Werte (Bild 93).

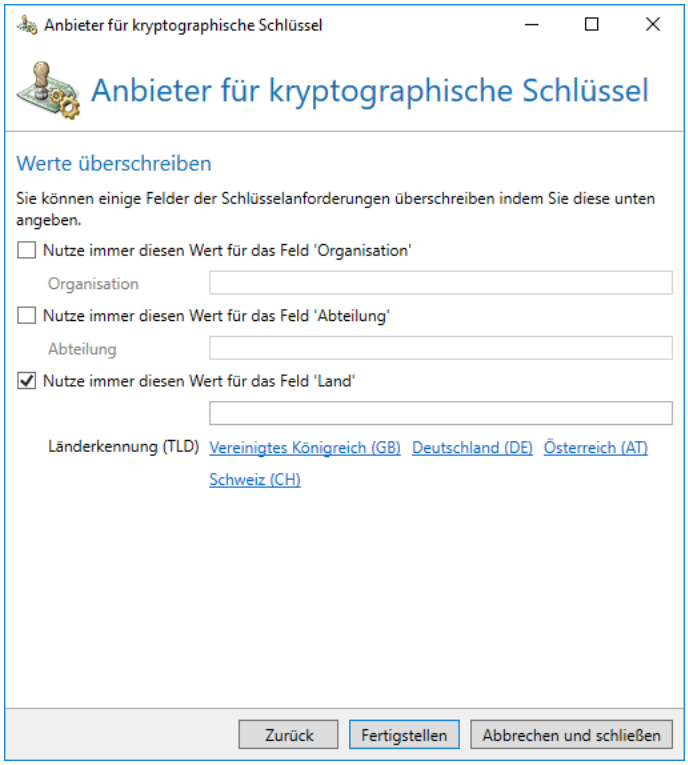


Bild 93: Standardwerte für den Anbieter am Beispiel der Active-Directory-Zertifikatdienste

Die folgenden Werte können von den unterschiedlichen Anbietern überschrieben werden:

- **D-Trust**
  Organisation, Abteilung
- **Active-Directory-Zertifikatdienste**
  Länderkennung, Organisation, Abteilung
- **SwissSign (Gold)**
  Länderkennung, Organisation
- **SwissSign (Silver Light)**
  keine
- **GlobalSign**
  keine
- **PGP-Schlüssel**
  keine

Nach dem Abspeichern eines Anbieters für kryptographische Schlüssel steht Ihnen dieser unter den Unternehmensbenutzern beim Aufrufen der Funktion Kryptographische Schlüssel für die markierten Benutzer beantragen zur Verfügung.

Schlüssel über den Open Keys Web Service bereitstellen

Sie können Ihre öffentlichen Schlüssel der Anbieter SwissSign, D-Trust und GlobalSign sowie Schlüssel der Active-Directory-Zertifikatsdienste über den Open Keys Web Service anderen Personen und Organisationen zur Verfügung stellen. Setzen Sie dazu auf der letzten Seite des Wizards den Haken bei **Den öffentlichen Schlüssel zu Open Keys hinzufügen (empfohlen)**. 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.

Bild 94: Den Open Keys Web Service nutzen

DKIM-Schlüssel

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 in diesem Abschnitt erstellten DKIM-Schlüssel können Sie auf dem Knoten **Domänen und Benutzer** ihren eigenen Domänen zuordnen. Die Zuordnung erfolgt beim Bearbeiten der eigenen Domäne auf der Seite DomainKeys Identified Mail.

Beim **Hinzufügen** eines neuen DKIM-Schlüssels wird das benötigte asymmetrische Schlüsselpaar von NoSpamProxy für Sie erzeugt. Der geheime private Teil des asymmetrischen Schlüssels wird dabei sicher in den NoSpamProxy-Einstellungen gespeichert und ist dadurch nur Ihnen bekannt.

Alternativ können Sie, z.B. mit OpenSSL, einen eigenen RSA-Schlüssel erzeugen und ihn über die entsprechende Schaltfläche importieren. Der Schlüssel muss dabei im PKCS#1-Format vorliegen.

Damit NoSpamProxy den benötigten DNS-Eintrag für Sie vorbereiten kann müssen Sie die eigene Domäne auswählen unter der der Schlüssel veröffentlicht wird und den Selektor (Bild 95). Der Selektor ist dabei ein eindeutiger Name für diesen Schlüssel im DNS der aus US-ASCII-Zeichen bestehen muss. Mögliche Selektoren sind zum Beispiel: 's2016', 'main16', 'key2016'. Sie können jeden Namen nehmen, es ist aber praktisch eine fortlaufende Nummer zu verwenden um ausgetauschte Schlüssel leichter zu unterscheiden.

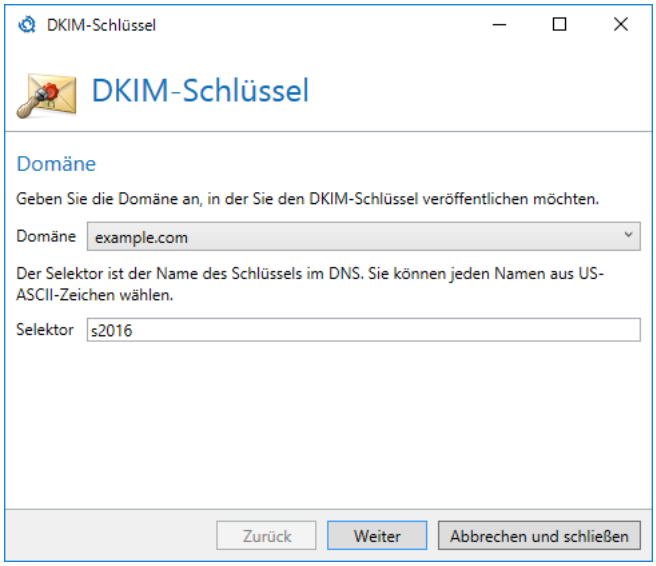


Bild 95: Der DNS-Eintrag mit dem öffentlichen Schlüssel für die gewählte Domäne

Nach der Auswahl der Domäne und des Selektors wird der DNS-Eintrag für Sie vorbereitet (Bild 96). Bitte kopieren Sie ihn in die Zwischenablage und veröffentlichen ihn im DNS. Wählen Sie dazu die DNS-Zone, die im Dialog angegeben wird.

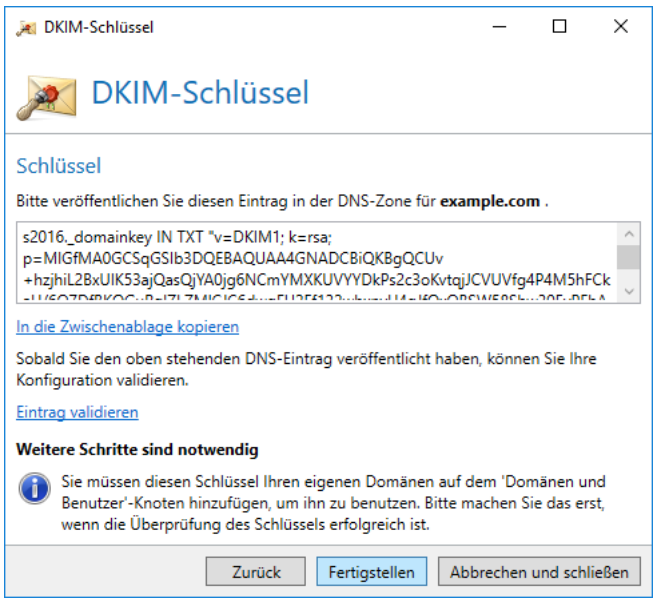


Bild 96: Der DNS-Eintrag mit dem öffentlichen Schlüssel für die gewählte Domäne

Wenn der DNS-Eintrag veröffentlicht und im Internet bekannt ist, können Sie ihn erneut öffnen und die Einstellungen überprüfen. Falls diese Validierung fehlschlägt, werden Ihnen die Unstimmigkeiten angezeigt.

Nach erfolgreicher Überprüfung müssen Sie den DKIM-Schlüssel einer Ihrer eigenen Domänen zuordnen, um ihn zu benutzen.

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.

Sie sollten den DKIM-Schlüssel exportieren, damit Sie ihn im Falle eines Datenverlustes wiederherstellen können. Über die Schaltfläche **Schlüssel exportieren** können Sie dies tun. Der Schlüssel wird im PKCS#1-Format abgespeichert.

Anforderungen für kryptographische Schlüssel

Alle Zertifikatsanforderungsanfragen werden im Bereich **Zertifikatsanforderungsanfragen** aufgelistet. Sie können selektiv fehlgeschlagene Anfragen, vollständige Anfragen oder die markierten Anfragen löschen

Wenn Sie Zertifikatsanforderungen löschen, die entweder ausstehen oder sich in einer Warteschlange befinden, werden die angeforderten Zertifikate ungültig und dadurch zerstört. Das Löschen kann nicht rückgängig gemacht werden.

Mit der Funktion **Details in die Zwischenablage kopieren** können Sie den Text aller markierten Einträge in die Zwischenablage kopieren. Diese Funktion ist bei Problemen mit der Zertifikatsanforderung hilfreich, da Sie dadurch sofort alle Statusmeldungen der betroffenen Anfragen für Supportfälle an Dritte weitergeben können.

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.

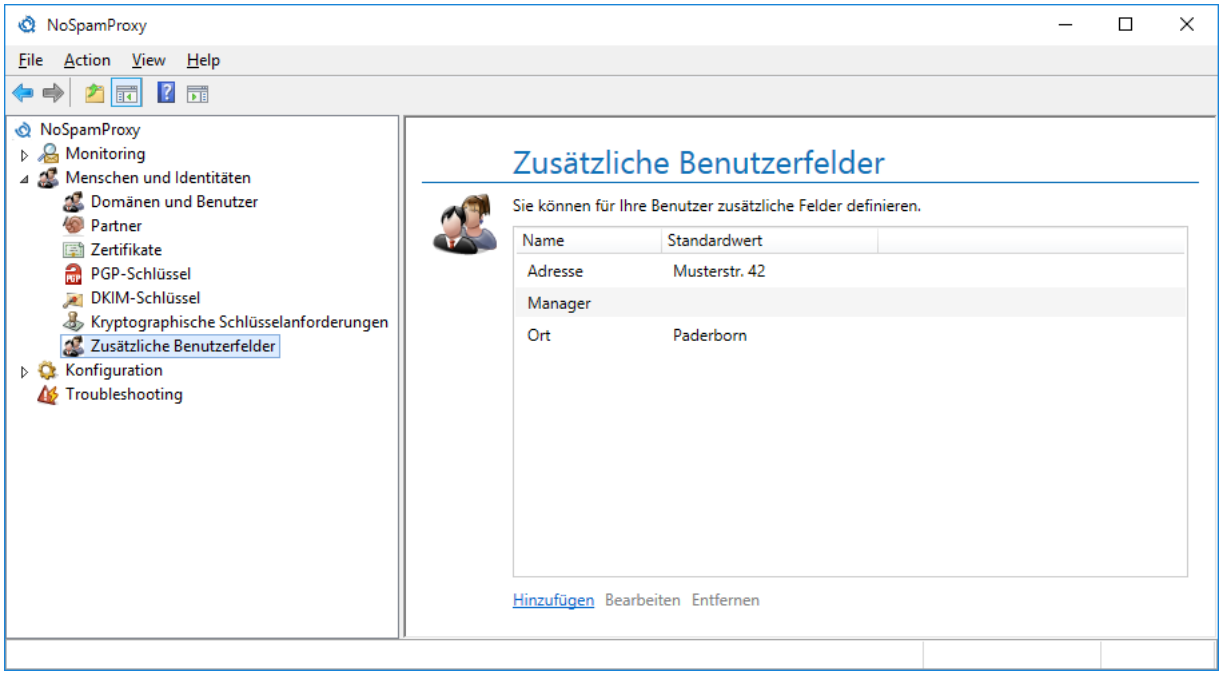


Bild 97: Liste aller benutzerdefinierten Felder

9. Konfiguration

Unter dem Knoten **Konfiguration** der Intranet Rolle befinden sich Einstellungen für die Verbindung zur Gateway Rolle, Verbindung und Einstellungen des Web Portals, Einstellungen der Datenbank, Benachrichtigungsadressen sowie der Schutz sensibler Daten (Bild 98).

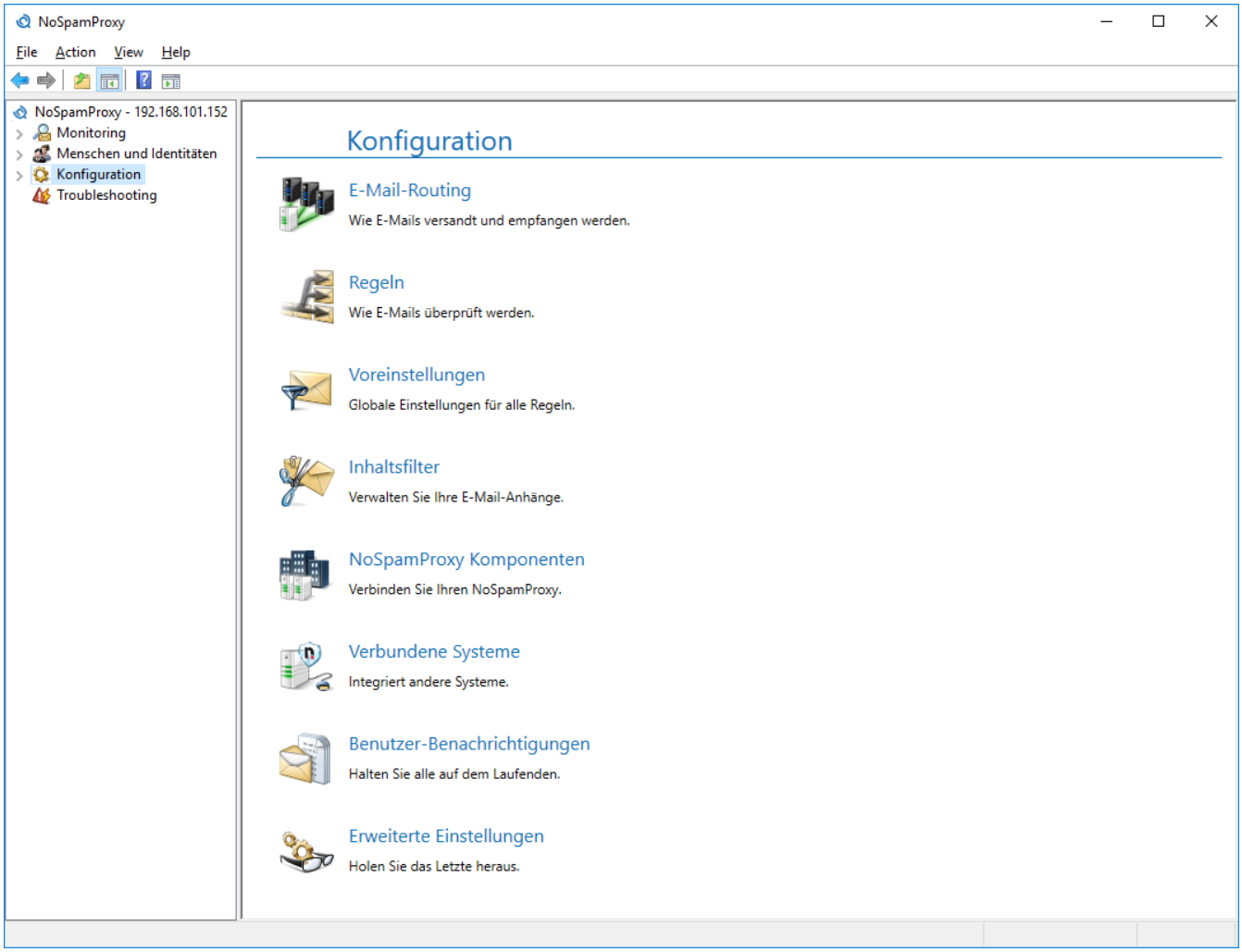


Bild 98: Einstellungen der Intranet Rolle

E-Mail-Routing

Unter dem Knoten **E-Mail-Routing** (Bild 125) 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 100).
- **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 100).
- **DNS-Domänenname**
  Ein Server gilt als lokal, sofern der hier konfigurierte DNS-Hostname auf die Adresse des Servers verweist (Bild 100).
- **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 101).
- **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 102).

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 99). 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 104). Abschließend können Sie noch einen Kommentar verfassen (Bild 105).

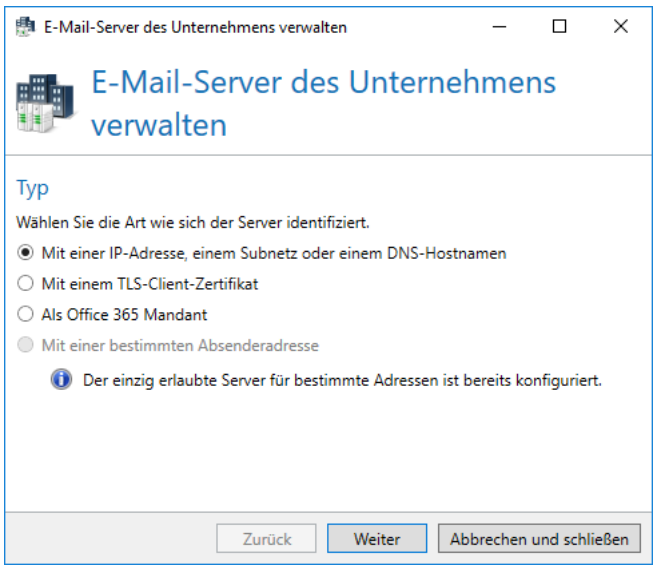


Bild 99: Die Auswahl des Server-Typs

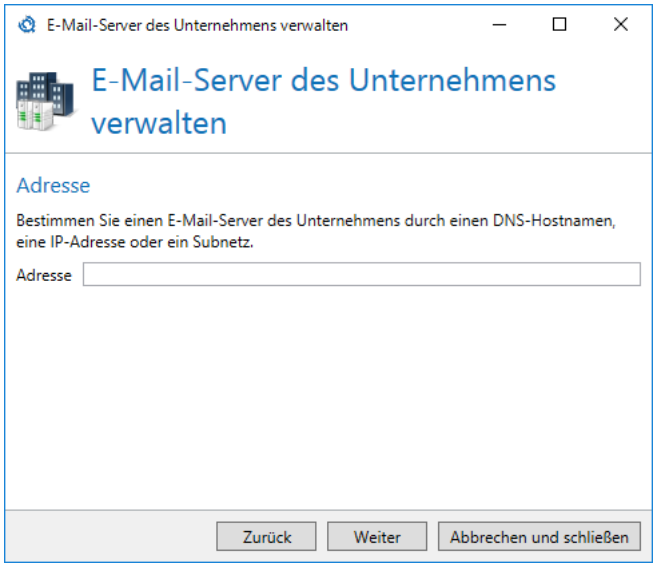


Bild 100: Authentifizierung über IP-Adresse, Subnetz-Zugehörigkeit oder DNS-Hostname

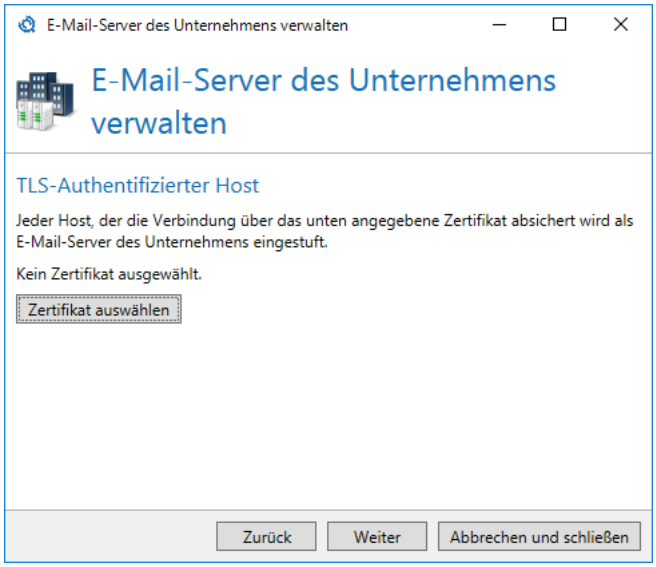


Bild 101: Authentifizierung über TLS-Zertifikat

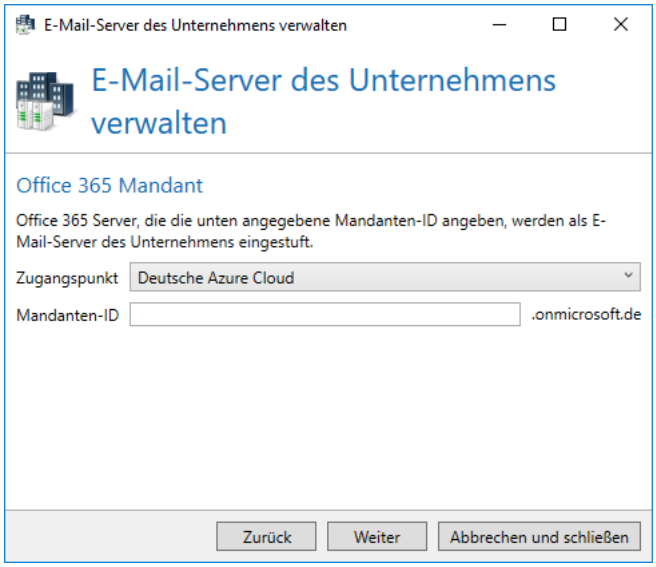


Bild 102: Authentifizierung über Office-365-Mandanten-ID

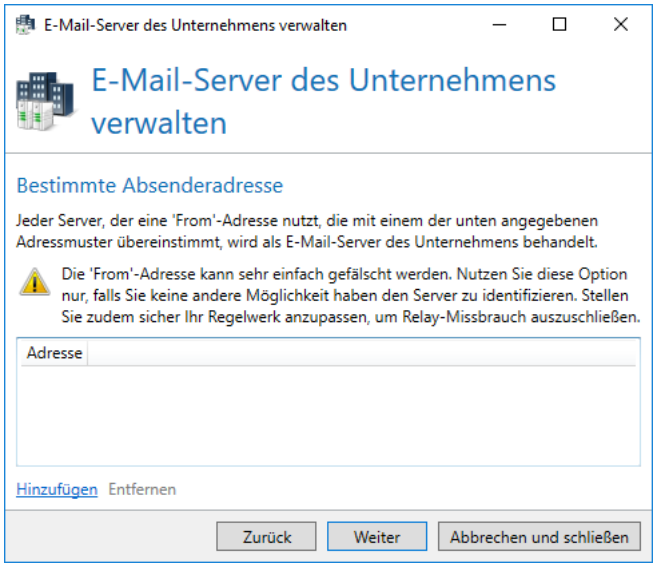


Bild 103: Authentifizierung über eine bestimmte E-Mail-Adresse

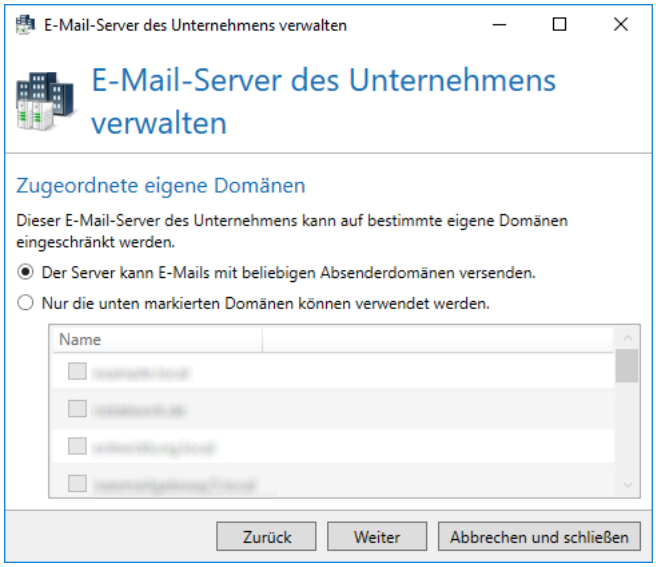


Bild 104: Geben Sie an, mit welchen eigenen Domänen der Server E-Mails versenden darf

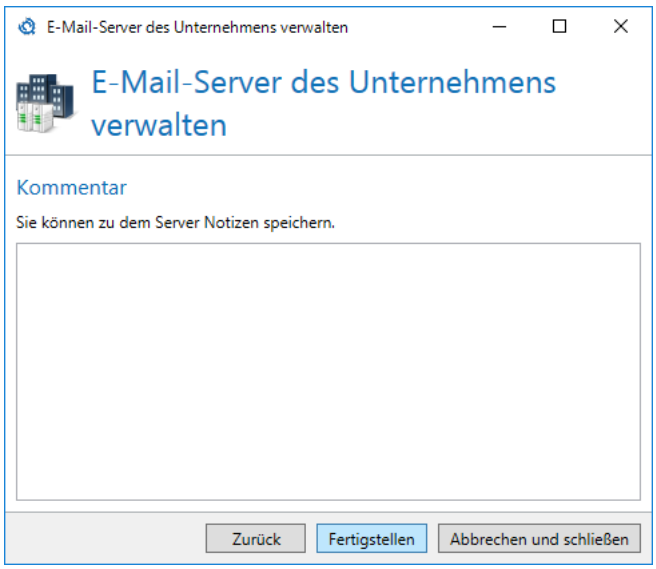


Bild 105: Sie können optional einen Kommentar verfassen

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 106) 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.

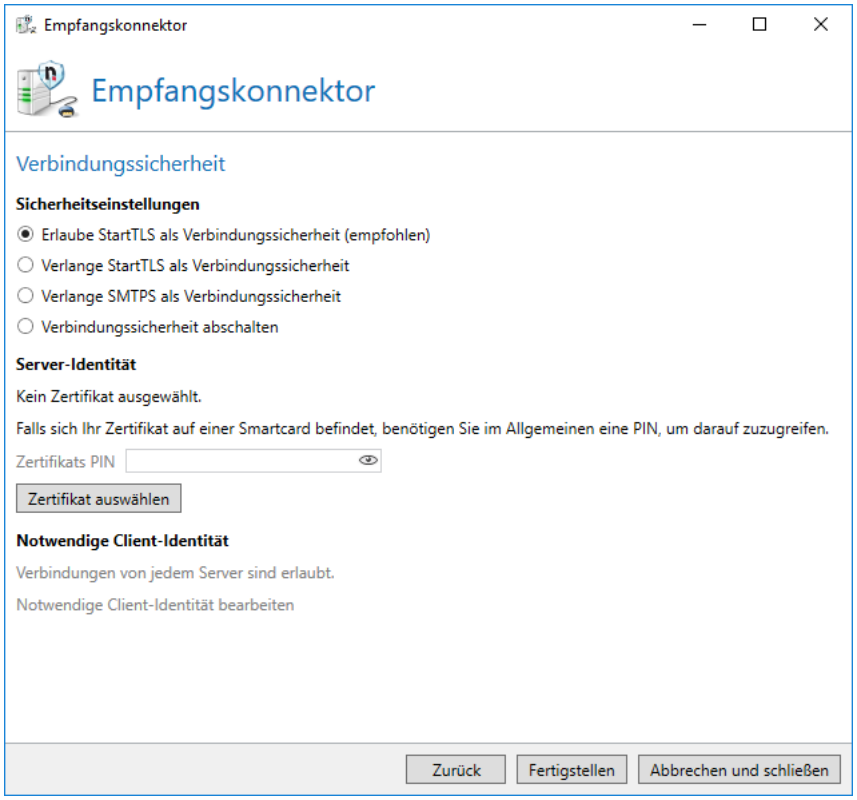


Bild 106: Einstellungen für die Verbindungssicherheit

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 107):

- **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.

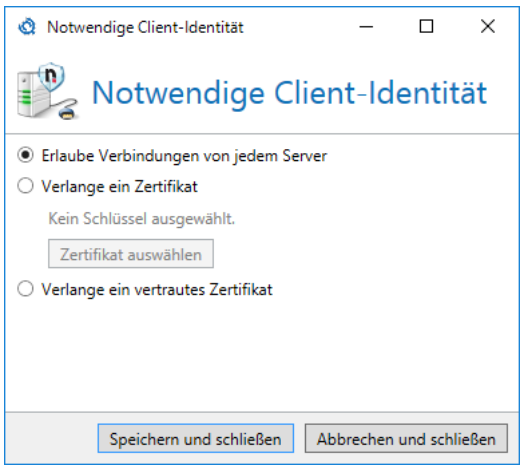


Bild 107: Festlegung der notwendigen Client-Identität

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.

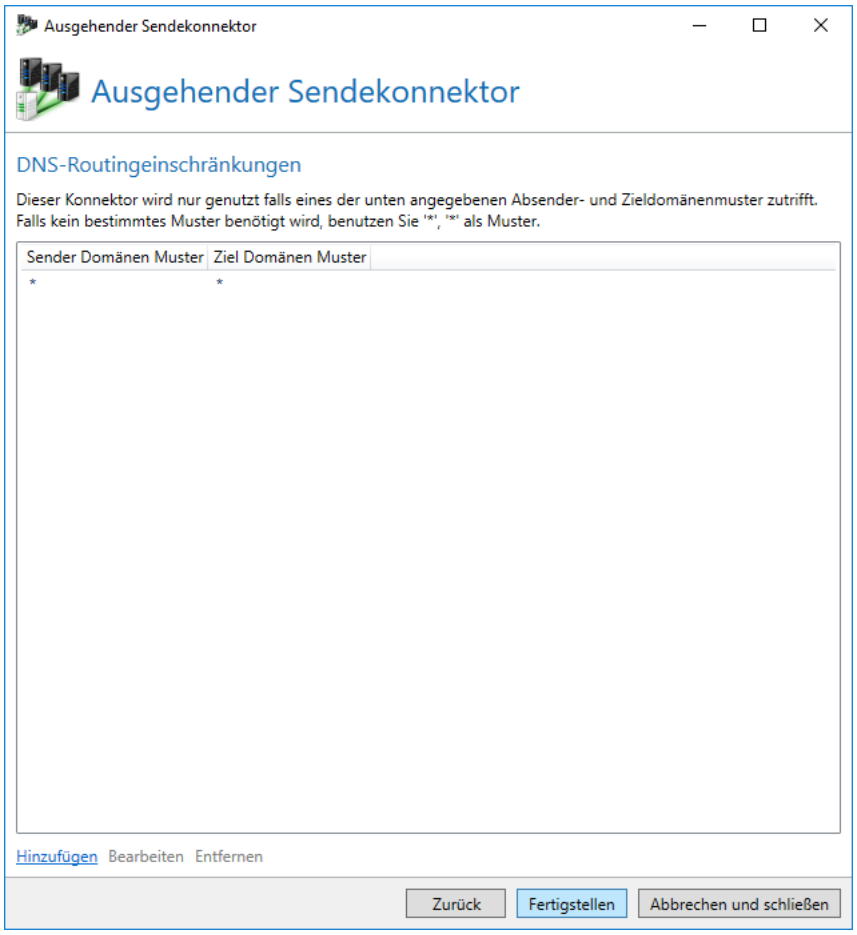


Bild 108: Die Konnektor-Namensräume bestimmen, welche Absender- oder Empfänger-Domänen von einem Konnektor verwaltet werden

Ein Konnektor-Namensraum (Bild 109) besteht aus einem Muster für sowohl die "Sender Domäne" als auch "Ziel Domäne". Dieses Muster darf auch Platzhalter ('*' und '?') enthalten.

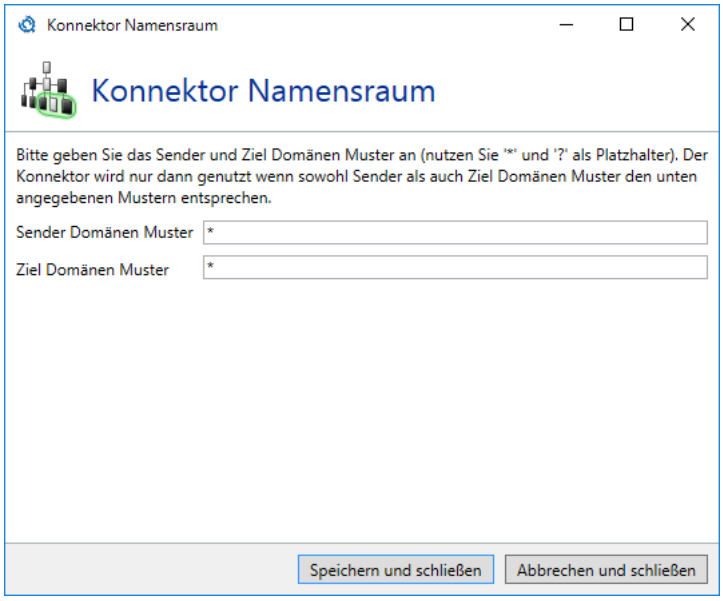


Bild 109: Eine Definition eines DNS Namensraums

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 110). Dies ist in der Regel die IP-Adresse bzw. der Servername des nächsten Mailsystems für E-Mails.

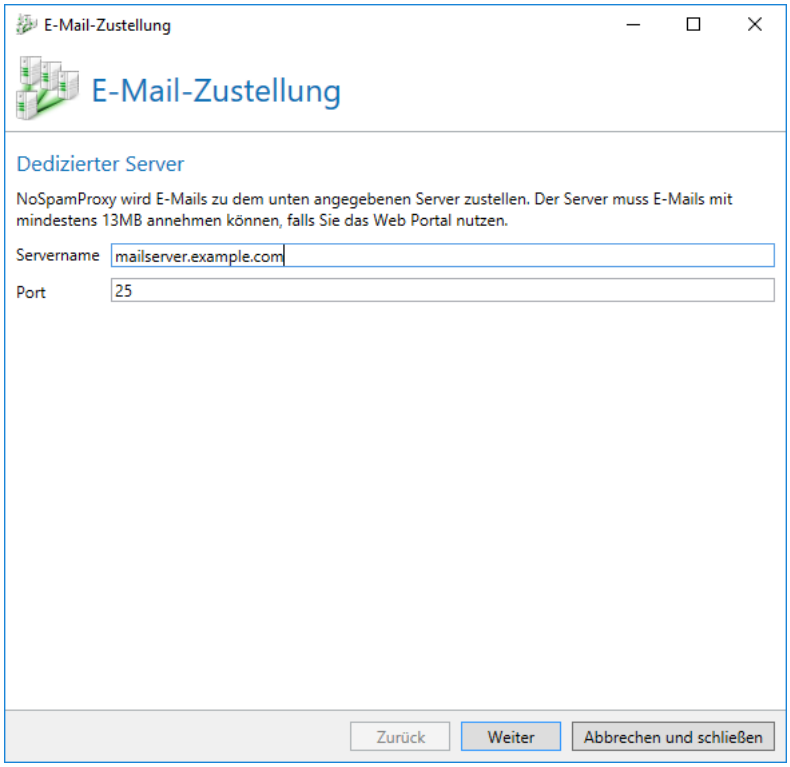


Bild 110: Verbindungseinstellungen für den dedizierten Server

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 111).

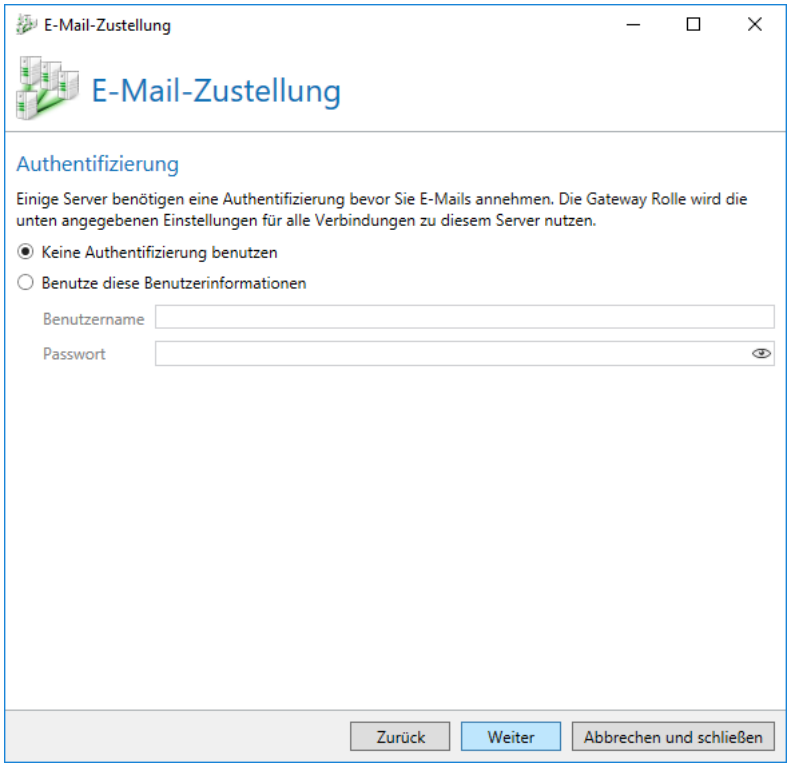


Bild 111: Hier können Sie ggf. Anmeldeinformationen für den dedizierten Server hinterlegen

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 112). SMTP-Sendekonnektoren für E-Mails an externe Adressen nutzen die zertifikatsbasierte Identität als Client-Identität.

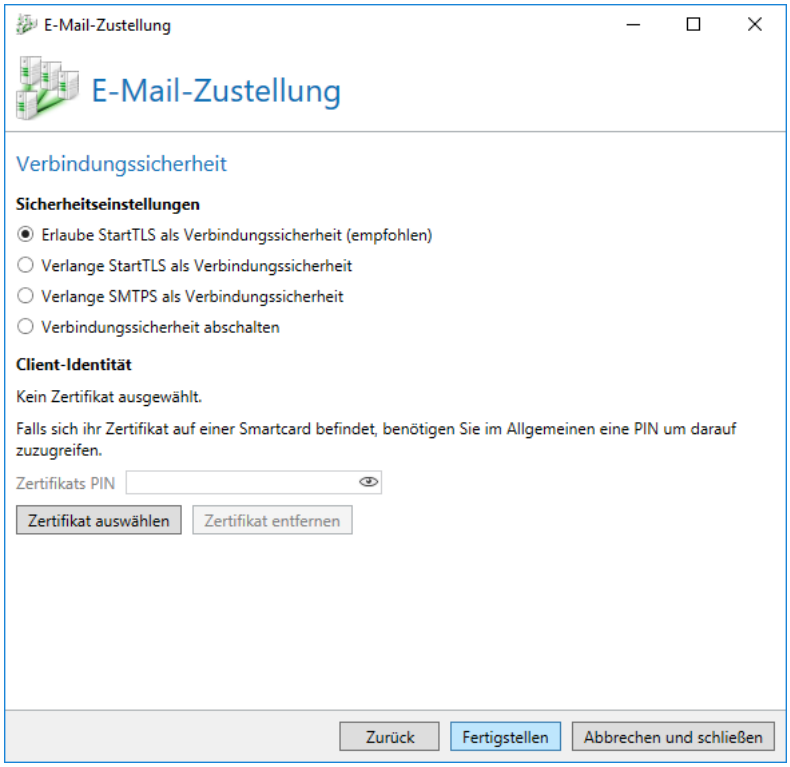


Bild 112: Verbindungssicherheit eines SMTP-Smarthosts

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.

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.

Als ersten Schritt legen Sie den Typ fest (Bild 113).

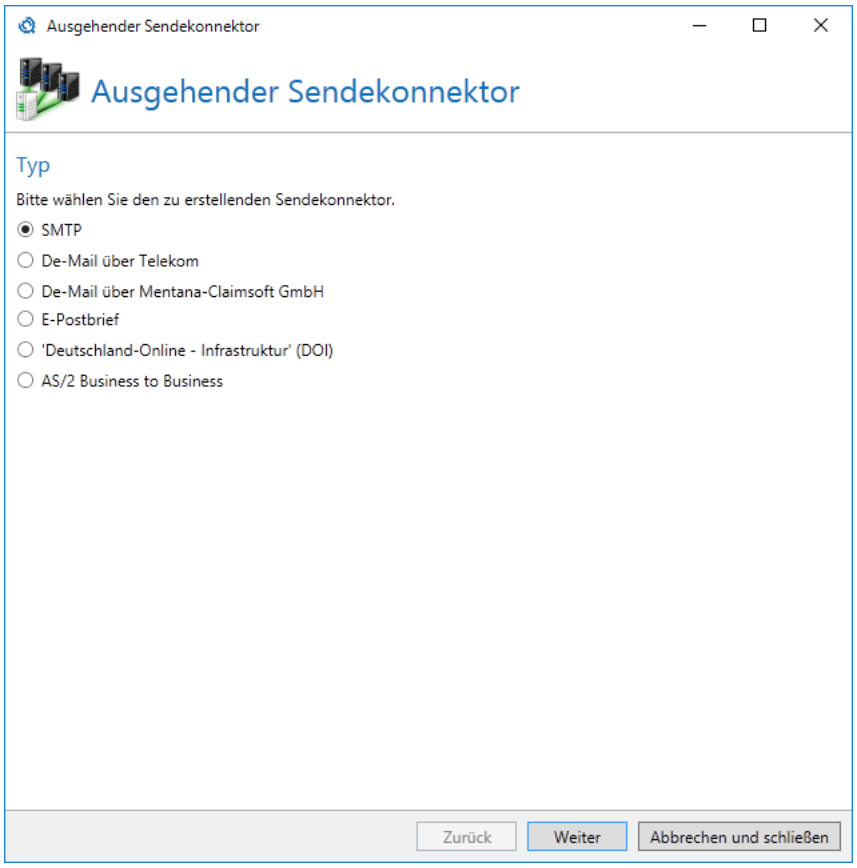


Bild 113: Die Typauswahl für einen neuen Sendekonnektor

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 114).

Bild 114: 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 115).

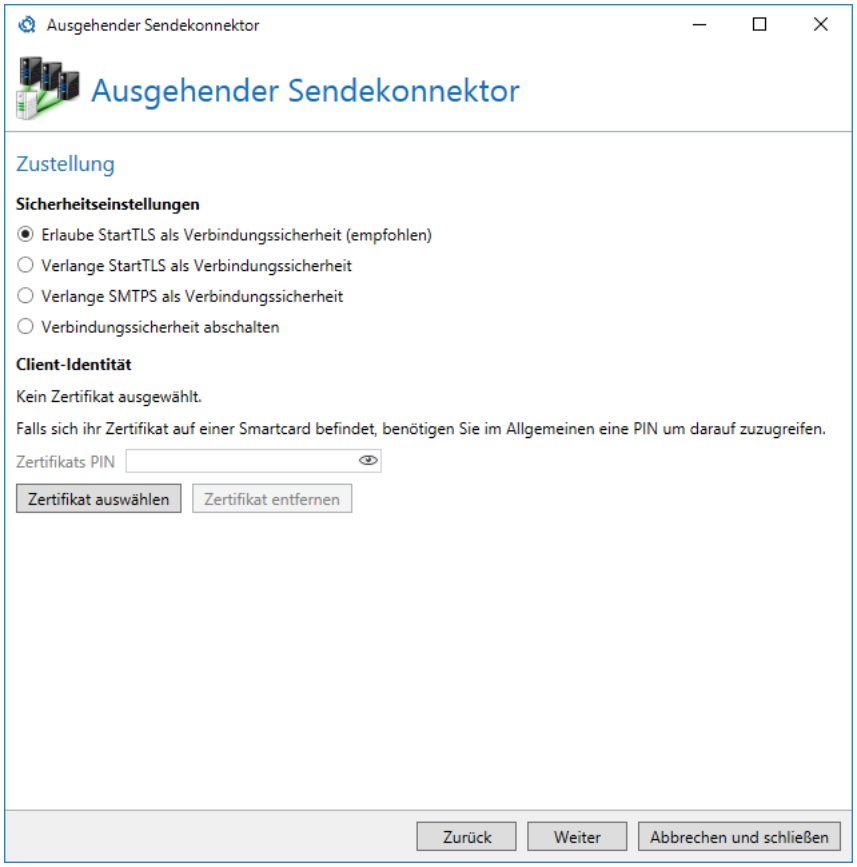


Bild 115: Verbindungssicherheit des SMTP-Sendekonnektors

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 116). Als nächsten Schritt konfigurieren Sie, wie bei allen De-Mail-Sendekonnektoren, die Zuordnung der eigenen Domänen.

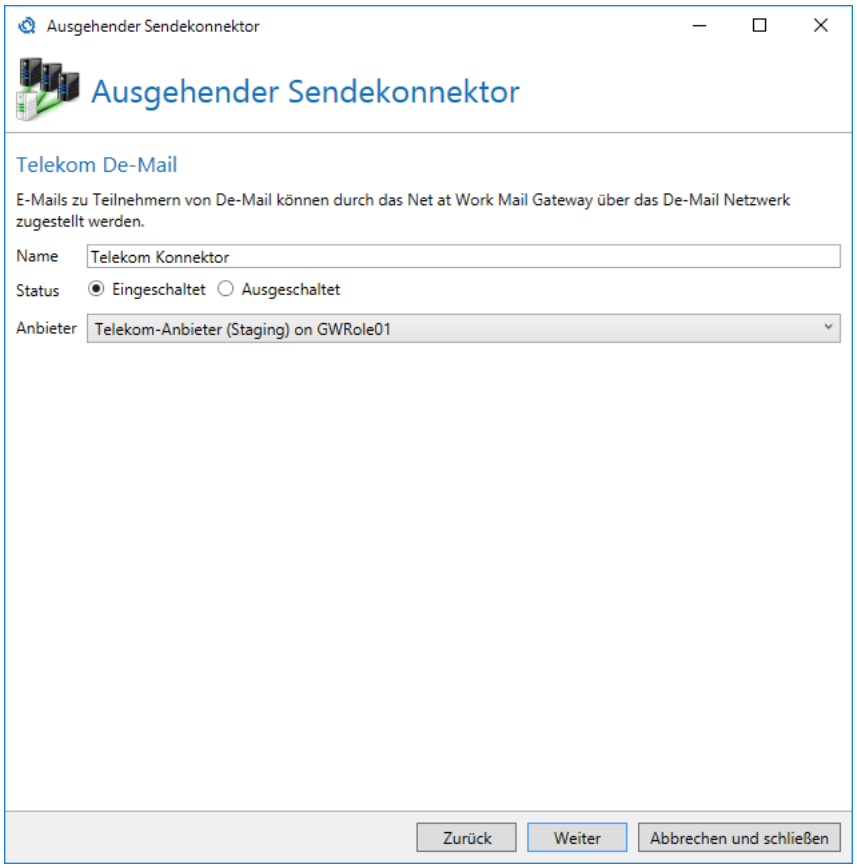


Bild 116: Einstellungen eines Telekom De-Mail-Konnektors

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 117). Wählen Sie im nächsten Schritt die eigenen Domänen die mit diesem De-Mail-Konnektor E-Mails versenden können.

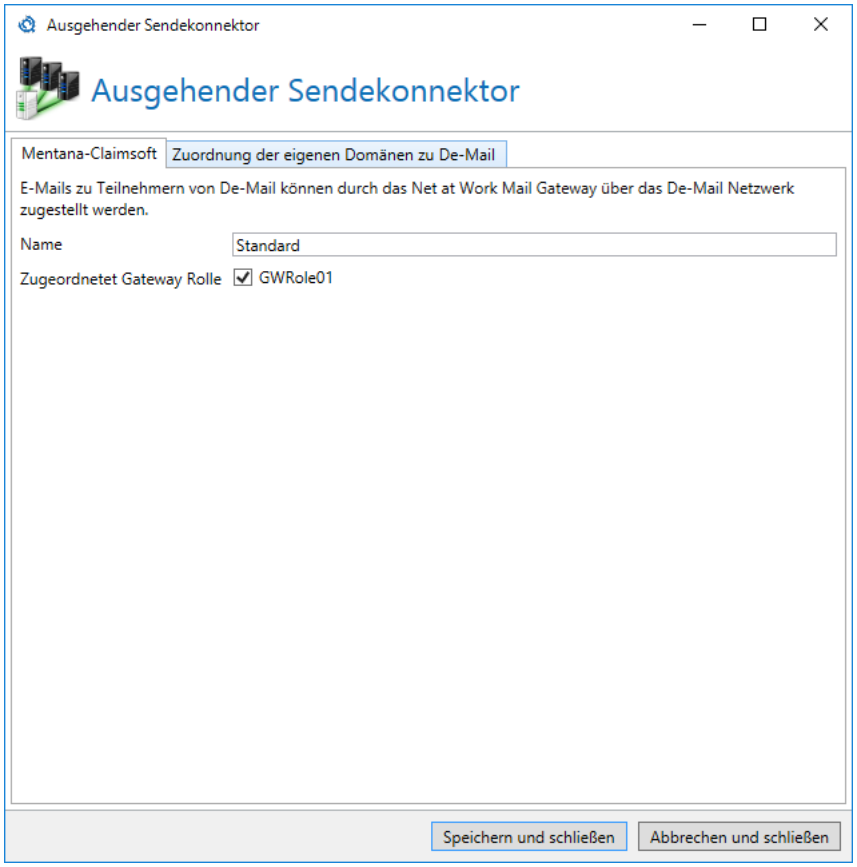


Bild 117: Mentana-Claimsoft De-Mail-Konnektor

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.

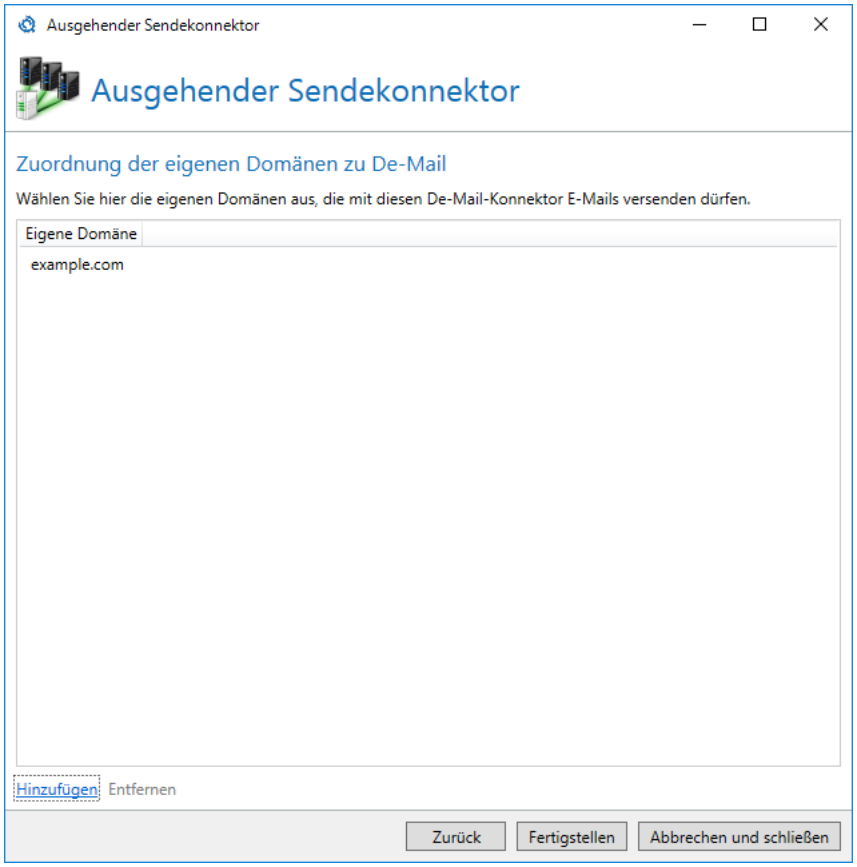


Bild 118: Zuordnung der eigenen Domänen zu den De-Mail-Sendekonnektor

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 119).

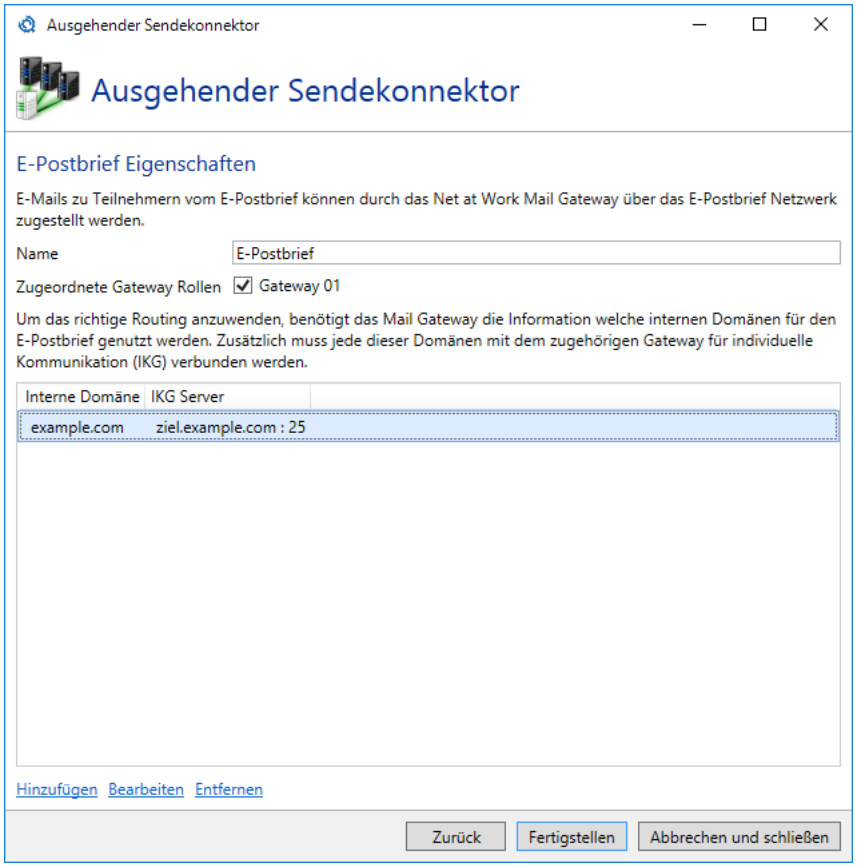


Bild 119: Die Konfiguration für die Zustellung von E-Postbriefen

Die Zuordnung der eigenen Domänen zu den IKGs erfolgt über einen eigenen Dialog (Bild 120).

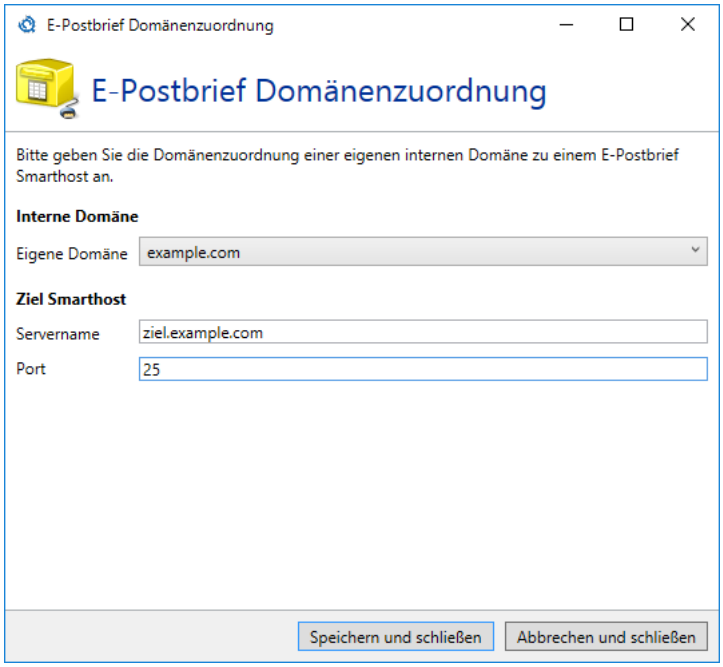


Bild 120: Die Zuordnung einer eigenen Domäne zu einem IKG

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 121).

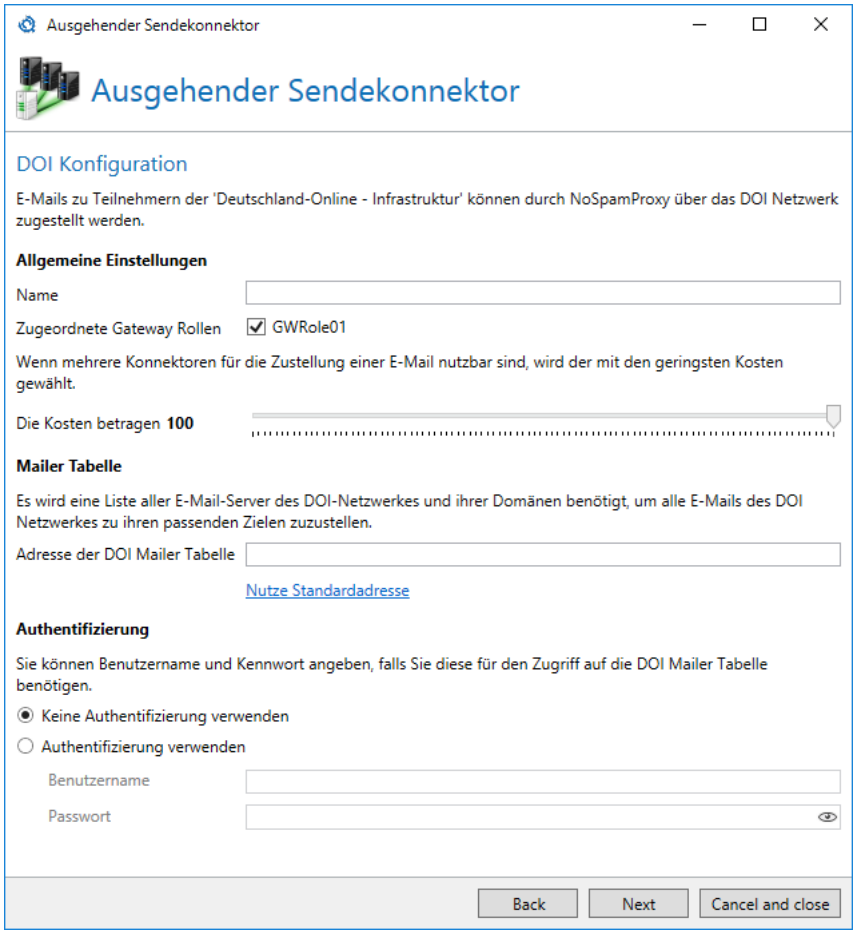


Bild 121: Die Konfiguration für die Zustellung in das Netz von Deutschland-Online - Infrastruktur

Auf der Seite **DOI Zustellung** können Sie das Verhalten für ungültige Absender konfigurieren (Bild 122). 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.

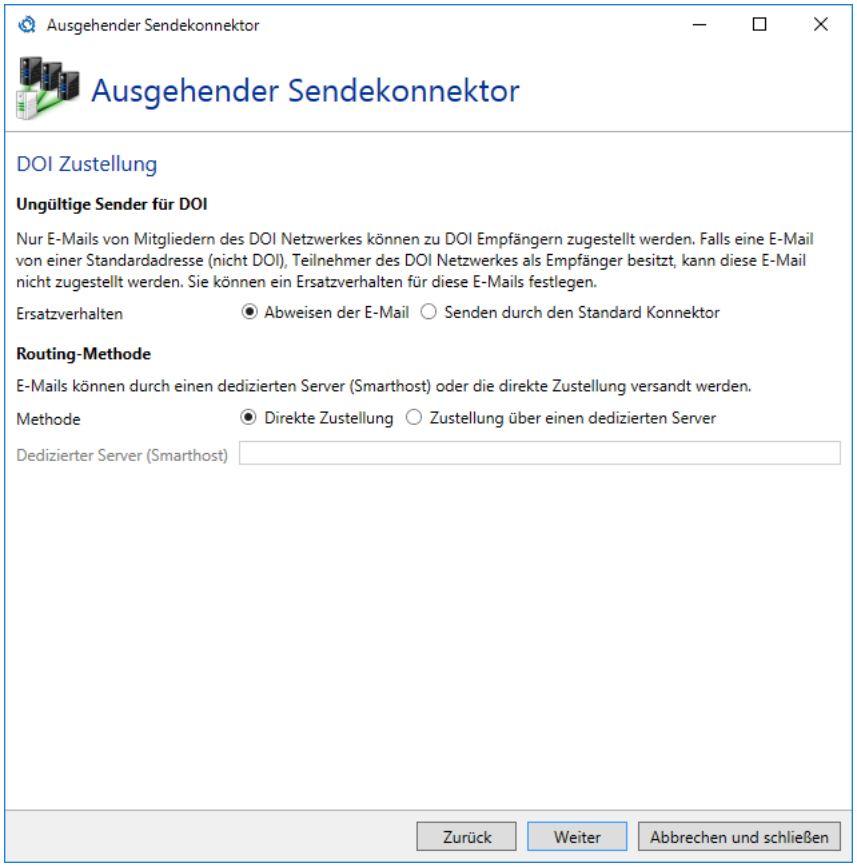


Bild 122: Erweiterte Zustelloptionen für das DOI Netz

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.

AS/2 Business To Business

Der AS/2-Konnektor erlaubt es Ihnen, EDI-Dateien an ein AS/2-konformes System weiterzuleiten (Bild 123).

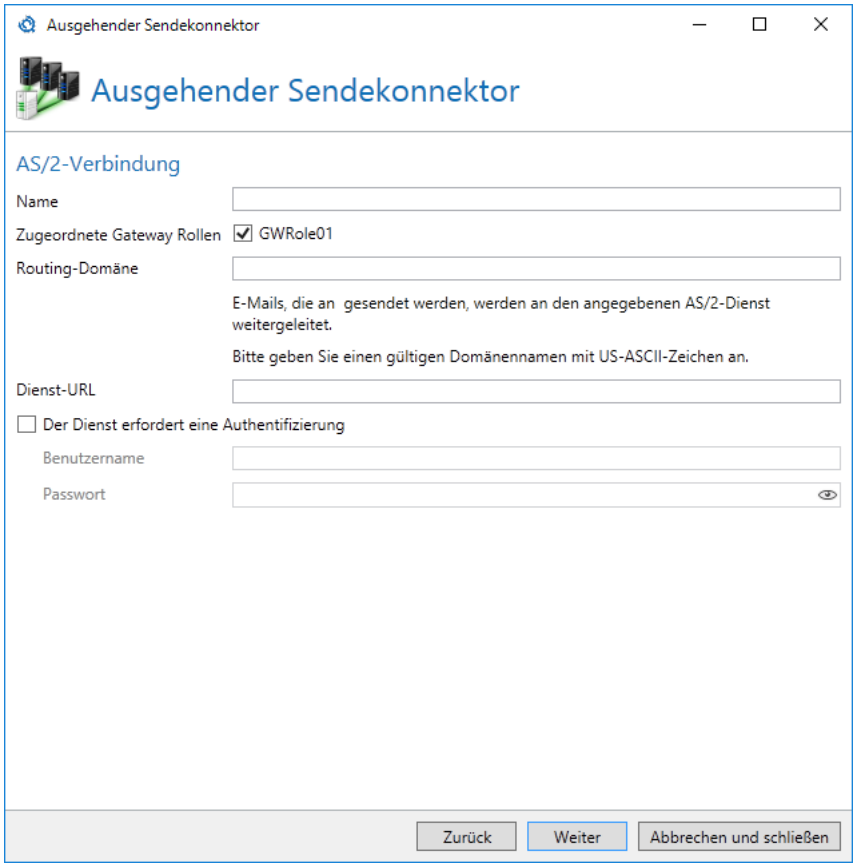


Bild 123: Die Konfiguration für die Zustellung über einen AS/2-Konnektor

Über die Routing-Domäne geben Sie an, welche E-Mails über diesen Konnektor geroutet werden. Wenn Sie hier z.B. 'example' eingeben, dann erfasst dieser Konnektor alle E-Mails, die an *@example.as2 geschickt werden. Sie können Ihr internes System also z.B. so konfigurieren, dass die EDIFACT-Daten an as2@example.as2 geschickt werden. Der lokale Teil der Adresse wird dabei ignoriert.

Der Konnektor wird immer eine synchrone Quittung (Mail Delivery Notification) anfordern. Berücksichtigen Sie dies, wenn Sie die Konfiguration mit Ihrem Handelspartner austauschen.

Der Konnektor wird alle E-Mails verarbeiten, die genau einen EDI-Anhang haben. Nach dem Versand der Datei wird die Zustellquittung des AS/2-Dienstes an den Absender der ursprünglichen E-Mail weitergeleitet.

Die Dienst-URL sowie, falls notwendig, Authentifizierungsdaten erhalten Sie von Ihrem Handelspartner. Gleiches gilt für die Daten auf der nächsten Seite (Bild 124).

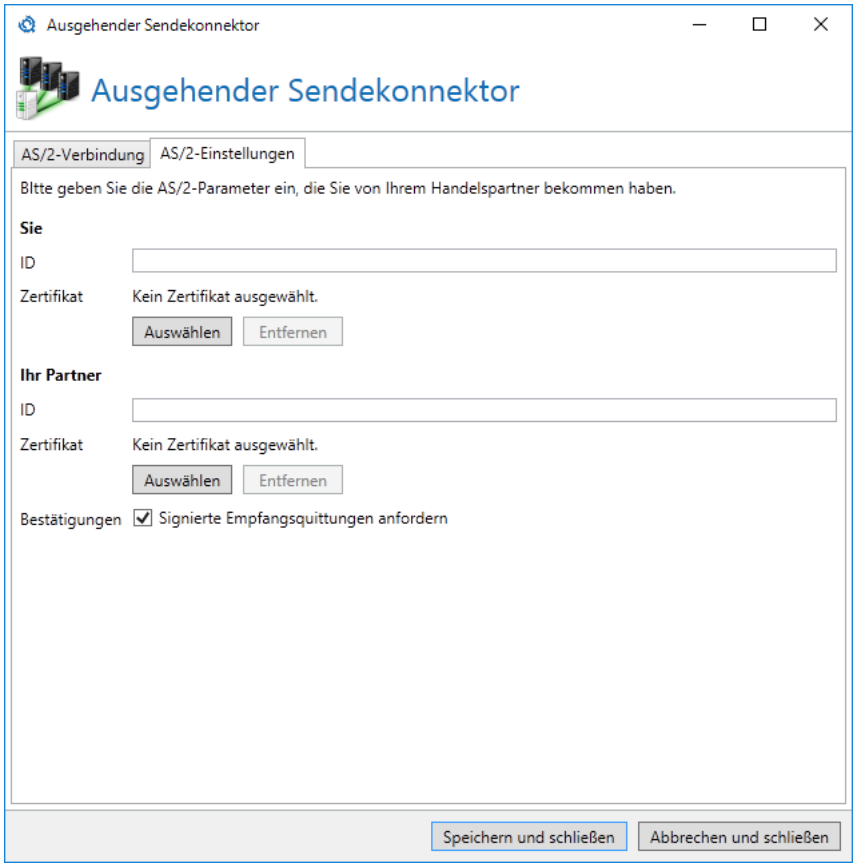


Bild 124: Die Verbindungsparameter für die Zustellung über einen AS/2-Konnektor

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.

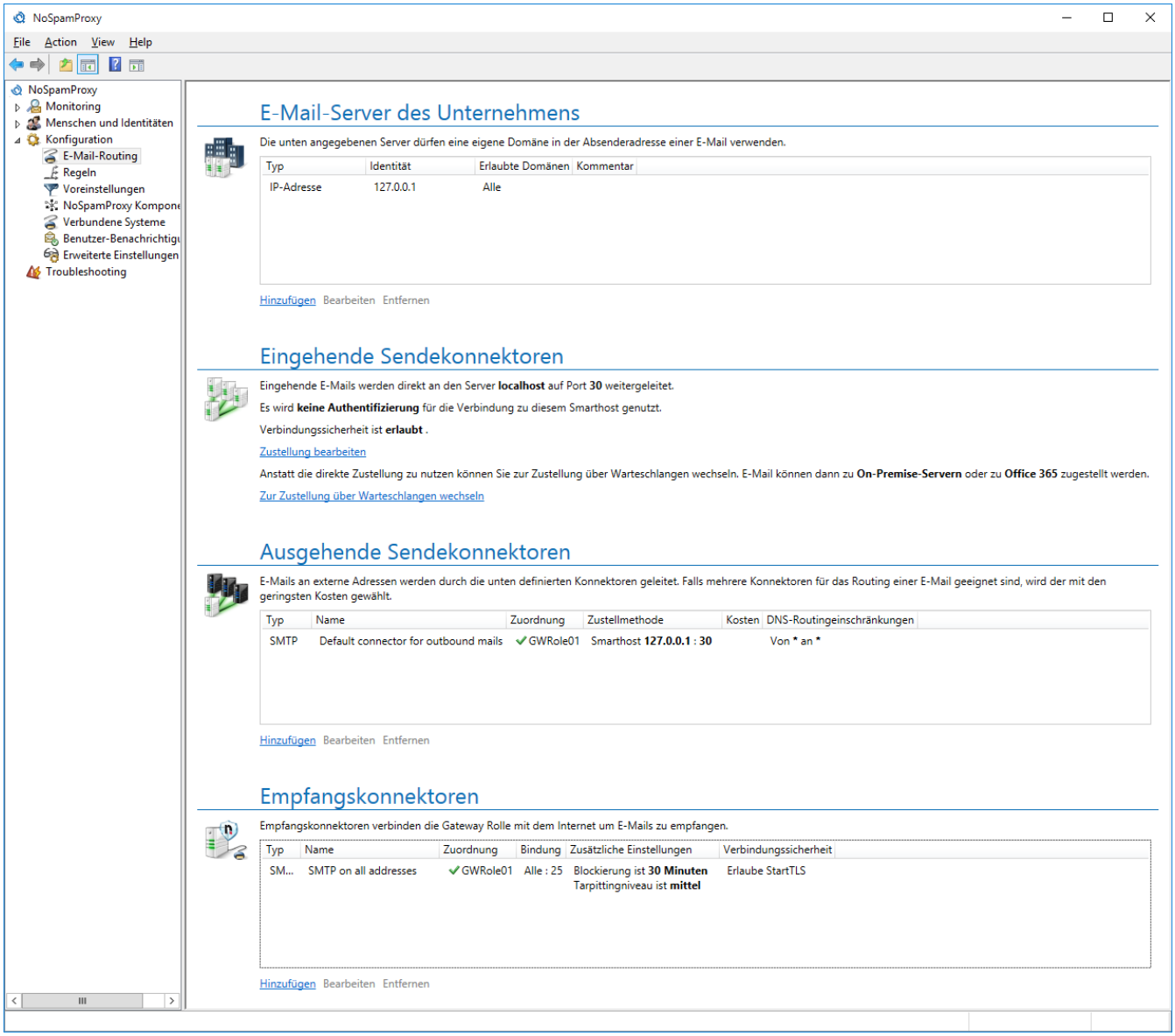


Bild 125: Die Übersicht über alle Konnektoren auf denen NoSpamProxy E-Mails empfängt und sendet.

Beim Erstellen eines neuen Empfangskonnektors wählen Sie auf der ersten Seite den Typ aus (Bild 126).

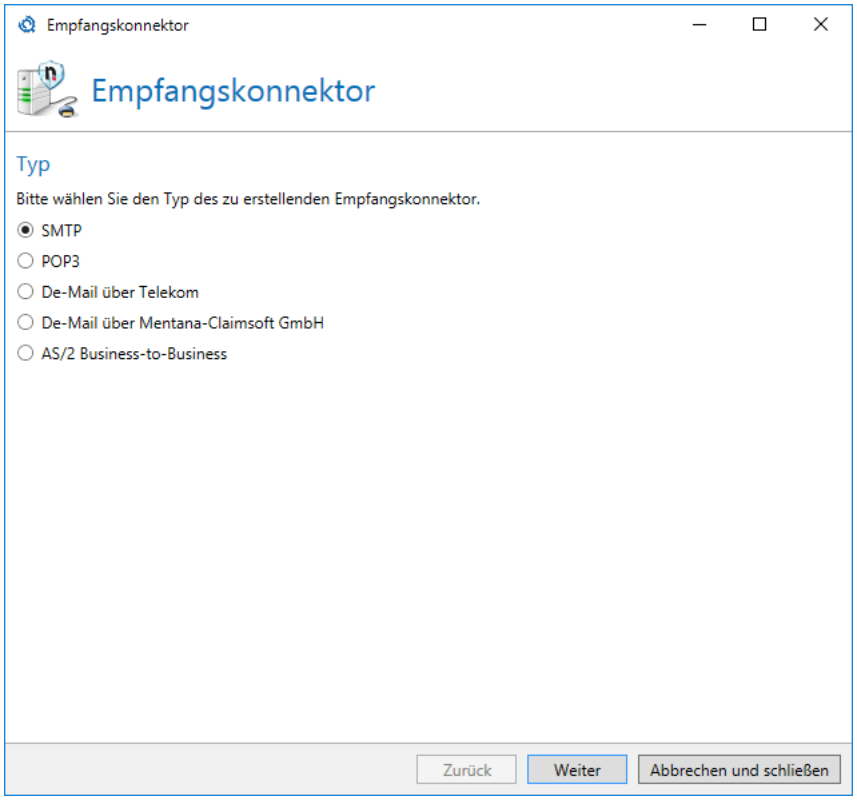


Bild 126: Die Auswahl des Konnektortyps

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 127) 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.

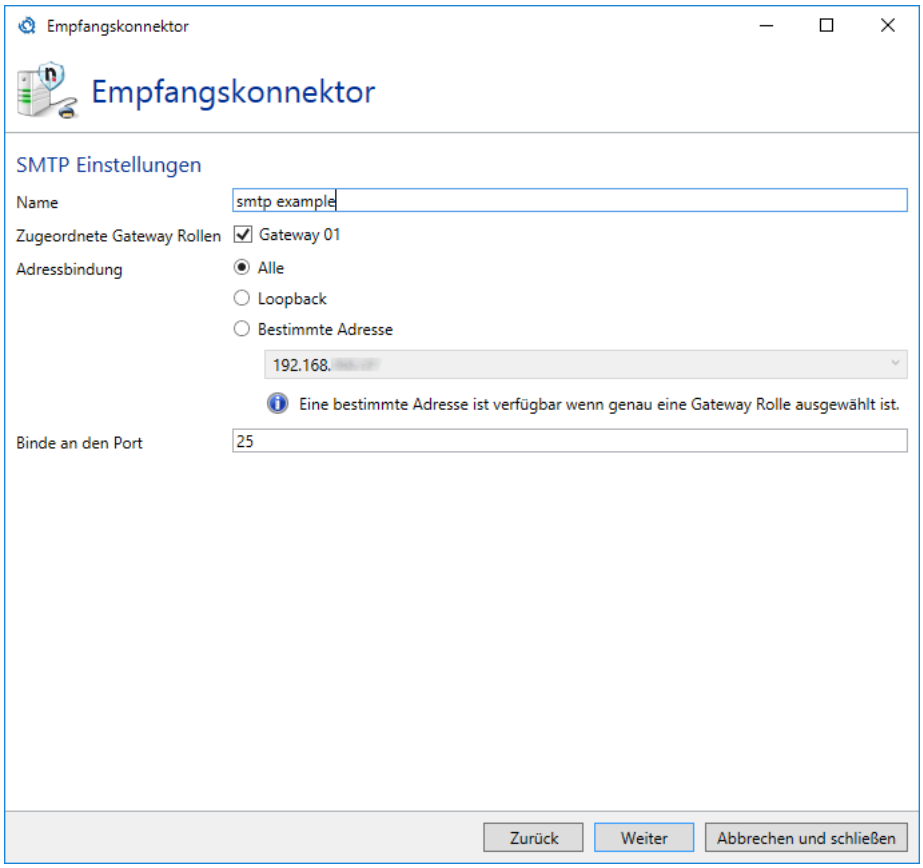


Bild 127: Die Verbindungssicherheit eines SMTP Empfangskonnektors

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 128) zeigt die Konfigurationseinstellungen für diese ungültigen Anfragen.

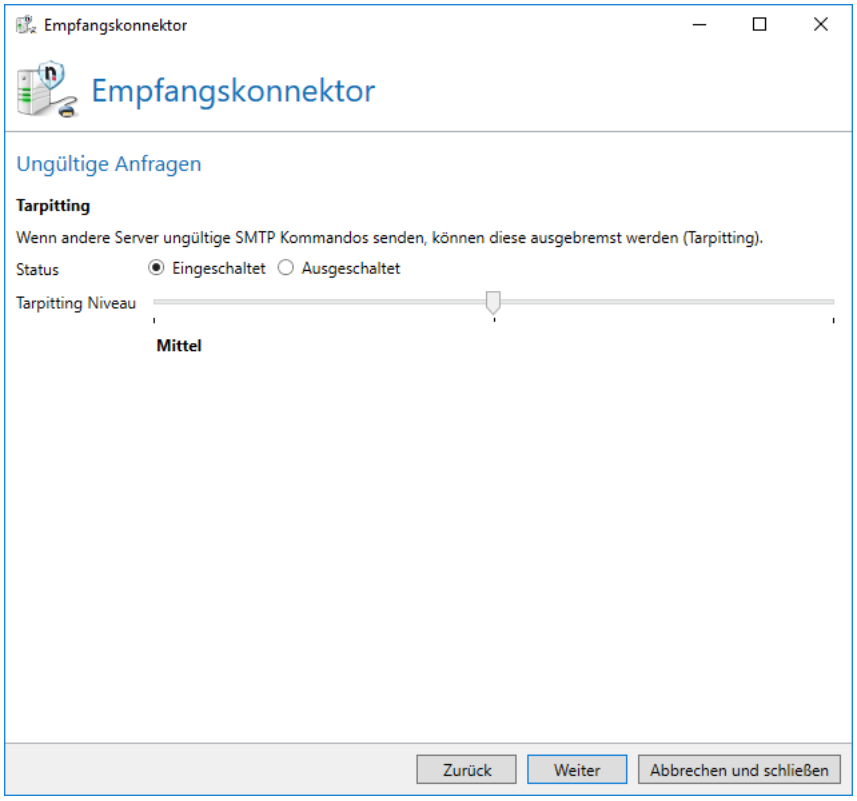


Bild 128: Bestimmen Sie die Verhaltensweise beim Empfang von ungültigen SMTP Kommandos

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 129). 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.

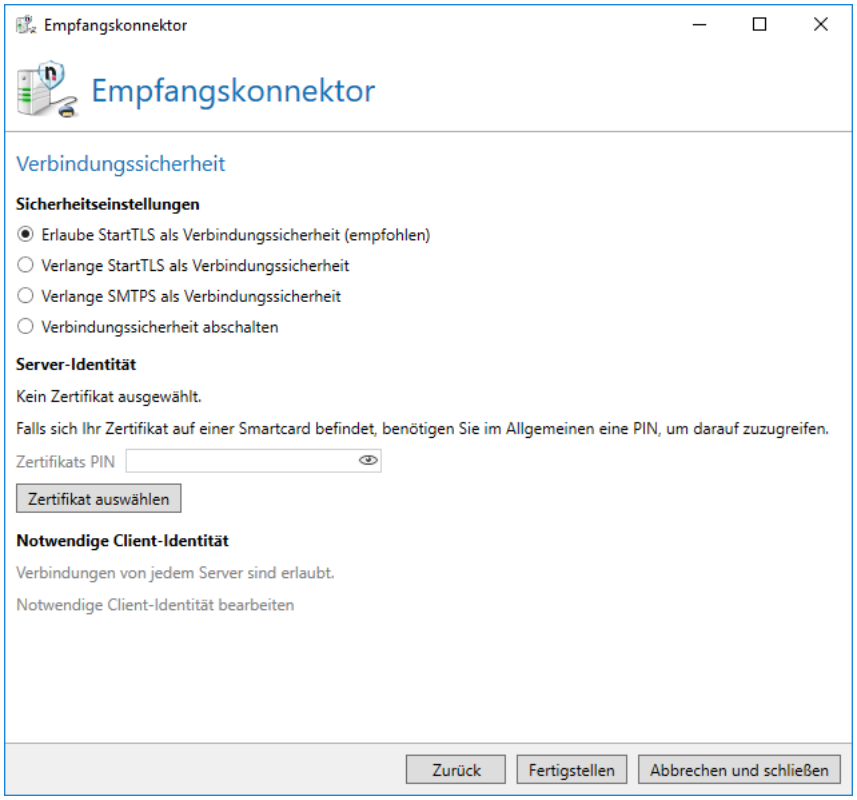


Bild 129: Die Verbindungssicherheit eines SMTP Empfangskonnektors

POP3 Konnektor

Mit dem POP3 Konnektor können externe POP3 Postfächer durch NoSpamProxy Encryption auf neue E-Mails überprüft und abgeholt werden. Alle abgeholten E-Mails werden dann vom Gateway an die konfigurierte interne Adresse zugestellt.

Bestimmen Sie einen eindeutigen Namen und die Gateway Rolle auf der dieser Konnektor arbeiten soll. Mit dem **Herunterladeintervall** bestimmen Sie in welchen Abständen der Konnektor neue E-Mails von der Gegenstelle herunterladen soll (Bild 130).

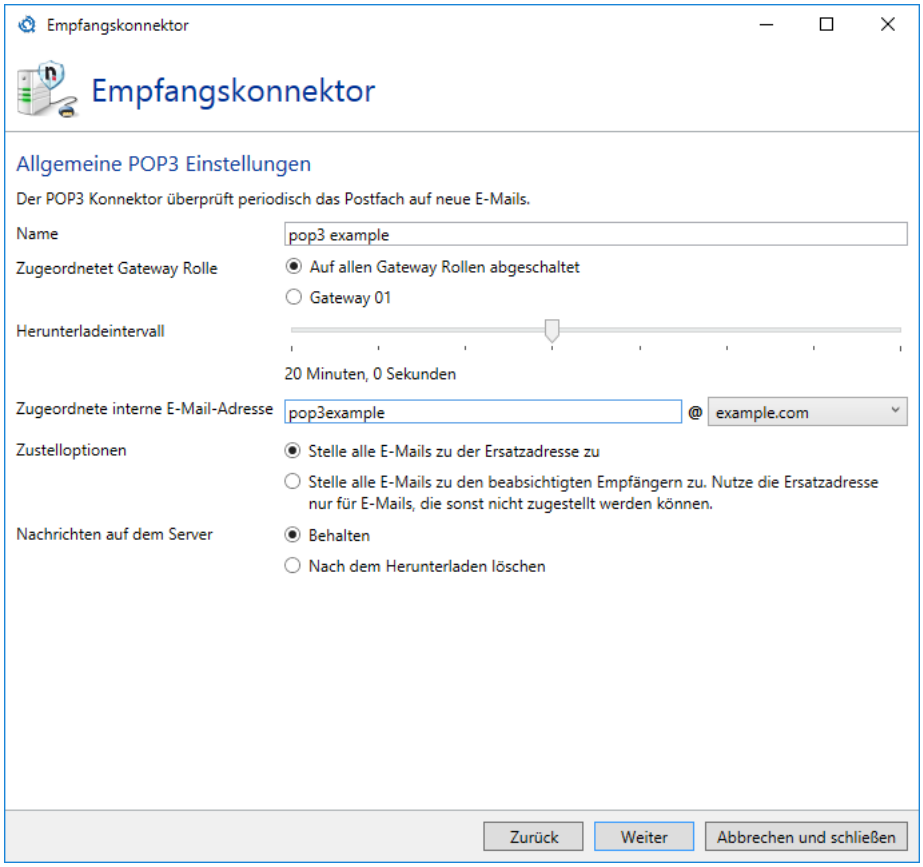


Bild 130: Allgemeine Einstellungen des POP3-Konnektors

Im Bereich **E-Mail-Zustellung** wird neben einer internen E-Mail-Adresse auch das Zustellverhalten konfiguriert. Wenn Sie als Zustelloption **Alle E-Mails an die zugeordnete interne E-Mail-Adresse zustellen** ausgewählt haben, werden die Empfängerdaten in den abgeholten E-Mails ignoriert und die E-Mails werden alle an die angegebene Adresse gesendet. Bei Auswahl der zweiten Option werden die Empfängerdaten aus den E-Mails extrahiert und die E-Mails werden an die entsprechenden Empfänger weitergeleitet. Die angegebene Adresse wird nur für E-Mails verwendet, in denen keine internen E-Mail-Adressen gefunden werden kann.

Sie können hier außerdem festlegen, ob die E-Mails nach dem Herunterladen vom Server entfernt werden. Falls Sie die E-Mails auf dem Server lassen, dann werden sie trotzdem nur einmalig heruntergeladen.

Auf der Seite **Postfacheinstellungen** werden Name, Netzwerk-Port des Servers sowie die Benutzerinformationen für den Zugriff auf diesen, hinterlegt (Bild 131).

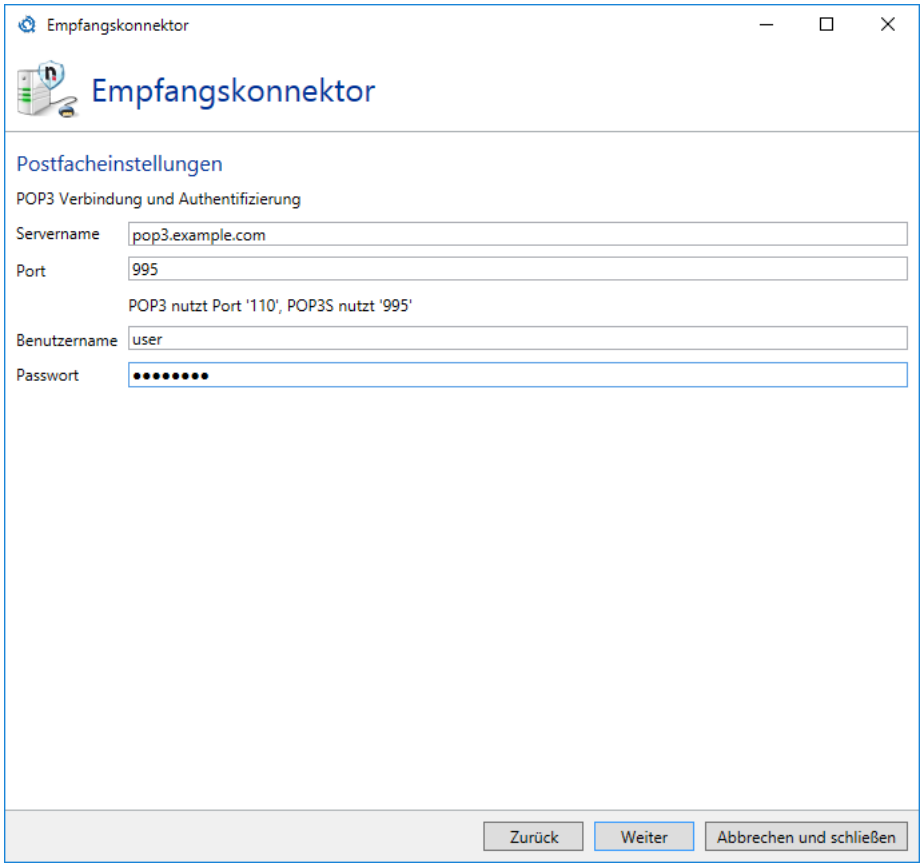


Bild 131: Die Einstellungen für den Server des POP3-Postfachs

Der Empfangskonnektor nutzt in der Verbindungssicherheit eine Server-Identität. Als Sicherheitseinstellungen für die Verbindungssicherheit stehen hier die Optionen TLS als Verbindungssicherheit nutzen, für eine Verbindung zu einem Server der eine verschlüsselte Verbindung über POP3S unterstützt, und Verbindungssicherheit abschalten für eine unverschlüsselte Verbindung über POP3 zur Verfügung (Bild 131).

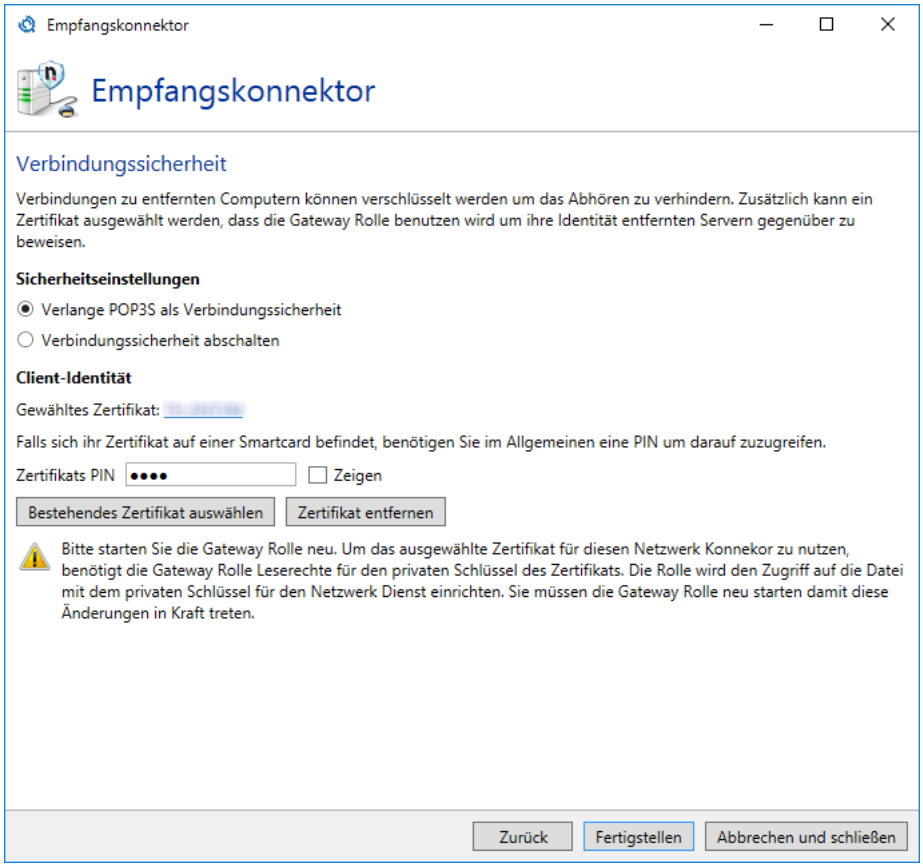


Bild 132: Die Verbindungssicherheit des POP3-Konnektors

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.

Legen Sie nun zuerst einen Namen fest, und bestimmen Sie dann, ob der Konnektor eingeschaltet oder abgeschaltet sein soll. Die Zuordnung zu einer Gateway Rolle wird durch den konfigurierten De-Mail-Anbieter festgelegt. Der Konnektor läuft immer auf der Gateway Rolle auf der das im De-Mail-Anbieter konfigurierte Zertifikat liegt. Bestimmen Sie durch die Einstellung des **Herunterladeintervalls**, wie oft NoSpamProxy Encryption das De-Mail-Postfach auf neue Nachrichten überprüfen soll (Bild 133).

Geben Sie in der Liste der De-Mail-Domänen für jeden Eintrag an, ob die De-Mails dieser Domäne heruntergeladen werden sollen. Legen Sie auch eine E-Mail-Adresse fest, die benutzt werden kann, falls der ursprüngliche Empfänger der De-Mail in Ihrem Unternehmen nicht mehr verfügbar ist.

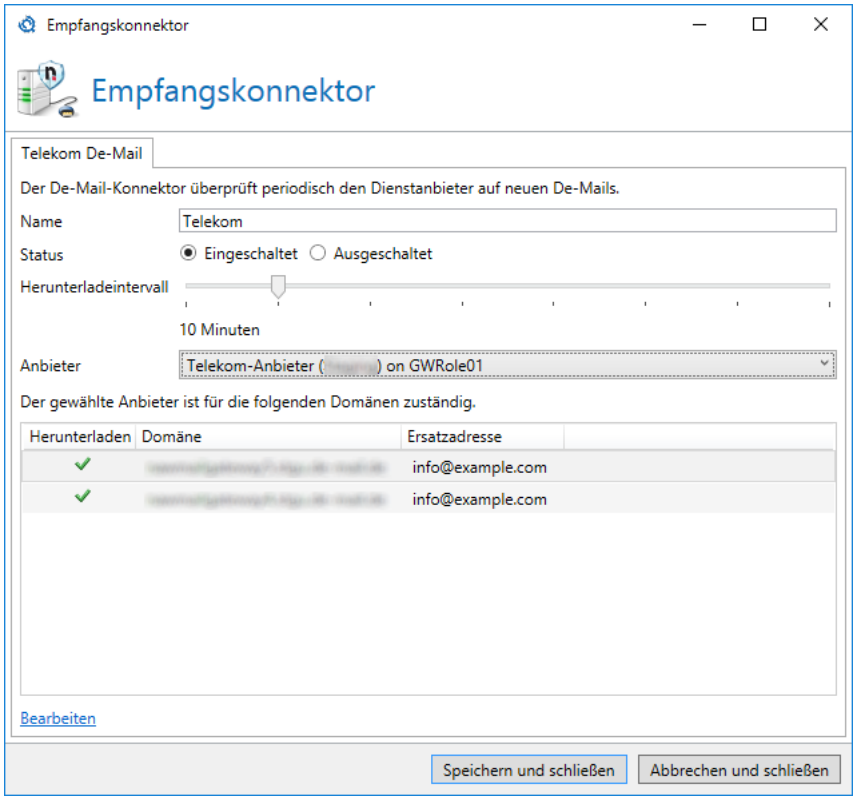


Bild 133: Ein Telekom De-Mail-Konnektor mit seinen De-Mail-Domänen

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.

Bestimmen Sie einen eindeutigen Namen und die Gateway Rollen, auf denen der Konnektor arbeiten soll. Mit dem **Herunterladeintervall** bestimmen Sie in welchen Abständen der Konnektor neue De-Mails von der Gegenstelle herunterladen soll (Bild 134).

Geben Sie in der Liste der Postfächer für jedes Postfach eine E-Mail-Adresse an, die benutzt werden kann, falls der ursprüngliche Empfänger der De-Mail in Ihrem Unternehmen nicht mehr verfügbar ist. Mindestens eine De-Mail-Domäne muss in der Liste zum Herunterladen markiert und mit einer Ersatzadresse konfiguriert sein.

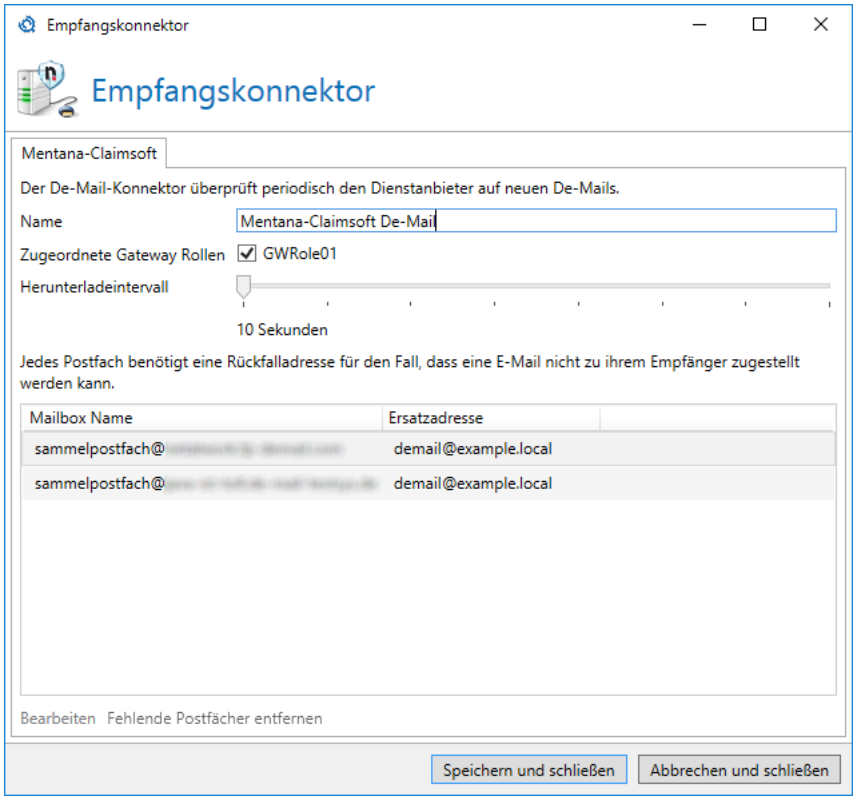


Bild 134: Mentana-Claimsoft De-Mail-Konnektor

AS/2 Business To Business

Der AS/2-Konnektor erlaubt es Ihnen, EDI-Dateien von einem Handelspartner zu empfangen. Die empfangenden Daten werden dann an einen E-Mail-Empfänger weitergeleitet. (Bild 135).

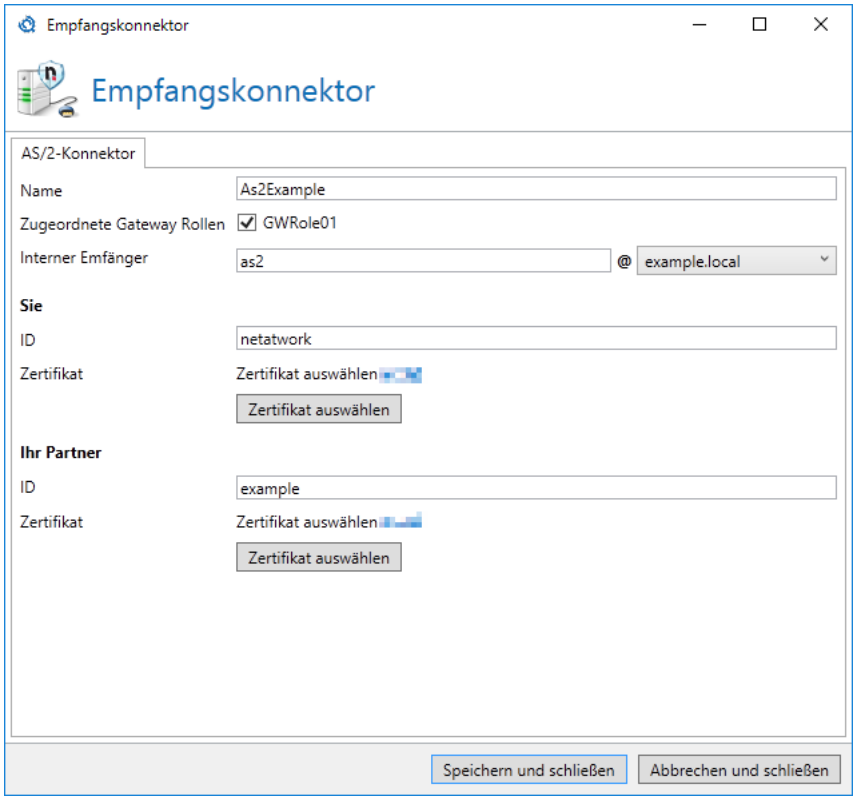


Bild 135: Die Konfiguration für den Empfang von Daten über einen AS/2-Konnektor

Geben Sie beim **Internen Empfänger** an, an wen empfangene Daten weitergeleitet werden.

Für die AS/2-Verbindung müssen Sie sowohl ein eigenes Zertifikat als auch ein Zertifikat Ihres Handelspartners haben. Des Weiteren benötigen Sie AS/2-Ids beider Teilnehmer. Diese Daten müssen Sie mit Ihrem Handelspartner abstimmen.

Der Konnektor setzt sowohl eine Signatur als auch eine Verschlüsselung voraus.

Der Konnektor ist nach der Einrichtung über die Adresse `http://gatewayrolle:6060/nospamproxy/api/as2/<name>` erreichbar. `<name>` ist hier der Name des Konnektors. Diese Adresse müssen Sie nun noch über Ihre Firewall im Internet veröffentlichen.

Veröffentlichen Sie unbedingt nur die URL `/nospamproxy/api/as2` und nicht den vollständigen Port. Andernfalls sind die Webservices für die Administration von NoSpamProxy über das Internet erreichbar.

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 Benutzung der Aktionen für die qualifizierte Signatur erfordert die Installation und Konfiguration eines digiSeal servers der secrypt GmbH (http://www.secrypt.de).

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 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

Die Filterung von E-Mails ist ohne die Funktion von NoSpamProxy Protection deaktiviert. Um E-Mails zu filtern, können Sie Ihre bestehende Lizenz jederzeit mit einer NoSpamProxy Protection Lizenz erweitern. Für weitere Details siehe Kapitel Mehrnutzen durch AntiSpam und AntiVirus

Aktionen

Aktionen für die E-Mail-Signatur und Verschlüsselung

Die Aktionen, die auf eine E-Mail angewandt werden können, gliedern sich in zwei Bereiche: Unterstützung von kryptographischen Schlüsseln durch S/MIME und PGP sowie qualifizierte Signaturen.

Die Unterstützung von kryptographischen Schlüsseln dient zur Verschlüsselung von E-Mail-Nachrichten, um zu verhindern, dass Dritte die Inhalte einsehen können. Qualifizierte Signaturen werden z.B. bei einem elektronischen Versand von Rechnungen benutzt, um die Authentizität der Dokumente zu belegen und zu sichern.

Konfiguration der Regeln

Die Regeln, wie E-Mails bearbeitet werden sollen, werden im Knoten **Regeln** gepflegt (Bild 136).

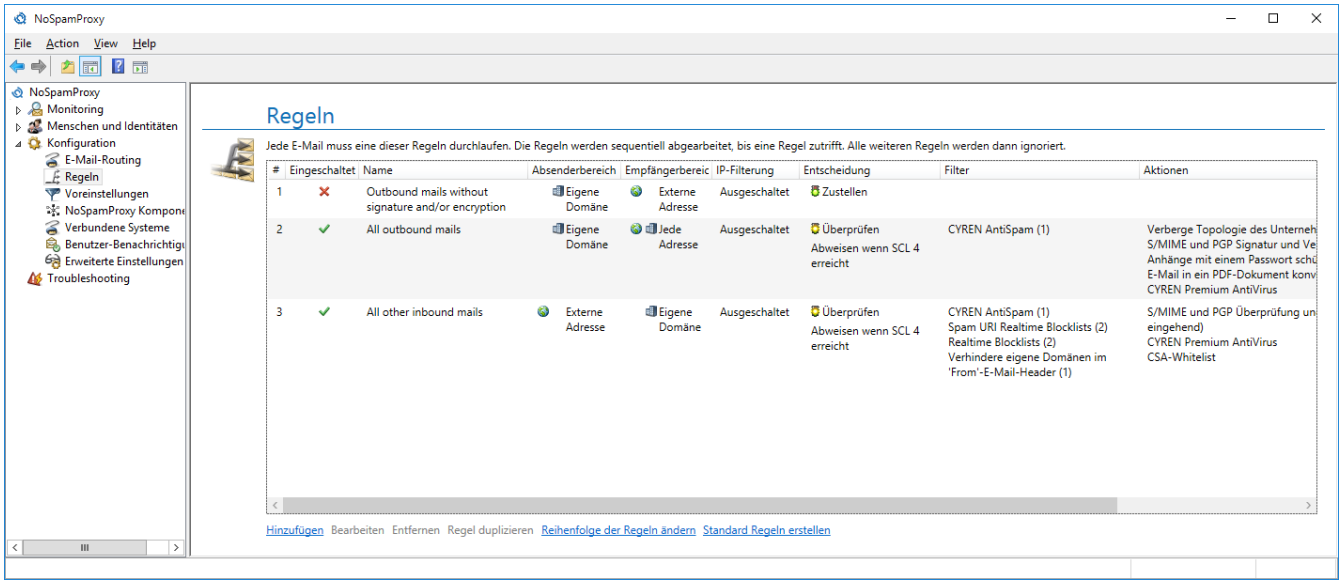


Bild 136: Die Übersicht über alle Regeln, die die Verarbeitung der E-Mails bestimmen

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 137). 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.

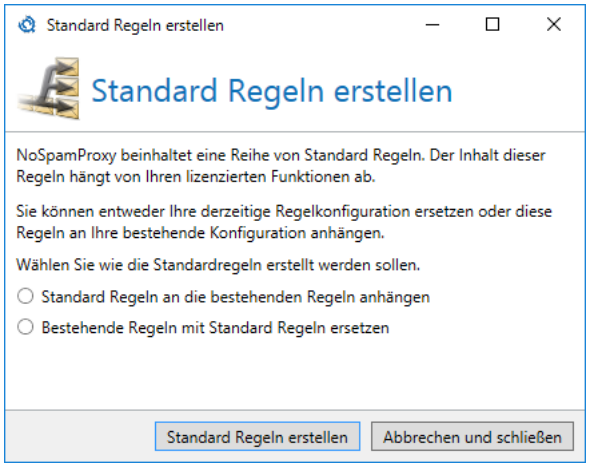


Bild 137: Erstellen der Standard Regeln

Neue Regel erstellen

Eine Regel besitzt folgende Einstellungen: **Allgemein**, **Richtung**, **Absender**, **Empfänger**, **Filter**, **Aktionen** und **Richtlinienverstoß**. 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 138) umfasst wichtige Parameter mit denen Sie grundlegende Eigenschaften festlegen.

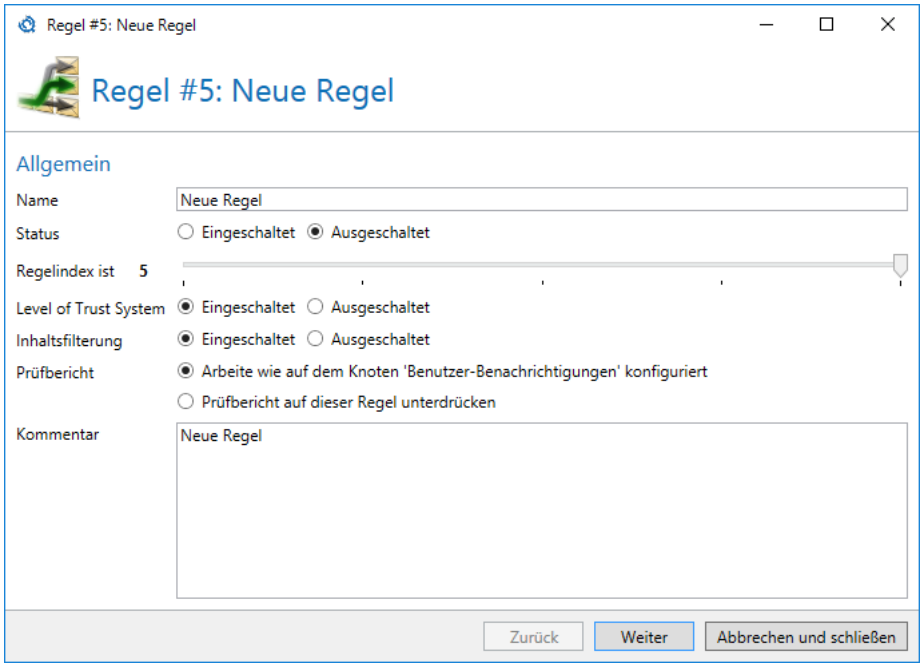


Bild 138: Allgemeine Einstellungen der Regel

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 **Inhaltsfilterung** können Sie die Überprüfung von Anhängen durch die Inhaltsfilter ein- oder abschalten.

Über die Option **Prüfbericht** können Sie die Erstellung des Prüfberichts auf einzelnen Regeln unterdrücken.

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 139).

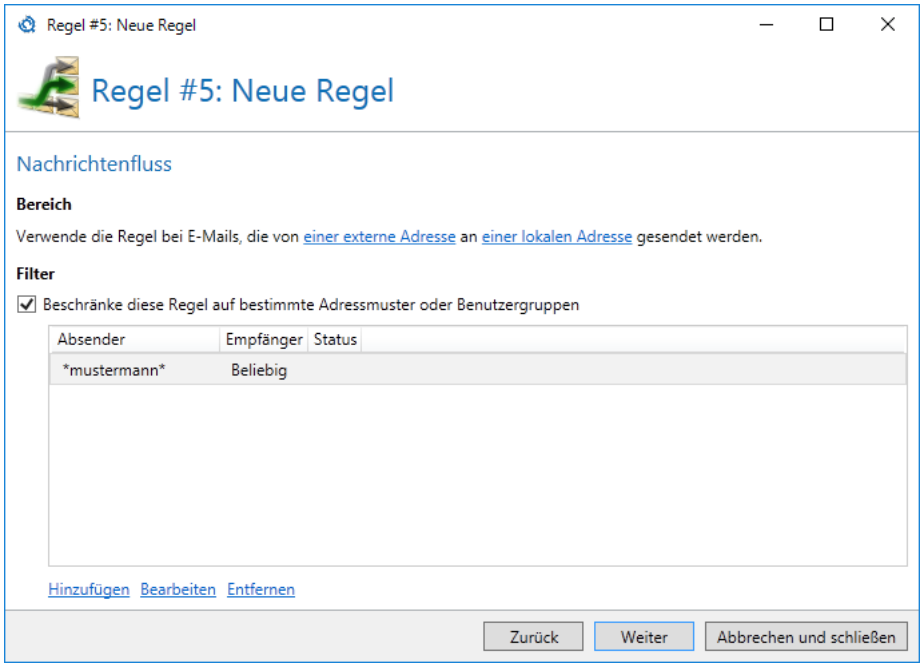


Bild 139: Geben Sie an, für welche Adressen diese Regel gelten soll.

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 140).

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.

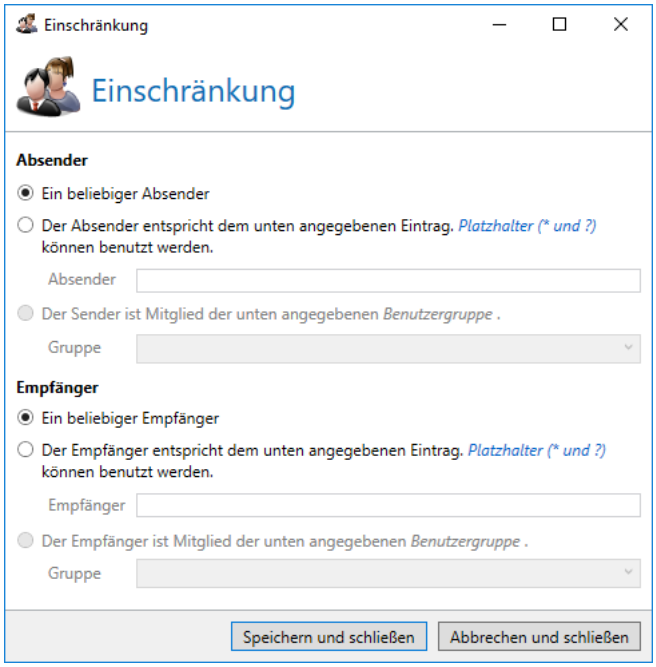


Bild 140: Konfigurieren eines Filtereintrags innerhalb einer Regel

Im Reiter **IP-Filterung** (Bild 141) können Sie die Regel auf bestimmte einliefernde Server einschränken.

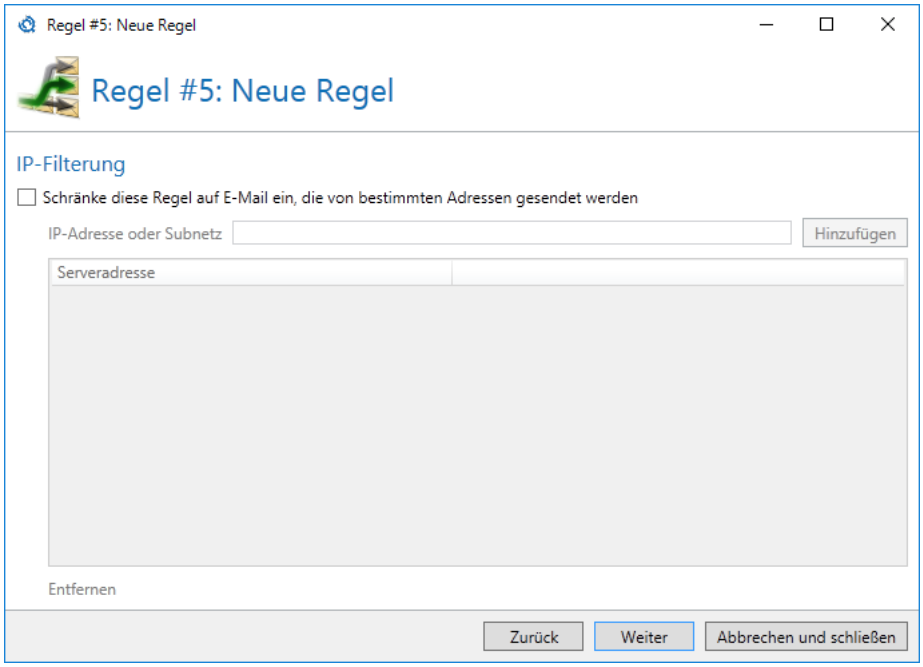


Bild 141: Definieren Sie die Gültigkeit der Regel in Bezug auf den einliefernden Server

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.

Durch NoSpamProxy Encryption steht Ihnen die Funktion "Automatisch Verschlüsseln" auf ausgehenden Regeln zur Verfügung. Das automatische Verschlüsseln von ausgehenden E-Mails benötigt die folgenden Aktionen.

- E-Mails in PDF-Dokumente konvertieren
- Anhänge mit einem Passwort schützen
- Signieren und/oder Verschlüsseln von E-Mails

Falls die oben aufgeführten Aktionen in der Regel fehlen, können Sie sie über den Link **Notwendige Aktionen hinzufügen** an die Liste anfügen lassen. Die Konfiguration der Aktionen entspricht dabei der Konfiguration der Standardregeln.

Die in der Regel aktiven Aktionen werden in der Liste **Aktive Aktionen** aufgeführt (Bild 142).

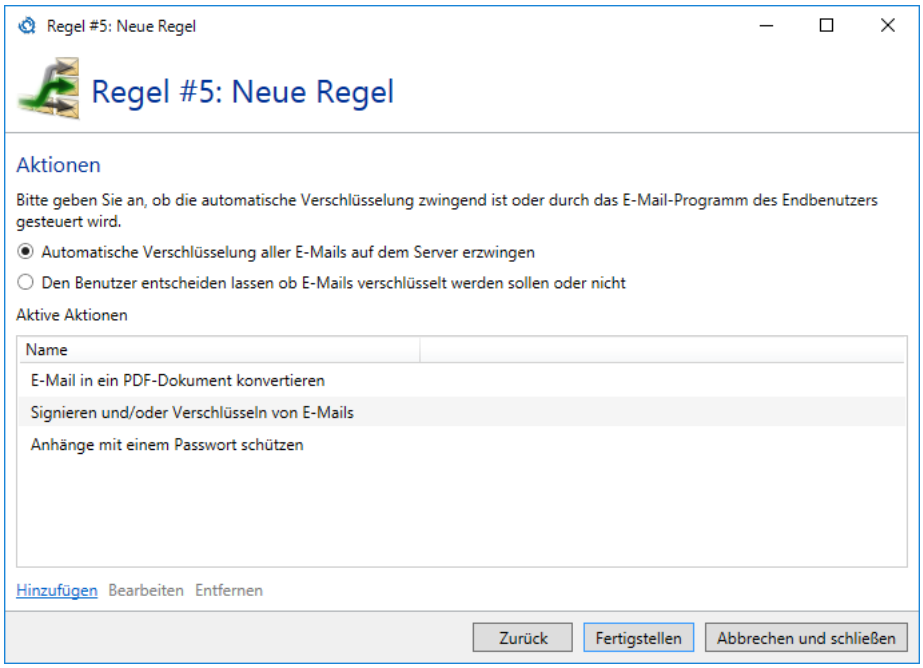


Bild 142: Die Aktionen einer E-Mail

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 143). 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.

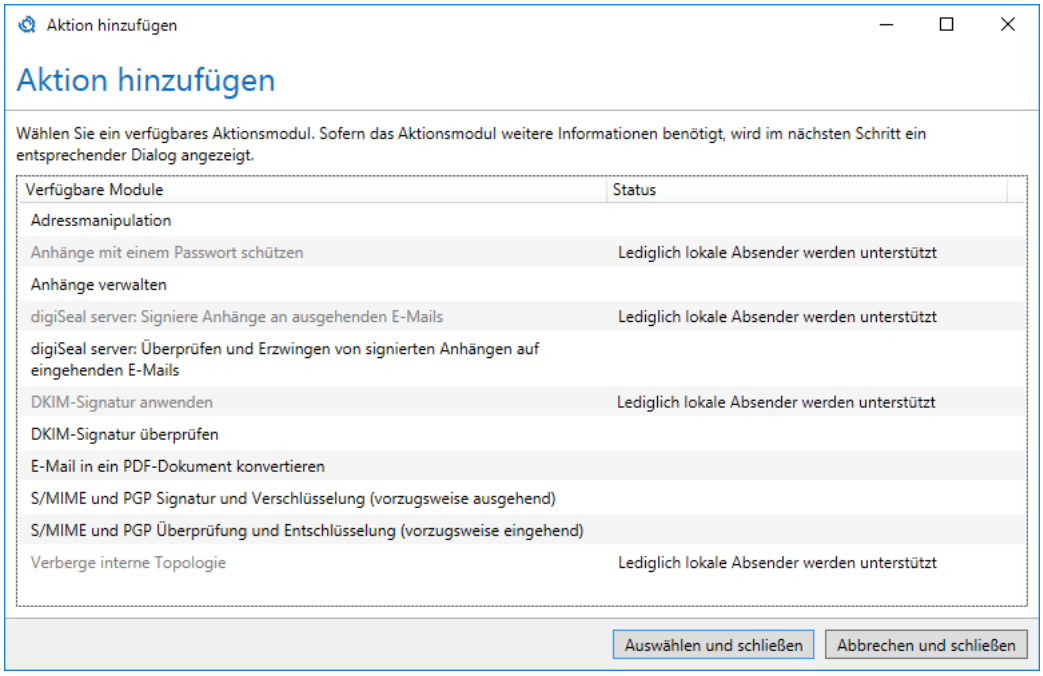


Bild 143: Aktionen aus dieser Liste können einer Regel hinzugefügt werden

Auf dem nächsten Reiter können Sie Einstellungen zum **Richtlinienvertoß** 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.

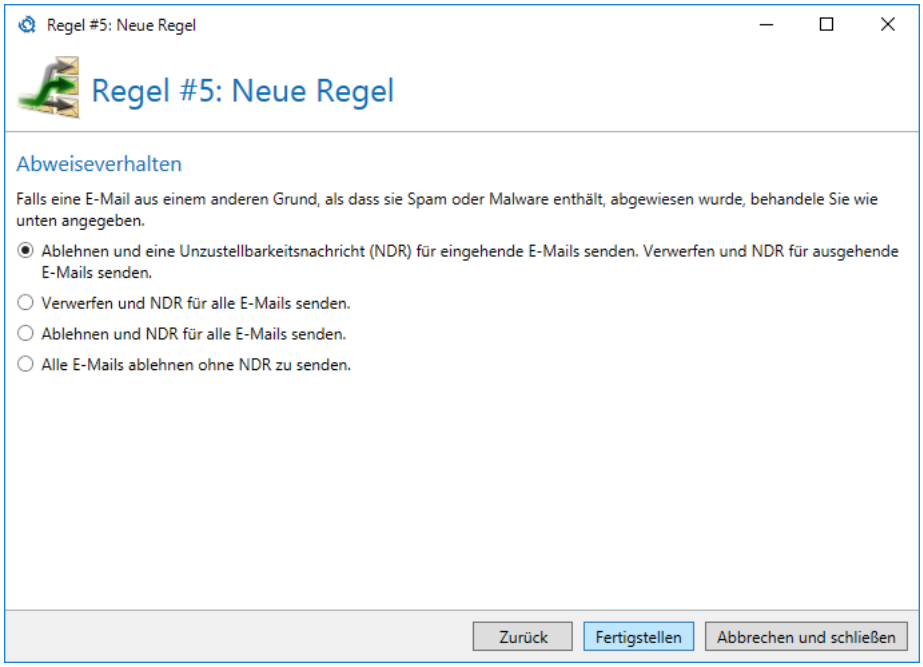


Bild 144: Verhalten bei Richtlinienverstoß

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.

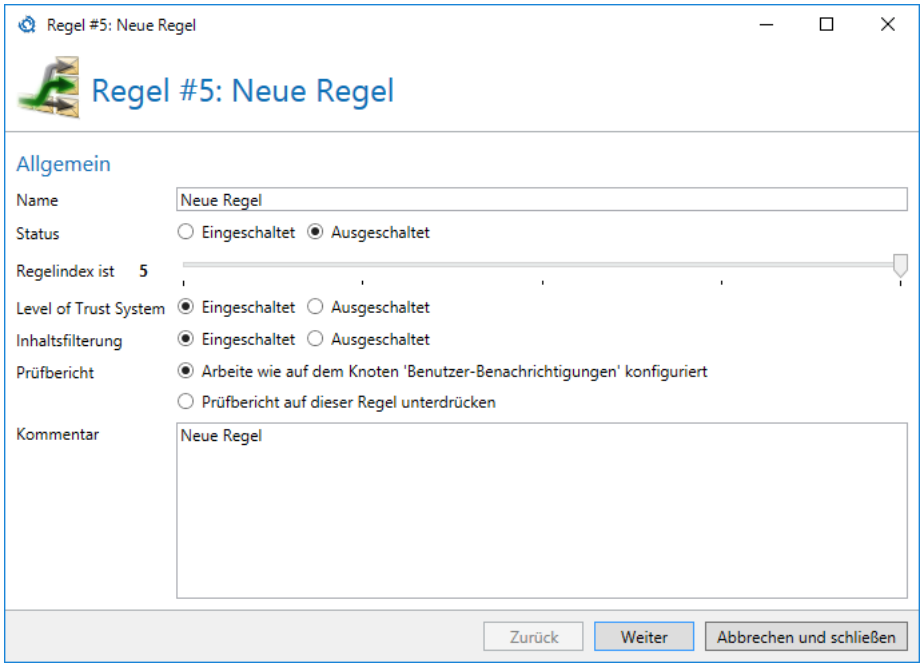


Bild 145: Über den Schieberegler für den "Regelindex" können Sie die Position der Regel verändern

Alternativ können Sie unter der Liste mit den Regeln auf **Regel Reihenfolge ändern** klicken (Bild 146).

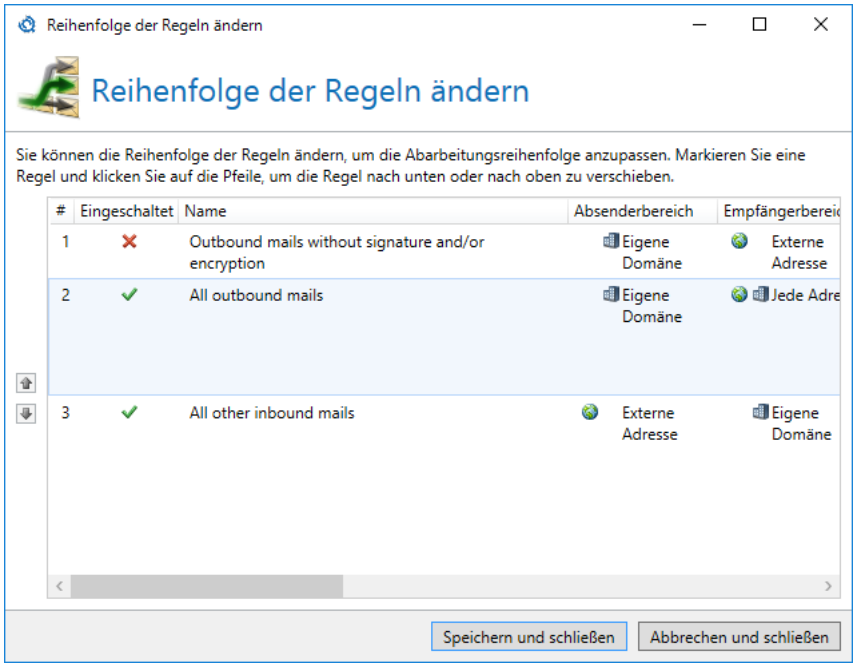


Bild 146: Hier kann die Reihenfolge aller Regeln zugleich verändert werden

Aktionen in NoSpamProxy

Aktionen können E-Mails verändern

Aktionen können E-Mails verändern; zum Beispiel die Adresse in der E-Mail verändern.

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 147).

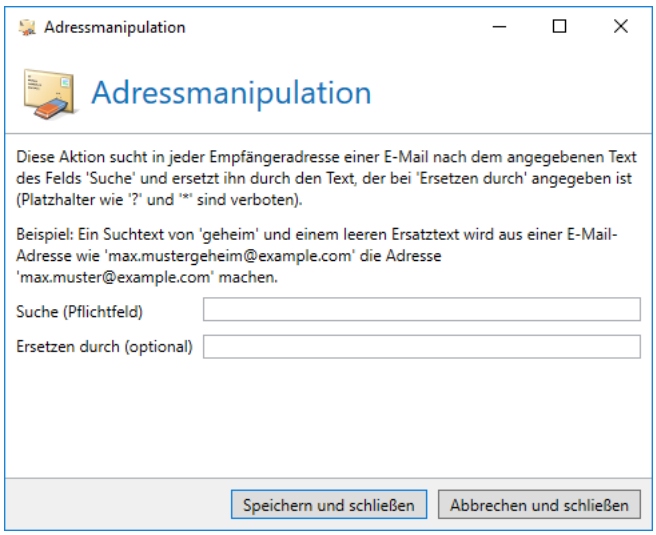


Bild 147: Konfigurieren Sie Ersetzungen auf den Empfängeradressen der E-Mails

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.

Anhänge mit einem Passwort schützen

Gültig für folgende Absender: **Lokal**.

Diese Aktion ermöglicht es, PDF-Anhänge mit einem Passwort zu schützen und den Zugriff auf die Dokumentinhalte einzuschränken.

NoSpamProxy Encryption unterstützt mit dieser Aktion den Passwortschutz von PDF-Dokumenten. Das heißt, dass an E-Mails angehängte PDF-Dokumente mit einem Passwort geschützt werden können, ohne dass der Empfänger der Dokumente bestimmte Voraussetzungen erfüllen muss. Dieses Kennwort kann optional automatisch an ein Mobiltelefon gesandt werden, wenn ein SMS-Anbieter unter dem Knoten SMS-Anbieter konfiguriert wurde.

Fügen Sie die Aktion **Anhänge mit einem Passwort schützen** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration.

Verschlüsselungsanforderungen

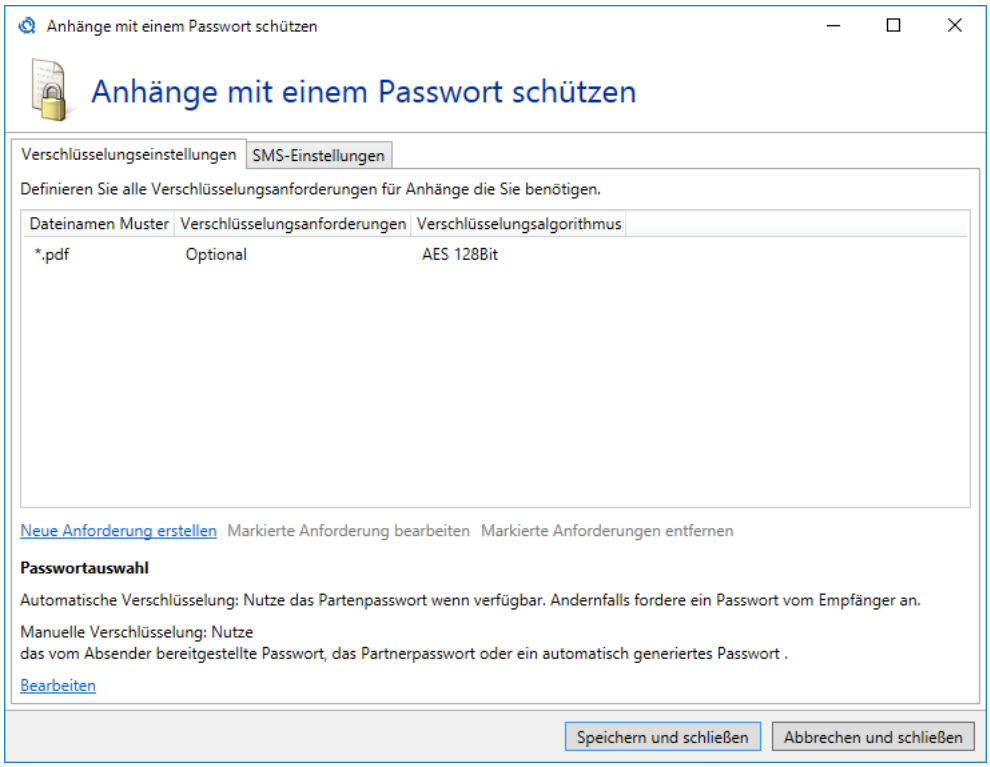


Bild 148: Die Einstellungen für die Verschlüsselung von PDF-Dokumenten

Zuerst müssen Sie im Schritt Verschlüsselungseinstellungen definieren, für welche PDF-Anhänge der Passwortschutz angewendet werden soll. Öffnen Sie mit dem Link **Neue Anforderung erstellen** den Dialog **Verschlüsselungsanforderungen für E-Mail-Anhänge**.

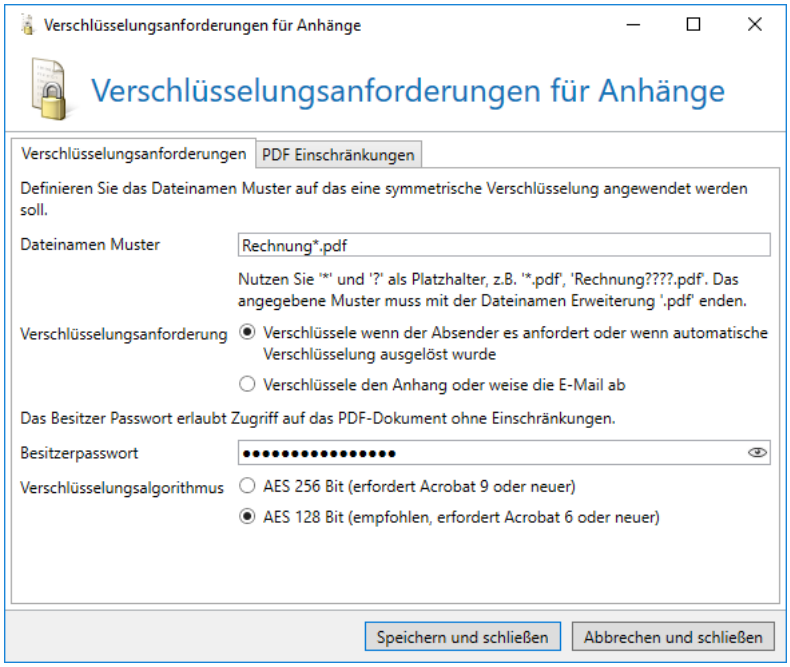


Bild 149: Definieren Sie, welche Dokumente auf welche Weise verschlüsselt werden

Tragen Sie im ersten Schritt des Assistenten Verschlüsselungsanforderungen das **Dateinamenmuster** für die zu verschlüsselnden PDF-Dateien ein. Sie können hier Platzhalter ('*' und '?') benutzen. Geben Sie nun an, ob alle PDF-Anhänge, die dem angegebenen Dateinamenmuster entsprechen, verschlüsselt werden müssen oder ob sie unverschlüsselt versendet werden sollen, wenn es weder vom Benutzer noch durch die Regel gefordert ist.

Ein Besitzerpasswort dient dazu, eventuelle PDF-Zugriffseinschränkungen zu verwenden. Um die Sicherheit eines PDF Dokumentes zu gewährleisten ist dieses Kennwort notwendig. Durch Kenntnis dieses Besitzerpassworts kann ein Leser die PDF-Zugriffseinschränkung abschalten. Geben Sie jetzt den Verschlüsselungsalgorithmus an. Hier wird AES mit 128 Bit für die optimale Balance aus Sicherheit und Kompatibilität empfohlen.

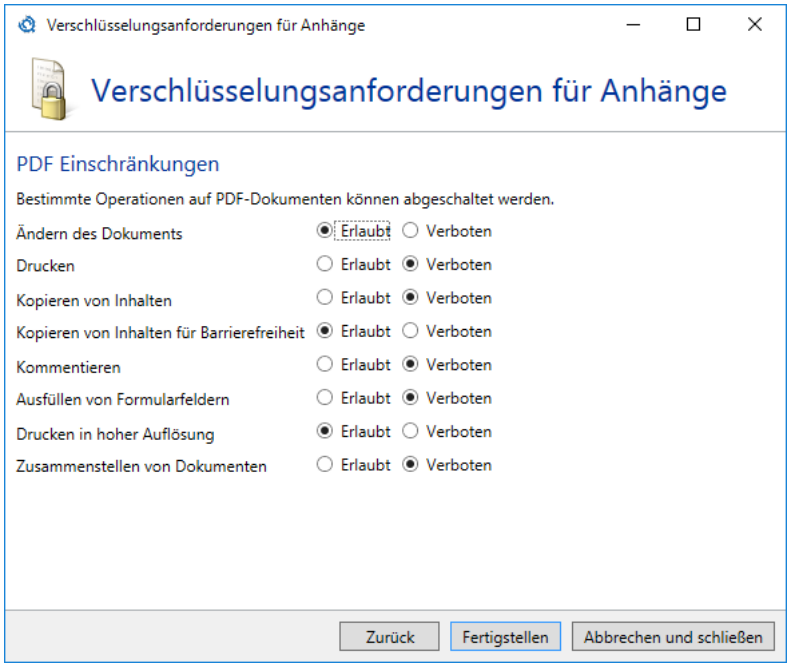


Bild 150: PDF-Einschränkungen

Im Schritt PDF-Einschränkungen können Sie unterschiedliche Operationen auf dem geschützten PDF-Dokument erlauben oder verbieten. Hier gewählte Einschränkungen können durch das im ersten Schritt angegebene **Besitzerpasswort** aufgehoben werden. Schließen Sie diesen Dialog im Anschluss mit **Fertigstellen**.

Passwortauswahl

In der unteren Hälfte der Seite **Verschlüsselungseinstellungen** definieren Sie, aus welchen Quellen die Passwörter bei der **automatischen Verschlüsselung** (Bild 151) sowie bei der **manuellen Verschlüsselung** (Bild 152) genommen werden.

Bild 151: Die Passwortquelle bei der automatischen Verschlüsselung

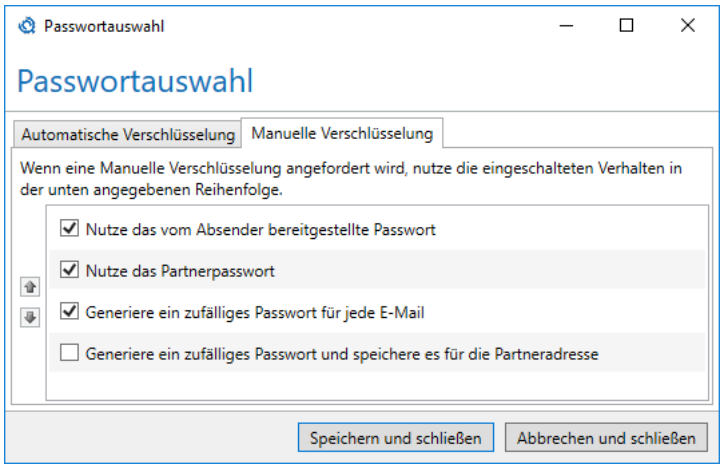


Bild 152: Reihenfolge der Passwortquellen bei der manuellen Verschlüsselung

Falls Sie bei der manuellen Verschlüsselung mehrere Quellen hinzufügen, werden diese von oben nach unten abgearbeitet. Die erste Quelle, die ein Passwort zurückliefert, wird verwendet. Sie müssen mindestens eine Passwortquelle hinzufügen um fortzufahren.

Im Schritt SMS Einstellungen können Sie definieren, ob und wie eine SMS mit dem Passwort versandt wird. Wählen Sie **Sende eine SMS um den Empfänger automatisch zu benachrichtigen**, wenn Sie einen SMS-Anbieter im Knoten **SMS-Anbieter** der Gateway Rolle konfiguriert haben. Wählen Sie nun den Namen in der Liste **SMS Provider Profil** aus. Als nächsten Schritt müssen Sie eine Textvorlage für die SMS definieren. Wählen Sie hier den Link **Standardvorlage einfügen**. Sie können nun den Text ggf. anpassen oder diese Text Vorlage direkt benutzen. Beachten Sie, dass die maximale Länge der Textvorlage auf 120 Zeichen beschränkt ist.

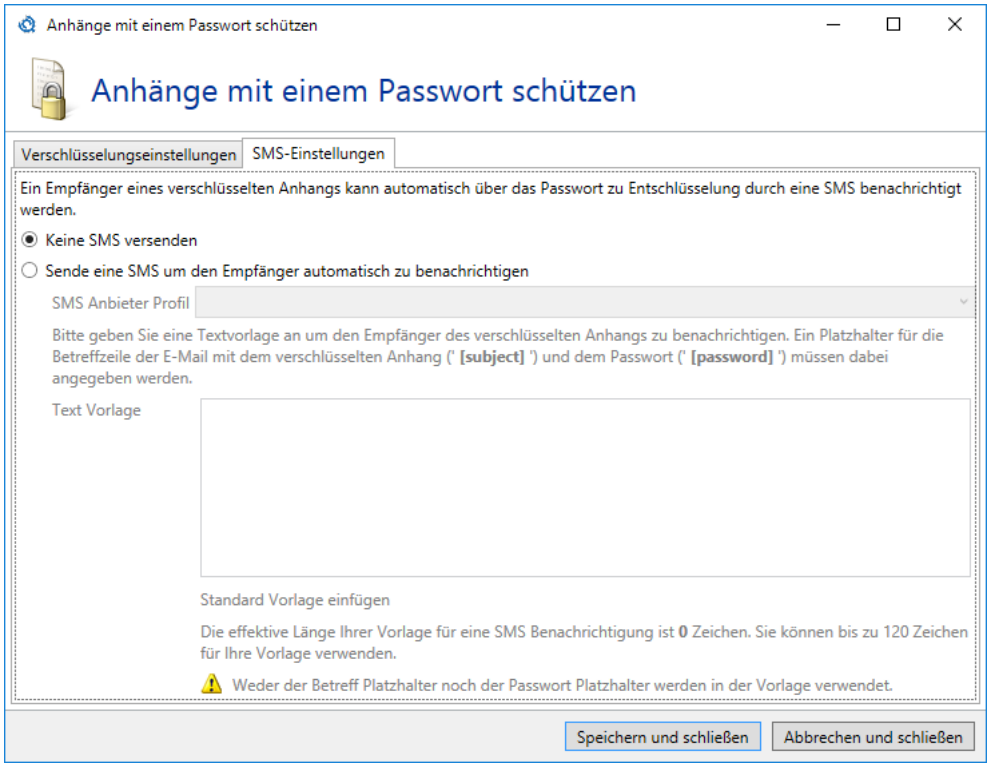


Bild 153: Definieren Sie, ob und wie eine SMS versandt werden soll

Steuerung der PDF-Verschlüsselung

Die Verschlüsselung kann über unterschiedliche Mechanismen gesteuert werden. Für die manuelle Eingabe von Passwort und Telefonnummer können bestimmte Kennzeichnungen in der Betreffzeile genutzt werden. Für die maschinelle Eingabe sind statt dieser Betreffkennzeichnungen, E-Mail-Header vorgesehen. Diese E-Mail-Header können über das Outlook Add-In von NoSpamProxy direkt beim Versenden der E-Mail auf dem Computer des Absenders gesetzt werden.

Lesen Sie im Kapitel über die Konfiguration der Betreffkennzeichnungen wie die Schlüsselworte für die PDF-Verschlüsselung in der Betreffzeilen genutzt werden. Im Handbuch **Outlook Add-In von NoSpamProxy** wird die Benutzung des Add-Ins für Outlook 2007 oder Outlook 2010 erklärt.

Qualifizierte Dokumentensignatur mit dem digiSeal server

Die Aktionen der qualifizierten Dokumentensignatur werden benutzt, um zum Beispiel Rechnungen zu signieren oder den Empfang von signierten Dokumenten zu überprüfen. NoSpamProxy Encryption bietet diese Funktion im Verbund mit dem digiSeal server der secrypt GmbH an. Das heißt, dass für diese Funktion, außer NoSpamProxy Encryption auch ein digiSeal server in Ihrer Infrastruktur zur Verfügung stehen muss.

Die qualifizierte Dokumentensignatur kann nur durchgeführt werden, wenn NoSpamProxy Encryption Zugriff auf einen für diese Arbeit konfigurierten digiSeal server hat.

Zur Installation eines digiSeal servers kontaktieren Sie uns bitte unter info@netatwork.de.

Die Verbindung zum digiSeal server richten Sie unter dem Knoten Erweiterte Einstellungen ein. Zusätzlich müssen die Dateien der digiSeal server API im Verzeichnis der Gateway Rolle liegen.

digiSeal server: Signiere Anhänge an E-Mails

Gültig für folgende Absender: **Lokal**.

Diese Aktion signiert Dokumente in Dateianhängen, die bestimmten Namensmustern entsprechen. Der Signaturprozess kann mit unterschiedlichen Signaturformaten arbeiten und auch einen optionalen Zeitstempel hinzufügen.

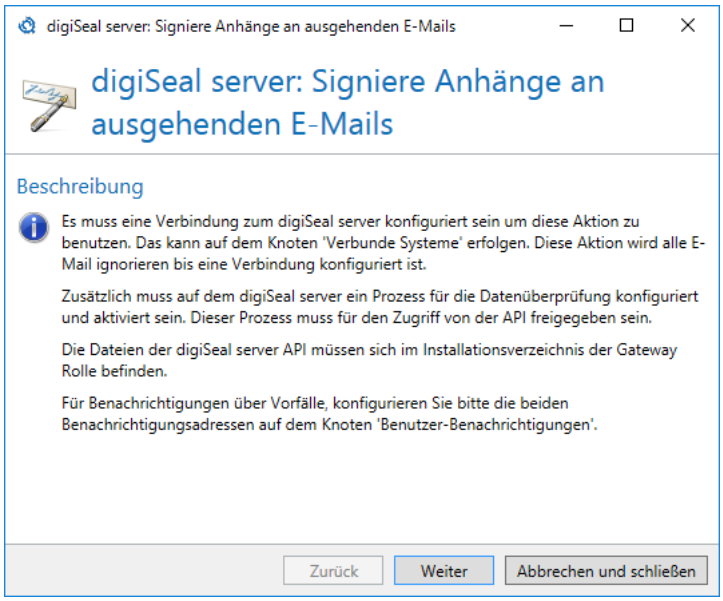


Bild 154: Für die qualifizierte Signatur mit dem digiSeal server muss die API installiert und freigeschaltet sein

Nachdem sichergestellt wurde, dass die Verbindung zum digiSeal server konfiguriert wurde, ein Prozess für die Datenüberprüfung auf dem digiSeal server definiert und aktiviert wurde, sowie die digiSeal server API Dateien in das Verzeichnis der Gateway Rolle gelegt wurden, kann die Qualifizierte Signatur Aktion konfiguriert werden (Bild 154).

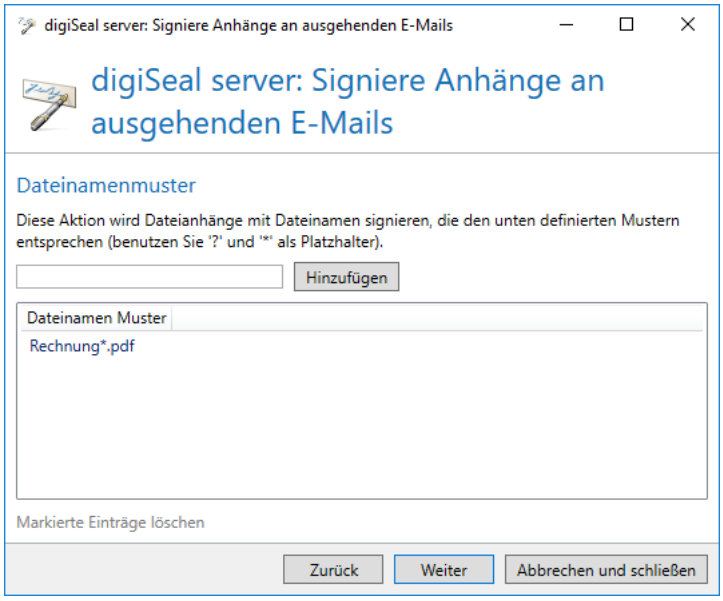


Bild 155: Definieren Sie die Dateinamenmuster, für die die qualifizierte Signatur durchgeführt werden soll

Die Aktion wird Dateien mit bestimmten Namensmustern signieren. Sie können hier die vollständigen Dateinamen von zu signierenden Dokumenten oder auch Teile davon hinterlegen (Bild 155)

Ein Beispiel: Sie möchten Rechnungen mit Dateinamen (zum Beispiel "Rechnung Mai 2017.pdf" oder "Rechnung März 2004.pdf") signieren. Hier können Sie einen Filter "Rechnung*.pdf" hinzufügen.
Die Aktion würde jetzt alle Dateien signieren, die diesem Muster entsprechen, auch zum Beispiel "RechnungAnMaxMustermannIstStorniert.pdf".

Sie können einen oder mehrere dieser Muster hinterlegen, damit Sie verschiedene Arten von Dateien mit derselben Aktion signieren können.

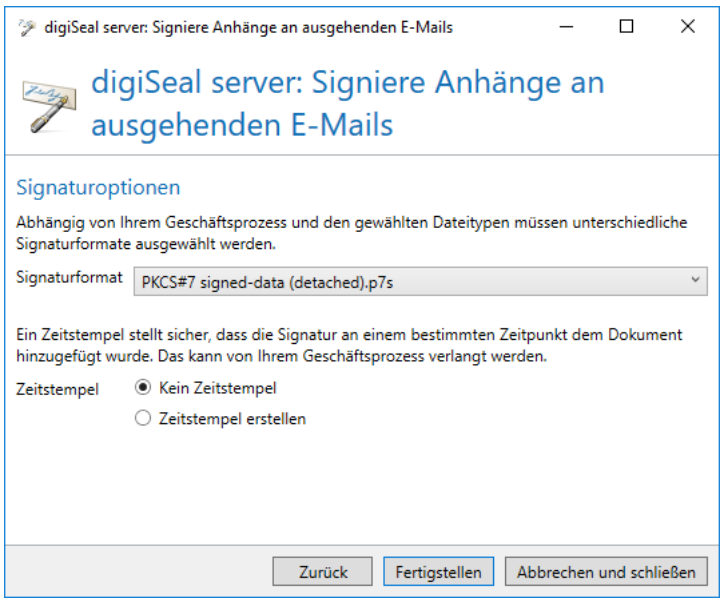


Bild 156: Geben Sie das Signaturformat an

In Abhängigkeit des Geschäftsprozesses und der zu signierenden Daten müssen Sie nun ein Signaturformat auswählen (Bild 156). Dabei stehen Ihnen folgende Signaturformate zur Verfügung:

- PKCS #7 verkapselte Signatur
- PKCS #7 alleinstehende Signatur
- PKCS #7 S/MIME Multipart Signatur
- XML alleinstehende Signatur
- XML eingebettete Signatur
- XML alleinstehende Signatur die den XADES Standard benutzt
- XML eingebettete Signatur die den XADES Standard benutzt
- EDIFACT Signatur
- Adobe PDF Referenz Version 1.6 PKCS #7 signierte Daten Signatur

Zusätzlich zum Signaturformat können Sie auch einen optionalen Zeitstempel hinzufügen. Dieser entspricht dem Zeitpunkt, an dem das Dokument signiert wurde.

Stellen Sie sicher, dass die Einstellungen dieser Aktion den Anforderungen Ihres Geschäftsprozesses für die qualifizierte Signatur genügen.

digiSeal server: Überprüfen und Erzwingen von signierten Anhängen auf E-Mails

Gültig für folgende Absender: **Extern**.

Diese Aktion überprüft die Anhänge von E-Mails an lokale Adressen und stellt das Vorhandensein von Signaturen sicher. Für jeden Dateityp können Sie festlegen, ob eine qualifizierte oder eine fortgeschrittene Signatur notwendig ist. Die Anforderungen hängen von dem jeweiligen Geschäftsprozess und ggf. beteiligten Gesetzen ab.

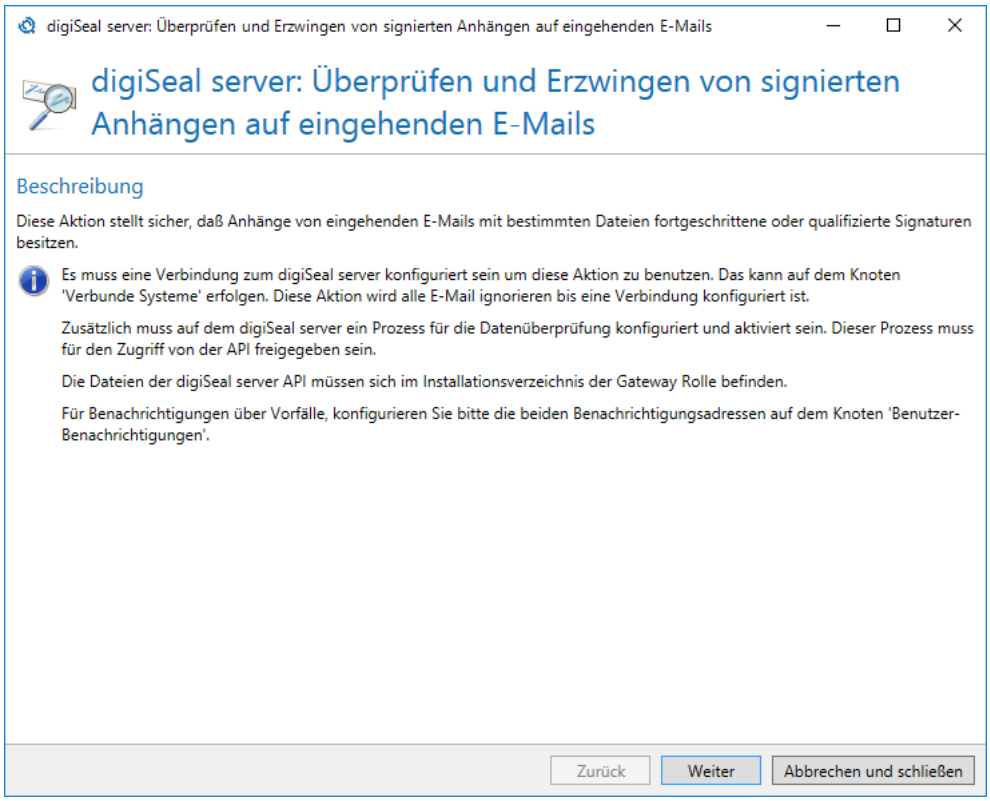


Bild 157: Um qualifizierte Signaturen zu überprüfen, muss die digiSeal server API installiert und freigeschaltet sein

Um diese Aktion erfolgreich einzusetzen, muss die Verbindung zum digiSeal server unter dem Knoten "Erweiterte Einstellungen" konfiguriert sein (Bild 157). Zusätzlich muss auf dem digiSeal server ein aktivierter Prozess für die Datenüberprüfung konfiguriert sein. Dieser Prozess muss für den Zugriff der API freigeschaltet sein. Die Dateien der digiSeal server API müssen sich im Verzeichnis der Gateway Rolle befinden.

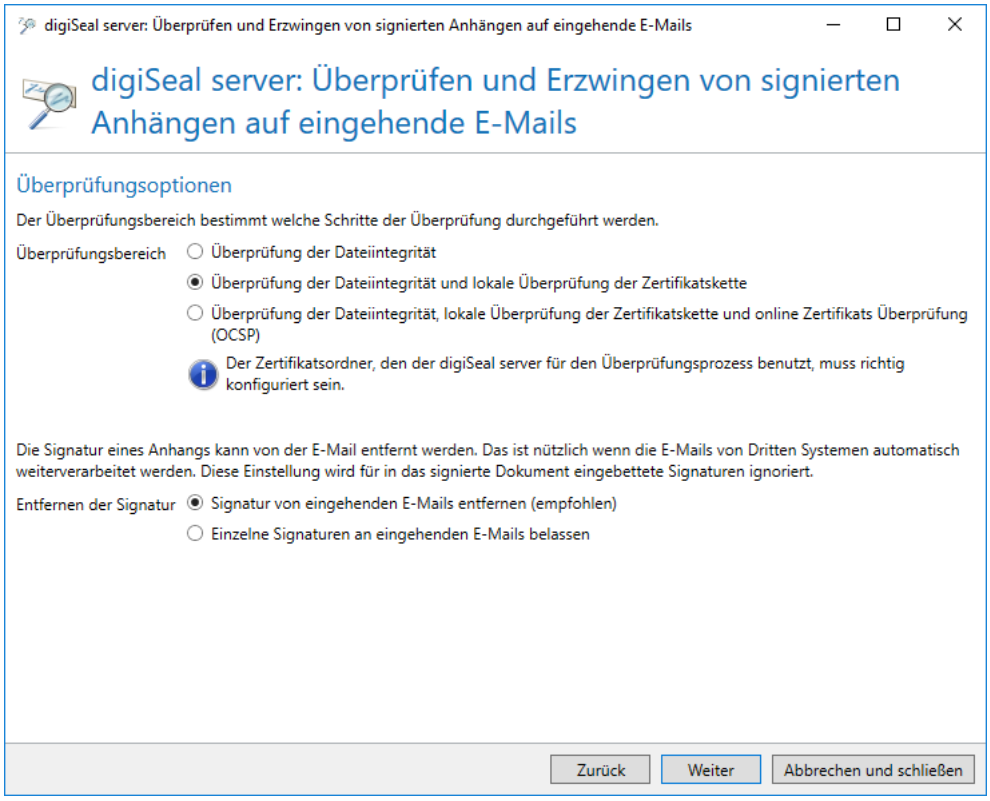


Bild 158: Um qualifizierte Signaturen zu überprüfen, muss die digiSeal server API installiert und freigeschaltet sein

Für die Überprüfung von Dokumenten stehen drei Stufen zur Verfügung (Bild 158). Die Option **Überprüfungsbereich** entspricht dabei dem Abschnitt **Prüftiefe** im digiSeal server, in der Karteikarte **2.5: Verifikation**

- Überprüfung der Dateiintegrität, d.h. ob die Datei seit der Signierung verändert wurde
- Lokale Überprüfung der Zertifikatskette
- Online Prüfung des verwendeten Zertifikates (durch das OCSP Protokoll)

Die zweite und dritte Stufe schließt jeweils die Prüfungen aus den vorhergehenden Stufen mit ein.

Signaturen, die an das signierte Dokument angehängt sind, können automatisch entfernt werden. Das Entfernen von Signaturen wird empfohlen, falls die E-Mails von weiteren Systemen automatisch verarbeitet werden sollen.

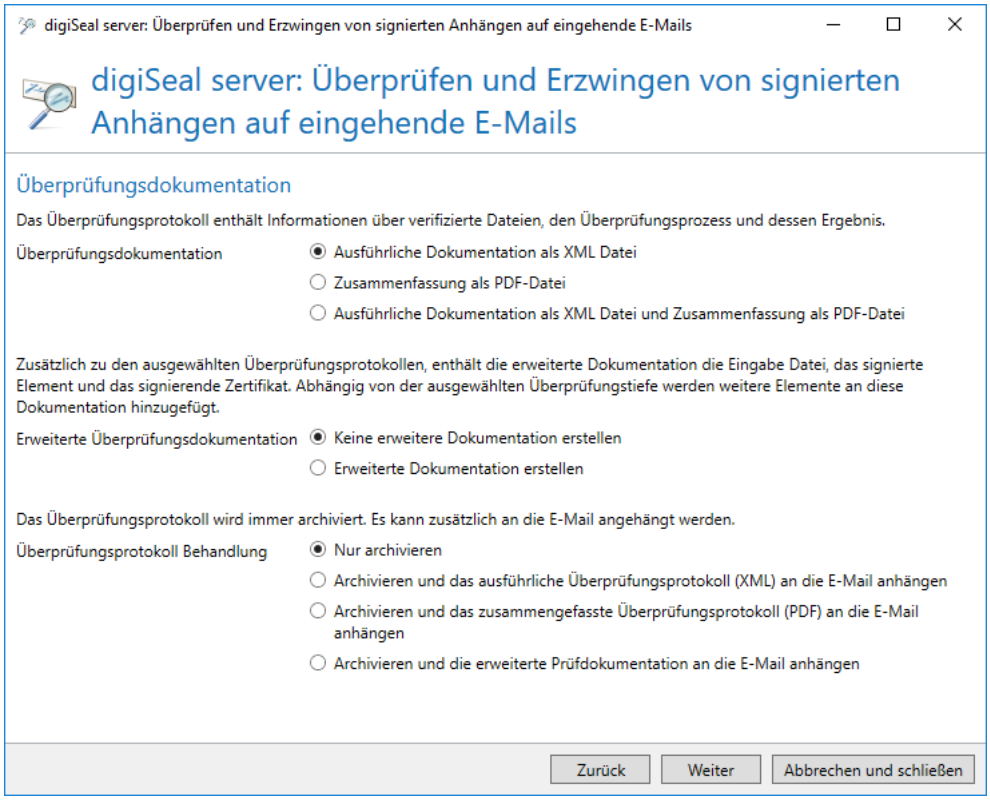


Bild 159: Sie können unterschiedliche Dokumentationen erstellen lassen und sie ggf. an die E-Mail anhängen

Die Optionen der Überprüfungsdokumentation bestehen aus drei Teilen: Den Einstellungen für das Überprüfungsprotokoll, der erweiterten Überprüfungsdokumentation und den Einstellungen für die Archivierung der erstellten Protokolle oder erweiterten Dokumentationen (Bild 159).

Das Überprüfungsprotokoll kann dabei aus einer ausführlichen XML Datei bestehen und / oder einer Zusammenfassung der Überprüfung als PDF-Dokument. Zusätzlich zu diesem Protokoll können weitere Details der Überprüfung in der erweiterten Überprüfungsdokumentation festgehalten werden. Sie können zusätzlich zur Archivierung des Überprüfungsprotokolls eventuell erstellte Protokolle oder Dokumentation an die E-Mail anhängen.

Für eine erfolgreiche Archivierung von E-Mails an lokale Adressen muss unter dem Knoten Archivschnittstelle ein passender Archivkonnektor definiert werden. Wenn kein Archivkonnektor definiert ist oder ein Archivkonnektor definiert ist, dessen Zuordnung von E-Mail-Adressen zu den Profilen nicht auf die E-Mail zutrifft, wird sie normal verarbeitet ohne archiviert zu werden.

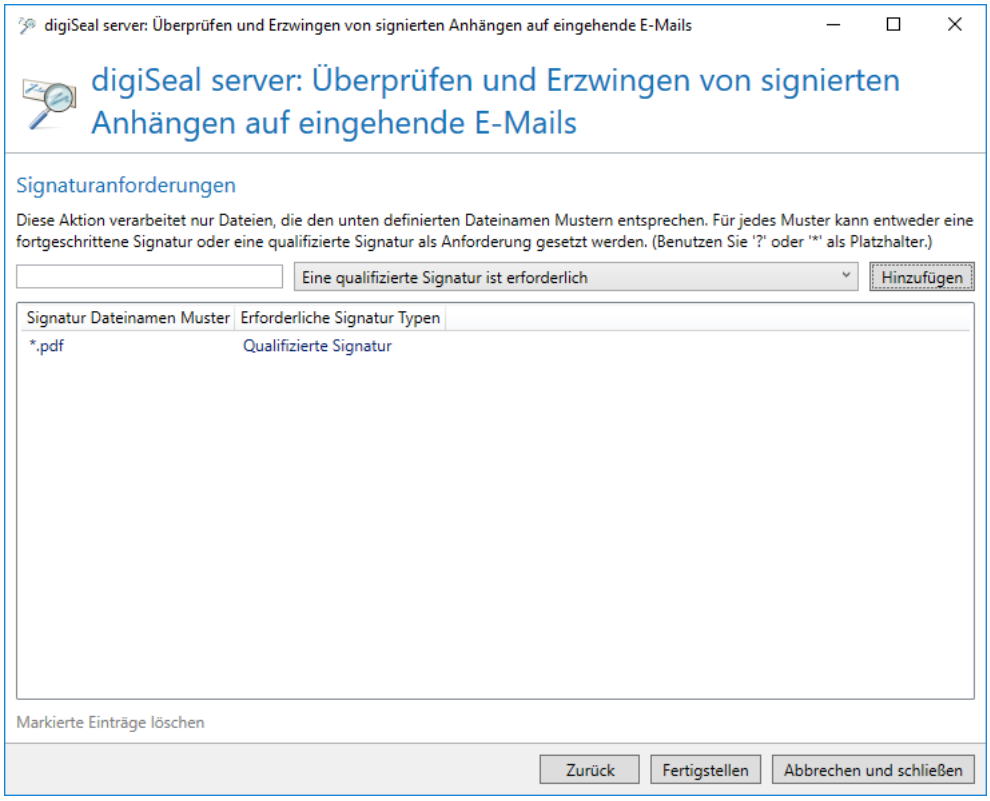


Bild 160: Legen Sie das Dateinamen Muster fest, für das qualifizierte Signaturen verifiziert werden sollen

Anhängig vom Dateinamen können Sie für die Ihnen zugesandten, unterschiedlich signierten Dateien festlegen, welchem Signaturtyp die Signatur entsprechen muss (Bild 160).

- Dokumente mit dem Dateinamensmuster: "EnergieRechnung*.pdf" müssen eine qualifizierte Signatur besitzen.
- Dokumente mit dem Dateinamensmuster: "TransportRechnung*.pdf" müssen eine fortgeschrittene Signatur besitzen.

E-Mails in PDF-Dokumente konvertieren

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

NoSpamProxy Encryption kann den gesamten Inhalt einer E-Mail in ein PDF-Dokument konvertieren. Alle bereits vorhandenen E-Mail-Anhänge werden dabei in das PDF-Dokument eingebettet. Das neu erstellte PDF-Dokument wird dann anstatt des ursprünglichen Inhalts an die E-Mail angehängt.

Um die Aktion hinzuzufügen wählen Sie **E-Mail in ein PDF-Dokument konvertieren**. Der Konfigurationsdialog erscheint. (Bild 161).

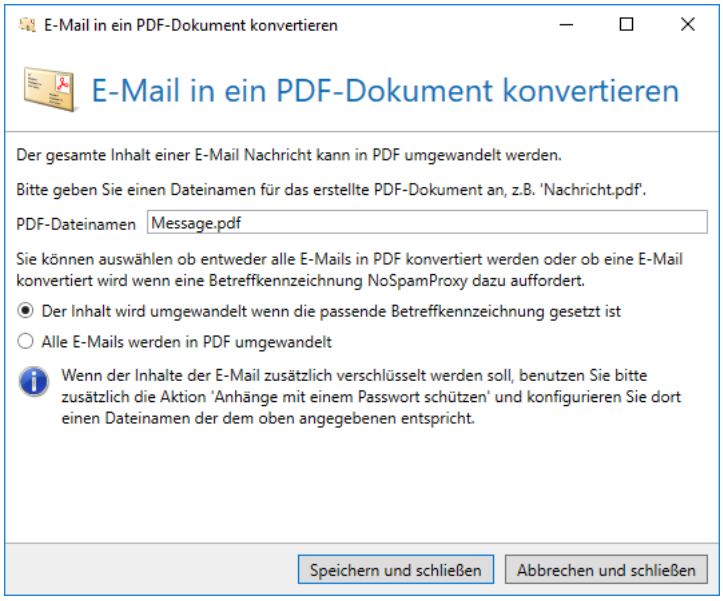


Bild 161: Die Optionen für die Konvertierung des E-Mail-Inhalts in ein PDF-Dokument.

Wählen Sie im Feld **PDF-Dateinamen** den Dateinamen des Anhangs aus, in den die zu versendende E-Mail mit allen zugehörigen Datei-Anhängen eingebettet werden soll. Durch die Auswahl von **Der Inhalt wird umgewandelt wenn die passende Betreffkennzeichnung gesetzt ist** wählen Sie, dass E-Mails nur umgewandelt werden wenn der Benutzer das über die Betreffkennzeichnung oder das Outlook Add-In bestimmt. Die Auswahl **Alle E-Mails werden in PDF umgewandelt** wandelt jede E-Mail in ein PDF-Dokument.

Durch gleichzeitigen Einsatz der Aktionen **E-Mail in ein PDF-Dokument konvertieren** und **Anhänge mit einem Passwort schützen** können Sie den Inhalt einer E-Mail gleichzeitig in ein PDF-Dokument umwandeln und mit einem Passwort schützen. Konfigurieren Sie dazu in der Aktion **E-Mail in ein PDF-Dokument konvertieren** einen Dateinamen der auch in der Aktion **Anhänge mit einem Passwort schützen** eingetragen wird. Dadurch wird die E-Mail in ein passwortgeschütztes PDF-Dokument konvertiert, das den konfigurierten Namen trägt. Bei unterschiedlichen Dateinamen in den beiden Aktionen werden die Anhänge ungeschützt übermittelt. Dies liegt daran, dass bei einem zu schützenden Dateinamen-Muster von zum Beispiel: "Rechnung.pdf" in der Passwort-Aktion, ein Anhang mit diesem Namen an einer E-Mail durch die Konvertierung in eine Datei mit dem Namen: "Nachricht.pdf" eingebettet wird. Dadurch befindet sich nicht mehr der eigentliche Anhang "Rechnung.pdf" an der E-Mail, sondern nur noch die Datei "Nachricht.pdf". Diese Datei ist aber nicht für den Schutz mit einem Passwort eingetragen.

Verschlüsselung

Mit diesen Aktionen können Sie E-Mails an externe Adressen signieren und verschlüsseln, sowie E-Mails an lokale Adressen überprüfen und entschlüsseln. Für die Verschlüsselung wird entweder S/MIME oder PGP eingesetzt.

Überprüfen der Signatur und/oder Entschlüsseln von E-Mails

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

Bei E-Mails an lokale Empfänger kann die digitale Signatur automatisch validiert und der Inhalt entschlüsselt werden. Sie können dabei die Optionen für Validierung wie auch Entschlüsselung individuell einstellen.

Überprüfungsrichtlinien

Folgende Validierungsrichtlinien für die Signatur sind möglich (Bild 162):

Für mittels S/MIME signierter E-Mail können Sie verschiedene Stufen der Validierung auswählen, die jeweils aufeinander aufbauen. Im Falle von mittels PGP signierter E-Mails können Sie lediglich festlegen, ob die Nachrichtenintegrität überprüft wird.

Des Weiteren können Sie hier festlegen, ob alle E-Mails an lokale Adressen signiert sein müssen. Wenn Sie dies auswählen, können Sie noch zusätzlich die möglichen Signaturverfahren einschränken.

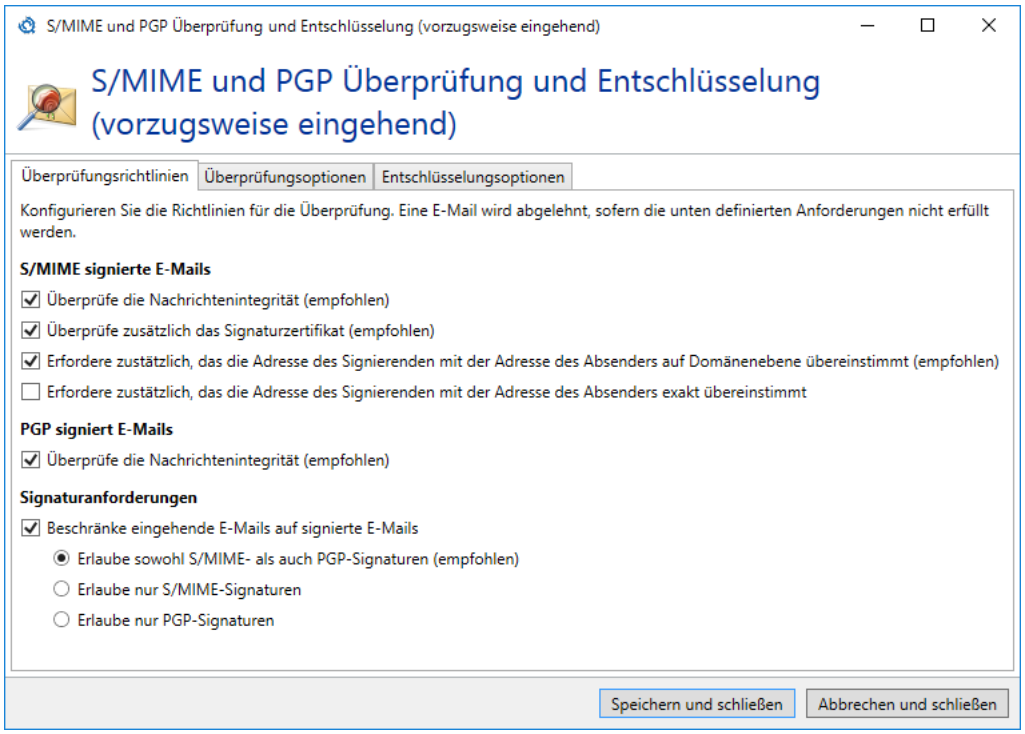


Bild 162: Die Validierungsrichtlinien der E-Mail-Signatur

Überprüfungsoptionen

Auf dieser Seite können Sie, jeweils für S/MIME und PGP, festlegen, ob Signaturschlüssel von der E-Mail entfernt werden. Dies ist sinnvoll, da ansonsten Benutzer diese Schlüssel verwenden können um Antworten schon auf dem Client zu verschlüsseln. Diese E-Mails können dann nicht mehr zuverlässig von NoSpamProxy überprüft werden.

Ebenfalls jeweils für S/MIME und PGP können Sie konfigurieren, ob angehängte Schlüssel automatisch in den Zertifikatsspeicher von NoSpamProxy importiert werden. PGP-Schlüssel werden dabei zunächst in Quarantäne genommen und müssen vom Administrator explizit freigegeben werden.

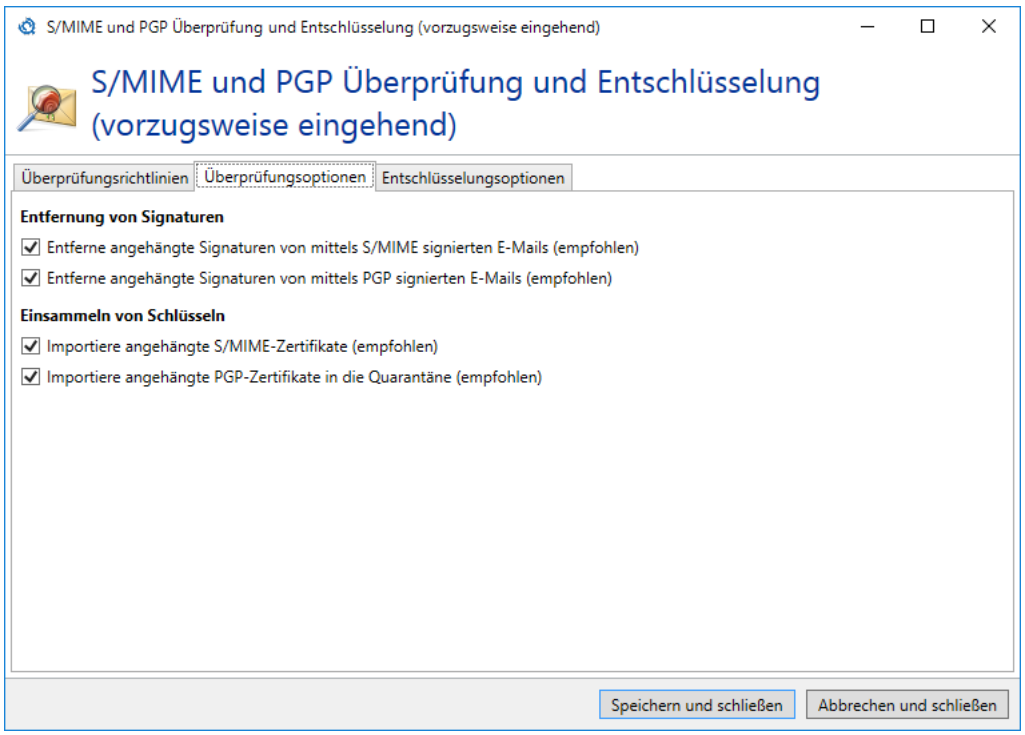


Bild 163: Die Validierungsoptionen der Signatur

Entschlüsselungsoptionen

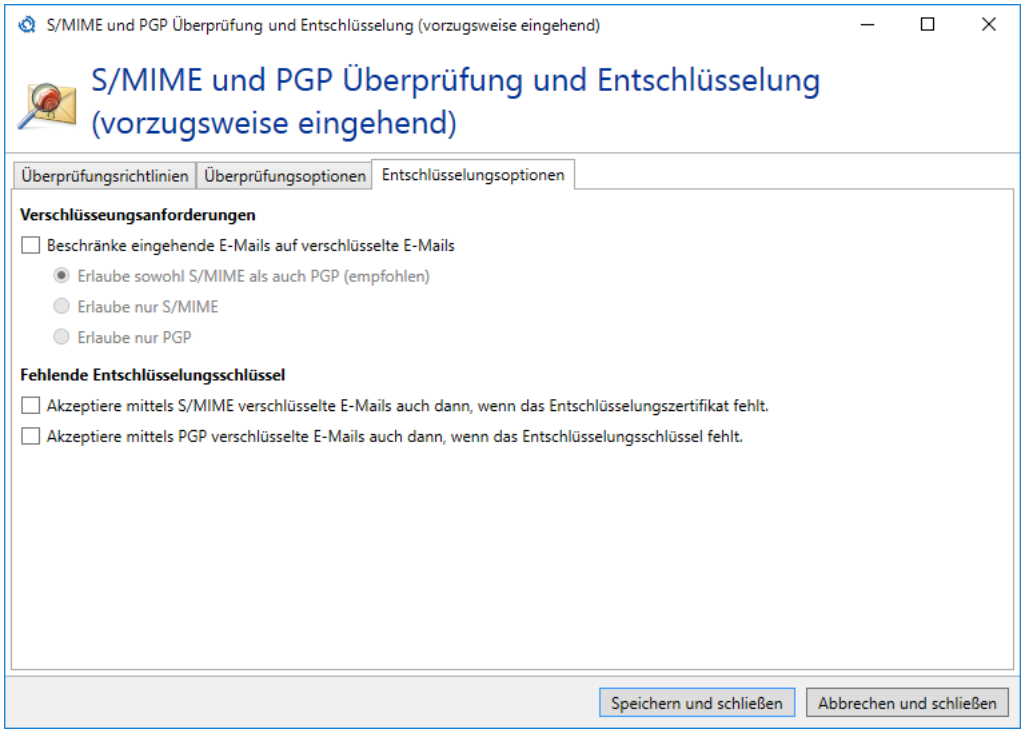


Bild 164: Sie können bei E-Mails an lokale Adressen Verschlüsselung verlangen und das Verhalten bei Entschlüsselungsfehlern hier festlegen

In der Registerkarte **Entschlüsselungsoptionen** (Bild 164) können Sie die Verschlüsselung von E-Mails erzwingen. Falls diese Option gewählt wird, werden alle unverschlüsselten E-Mails an lokale Adressen abgewiesen. Zusätzlich können die Sie möglichen Technologien einschränken.

Es kann vorkommen, dass E-Mails verschlüsselt empfangen werden, aber kein privates Zertifikat für die Entschlüsselung in der Zertifikatsverwaltung zur Verfügung steht. Diese E-Mails können abgewiesen werden oder zum Empfänger der E-Mail in ihrer verschlüsselten Form zugestellt werden. Da solche E-Mails nicht auf Spam oder Schadsoftware untersucht werden können, sollten sie abgewiesen werden.

Auch wenn Sie "Verschlüsselung erzwingen" ausgewählt haben, kann eine unverschlüsselte E-Mail erst abgewiesen werden, nachdem sie übertragen wurde.

Signieren und/oder Verschlüsseln von E-Mails

Gültig für folgende Absender: **Lokal**.

Diese Aktion kann E-Mails mit den unter der Zertifikats- oder PGP-Schlüsselverwaltung vorhandenen kryptographischen Schlüsseln signieren oder verschlüsseln (Bild 165).

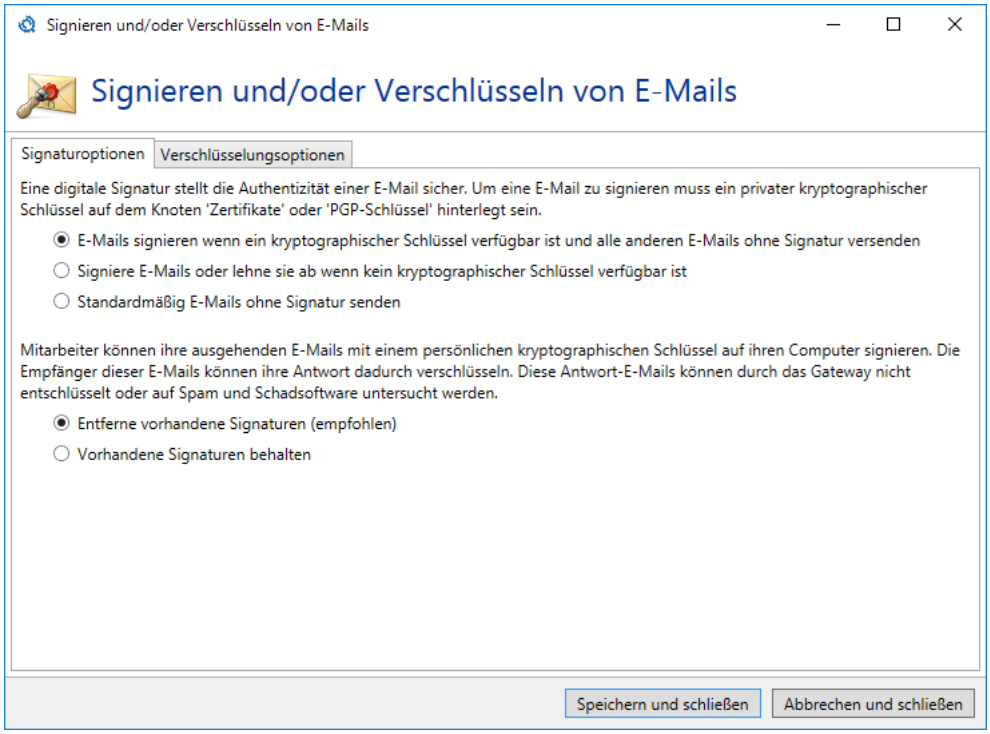


Bild 165: Die Signaturoptionen bei E-Mails an externe Adressen

Digitale Signatur

Legen Sie für die Signatur eines der folgenden Verhalten fest:

- E-Mail signieren, wenn ein kryptographischer Schlüssel für den Absender verfügbar ist und alle anderen E-Mails ohne Signatur versenden.
- E-Mail mit einem kryptographischen Schlüssel des Absenders signieren oder den Versand ablehnen, falls kein kryptographischer Schlüssel vorhanden ist.
- Alle E-Mails ohne Signatur versenden.

Vorhandene Signaturen

E-Mails von lokalen Absendern können bereits Signaturen enthalten. Diese Schlüssel stellen ein Sicherheitsrisiko dar, da eine Antwort auf eine solche E-Mail verschlüsselt werden kann. Dieser verschlüsselte Inhalt kann beim gleichzeitigen Einsatz von NoSpamProxy Protection nicht auf Spam und Malware analysiert werden, da der notwendige Schlüssel zum Entschlüsseln nicht auf dem Server liegt sondern nur dem Absender bekannt ist (Bild 166). Sie können bereits bestehende Signaturen von E-Mails entfernen lassen um das zuvor beschriebene Risiko zu minimieren.

E-Mail-Verschlüsselung

Hier können Sie einstellen, ob Sie E-Mail verschlüsseln möchten oder nicht. Außerdem können Sie festlegen, wie mit bereits verschlüsselten E-Mails umgegangen werden soll. Für den Fall, dass Sie die E-Mails auf gar keinen Fall unverschlüsselt senden möchten, können Sie noch eine Ausnahme für Besprechungsanfragen konfigurieren. Werden diese nämlich verschlüsselt, können diese von Outlook nicht mehr verarbeitet werden.

Da verschlüsselte E-Mails üblicherweise die Signatur des Absenders enthalten, tritt dadurch das gleiche Sicherheitsrisiko auf, wie bei in der E-Mail bereits vorhandenen Signaturen. Sie können aus den gleichen Gründen wie im Abschnitt "Vorhandene Signaturen" die Auslieferung von verschlüsselten E-Mails verhindern.

NoSpamProxy Encryption besitzt eine umfangreichere Unterstützung des S/MIME Standards als die meisten E-Mail-Programme. Sie können NoSpamProxy Encryption auch zum Verschlüsseln von E-Mails nutzen, ohne diese E-Mails zu signieren. Das bedeutet, dass der Inhalt mit Hilfe des Empfängerzertifikates verschlüsselt werden kann, ohne dass man ein eigenes Zertifikat besitzen muss. Wir empfehlen Ihnen allerdings ein Zertifikat einzusetzen, um dem Empfänger die Authentizität der E-Mail anzuzeigen.

Falls NoSpamProxy Encryption keinen Verschlüsselungsschlüssel für einen Empfänger besitzt, können die bereits konfigurierten öffentlichen Schlüsselserver befragt werden. Wird dort ein Schlüssel gefunden, dann wird er für die Verschlüsselung der E-Mail herangezogen.

Sie können hier auswählen, das auf allen konfigurierten Schlüsselservern gesucht wird. Nutzen Sie diese Einstellung bitte nicht auf der Standardregel für Nachrichten an externe Adressen. Dies würde die Leistung der Gateway Rolle massiv beeinträchtigen.

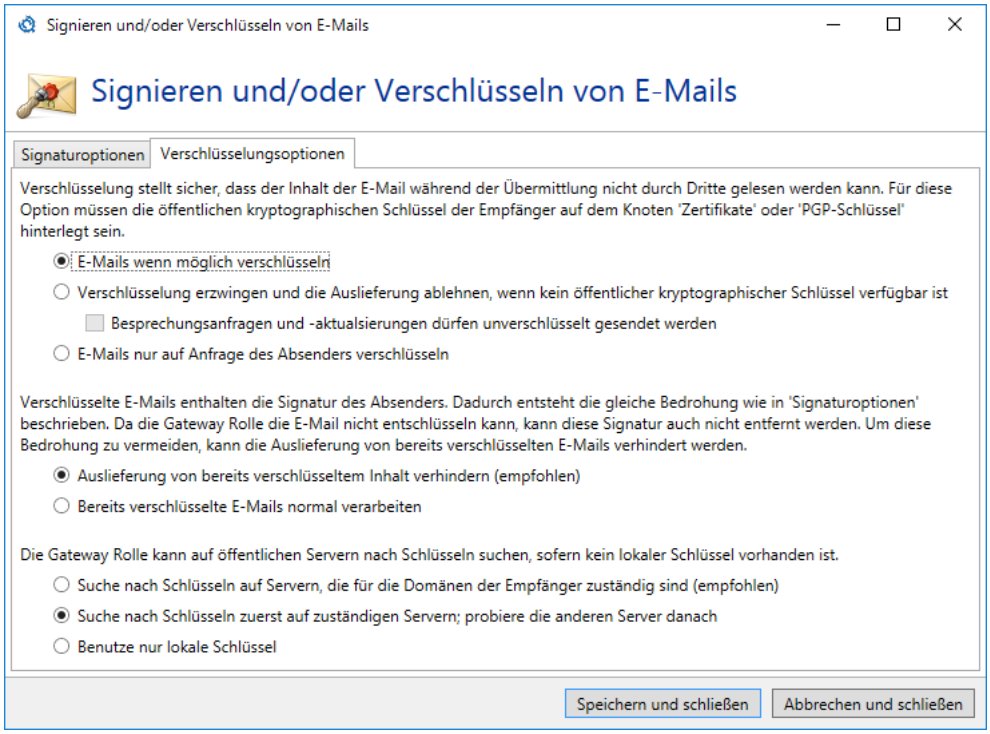


Bild 166: Die Verschlüsselungsoptionen bei E-Mails an externe Adressen

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 167). 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.

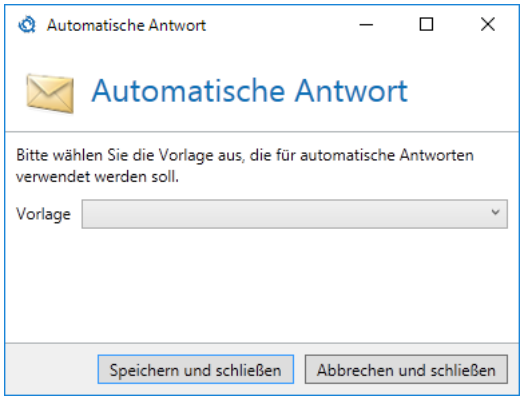


Bild 167: Automatische Antwort erstellen

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 168).

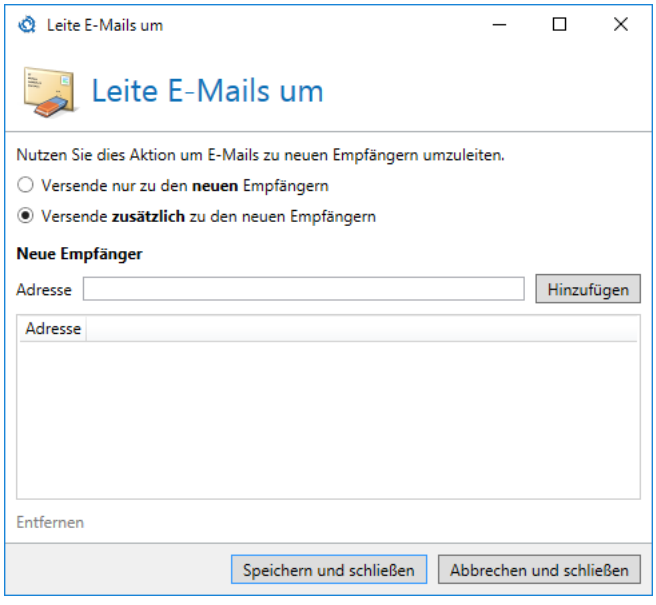


Bild 168: Konfiguration zur Umleitung von E-Mails

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.

Voreinstellungen

Dieser Bereich beinhaltet globale Einstellungen, die in anderen Bereichen der Konfiguration (zum Beispiel Regeln, Partner oder Unternehmensbenutzer) benutzt werden können (Bild 169).

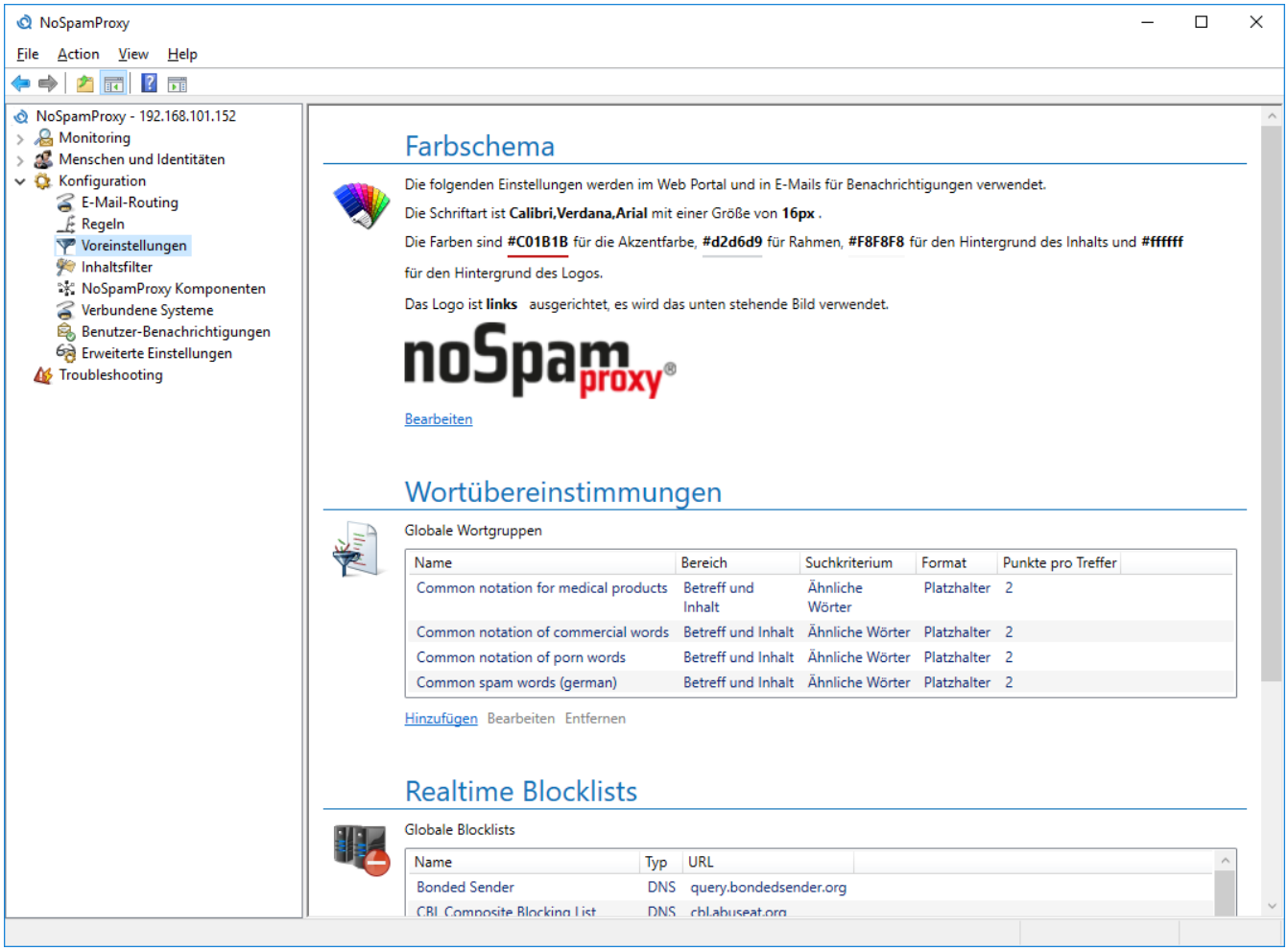


Bild 169: Voreinstellungen

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 170)

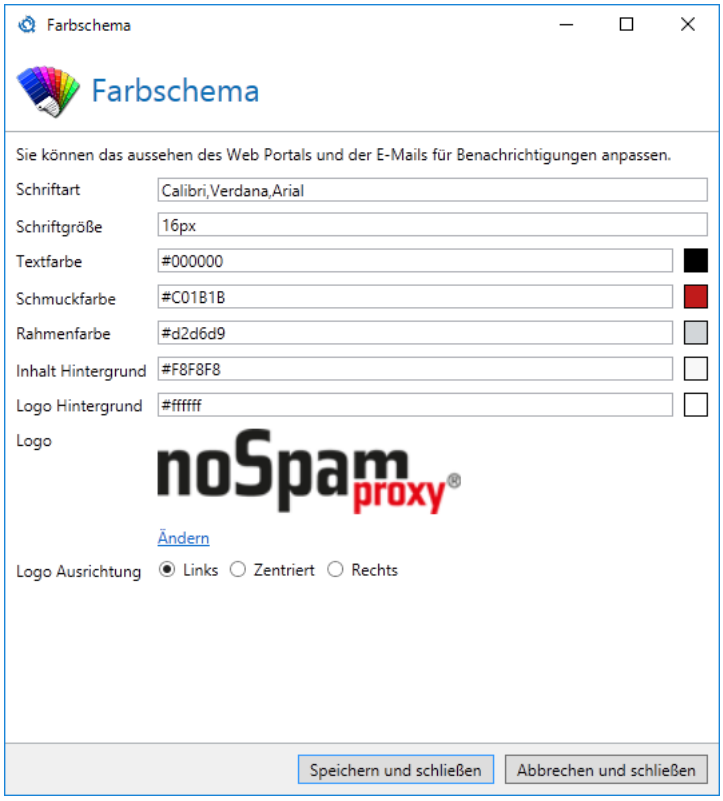


Bild 170: Dialog für das Ändern des Farbschemas.

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.

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 171). 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.

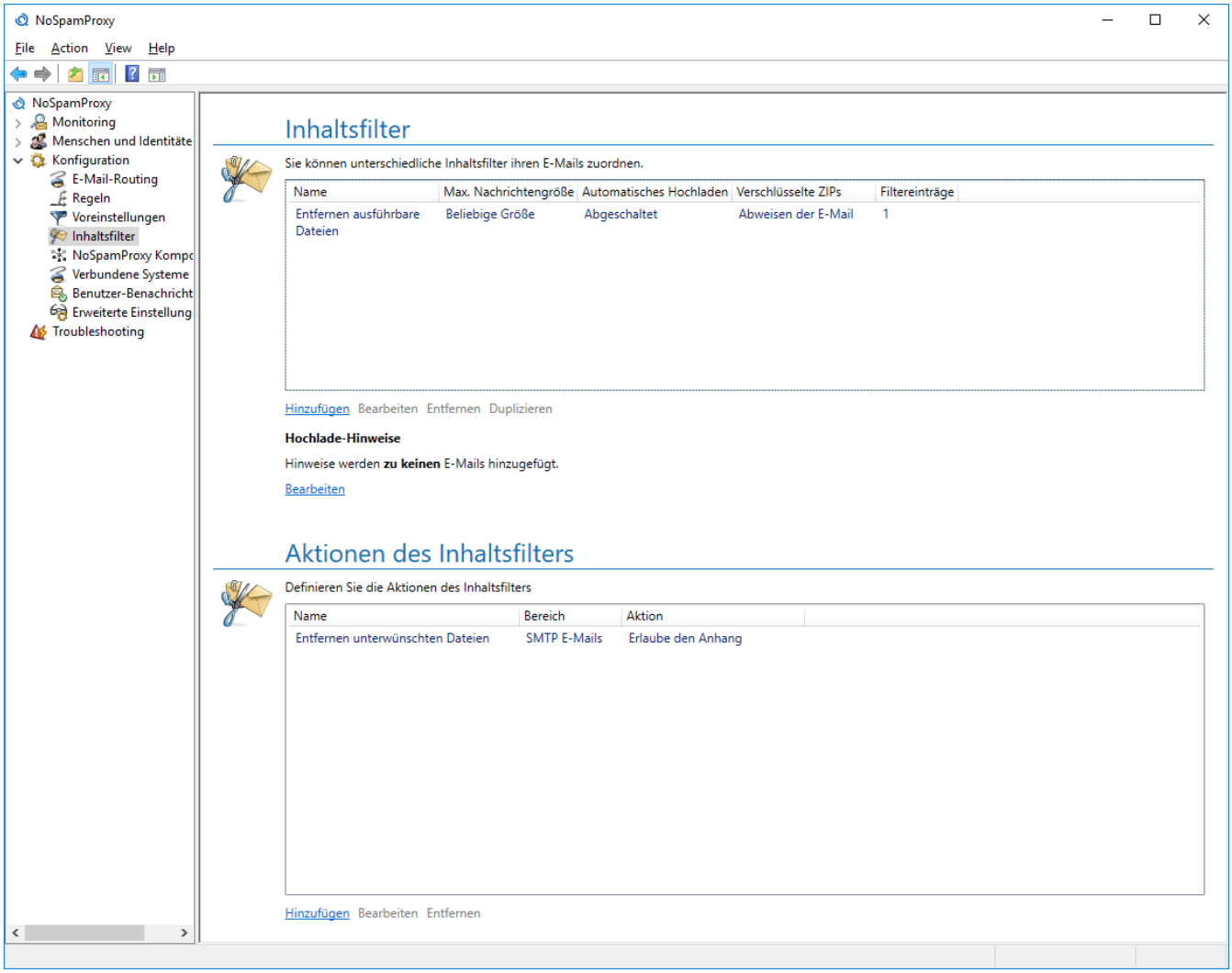


Bild 171: Die Übersicht der Inhaltsfilter

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 172).

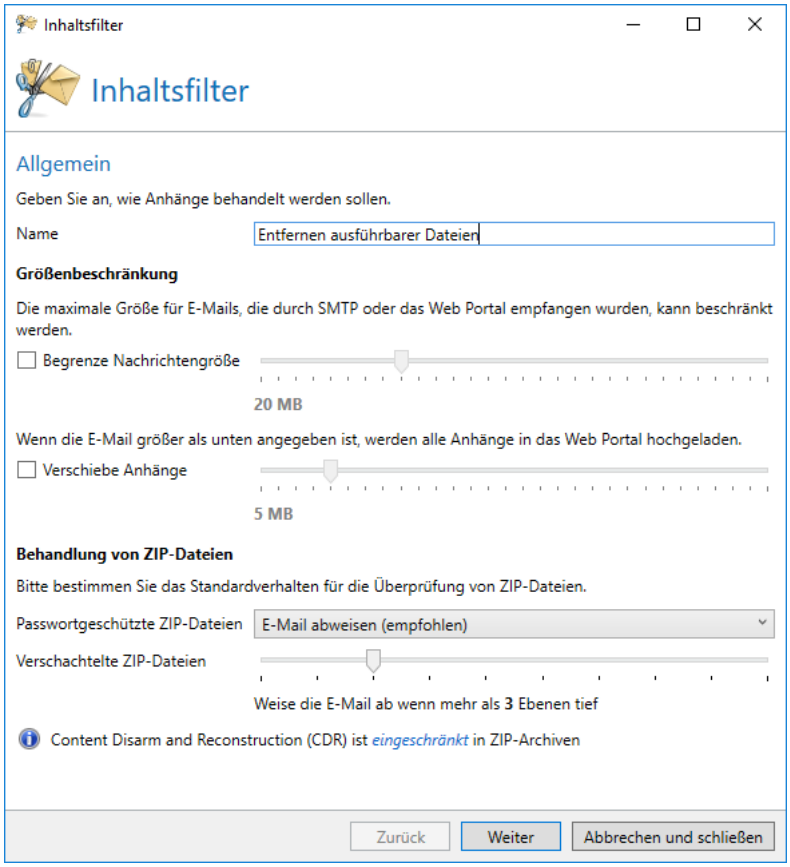


Bild 172: Allgemeine Einstellungen eines Inhaltsfilters

Ein Inhaltsfilter kann mehrere Einträge enthalten, um für einen Benutzer alle notwendigen Aktionen auf unterschiedlichen Dateianhängen konfigurieren zu können (Bild 173). 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.

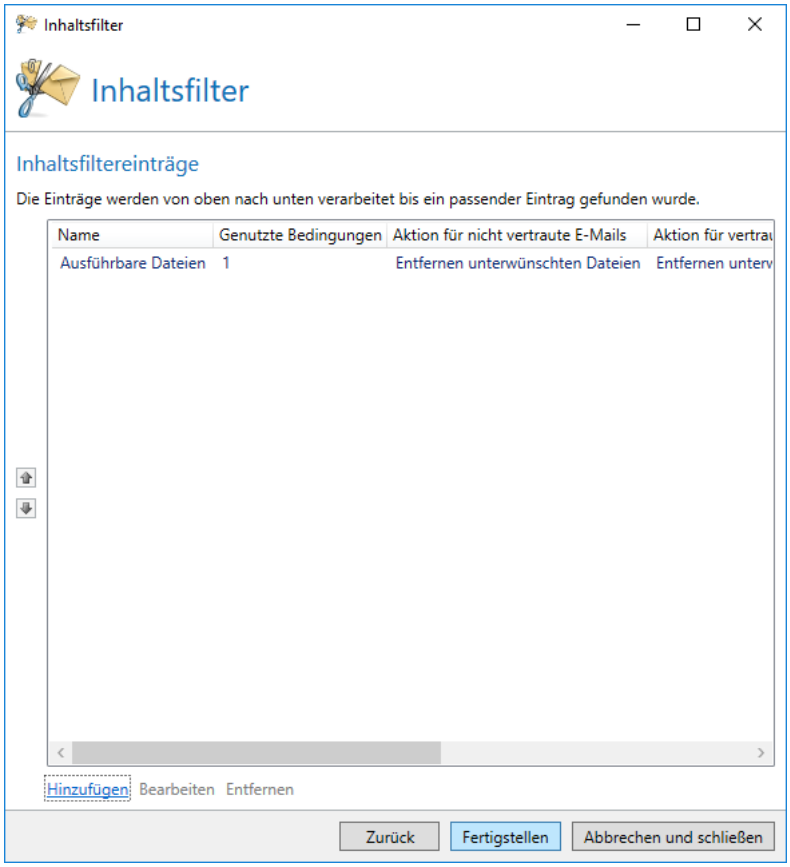


Bild 173: Die Liste der Inhaltsfiltereinträgen

Ein Eintrag eines Inhaltsfilters kann Bedingungen enthalten, nach denen Anhänge ausgewählt werden (Bild 174). Hier stehen Ihnen mehrere Auswahlkriterien zur Verfügung, die auch kombiniert werden können (Bild 175). 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.

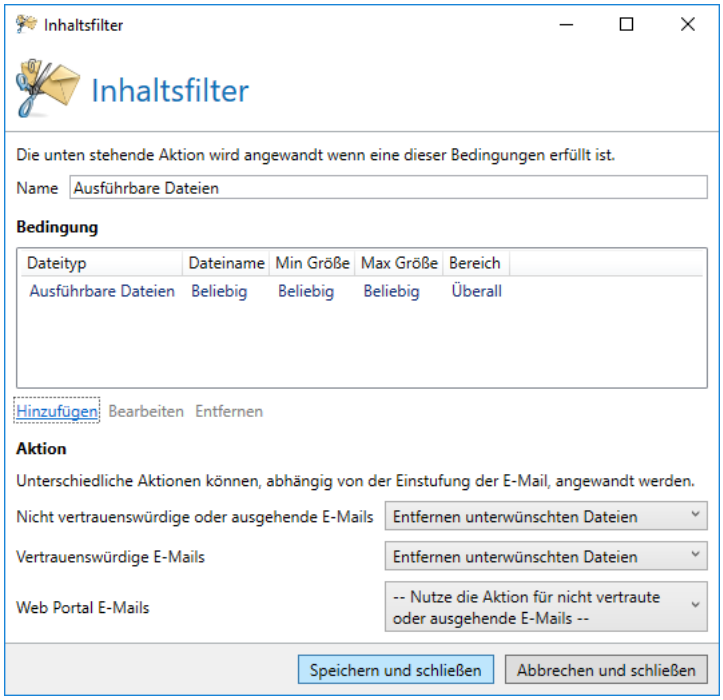


Bild 174: Ein Inhaltsfiltereintrag

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.

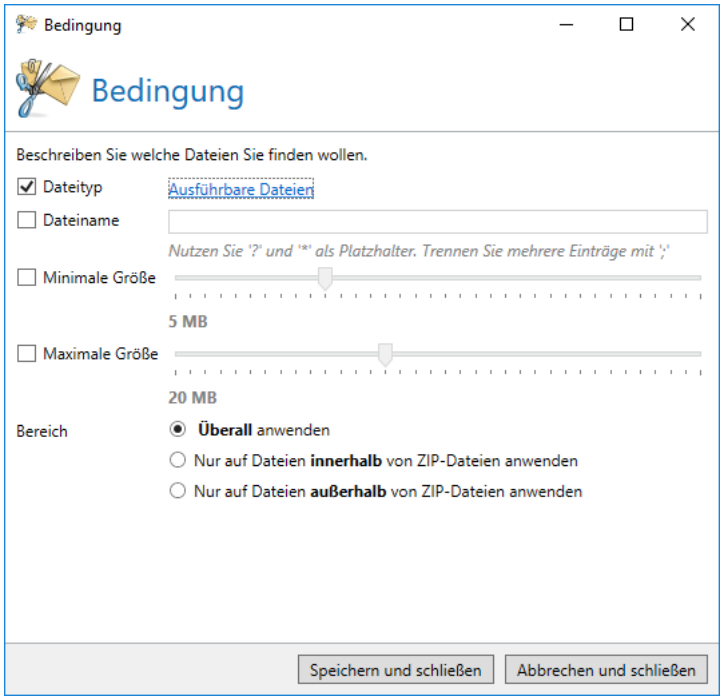


Bild 175: Eine Bedingung für die Auswahl von Anhängen

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 176).

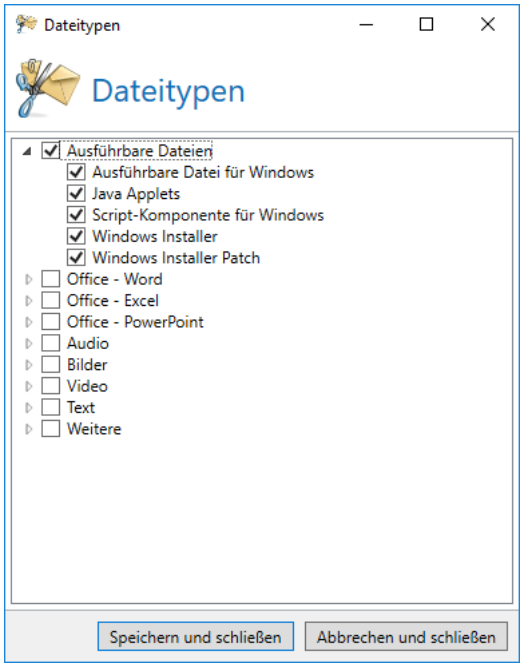


Bild 176: Der Dialog für die Auswahl von Dateitypen

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 177).

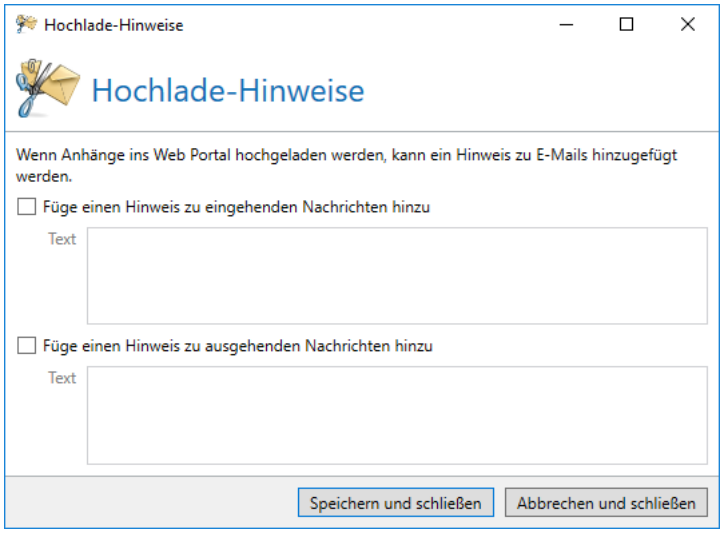


Bild 177: Der Text für Hinweise über hochgeladene Anhänge

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 178).

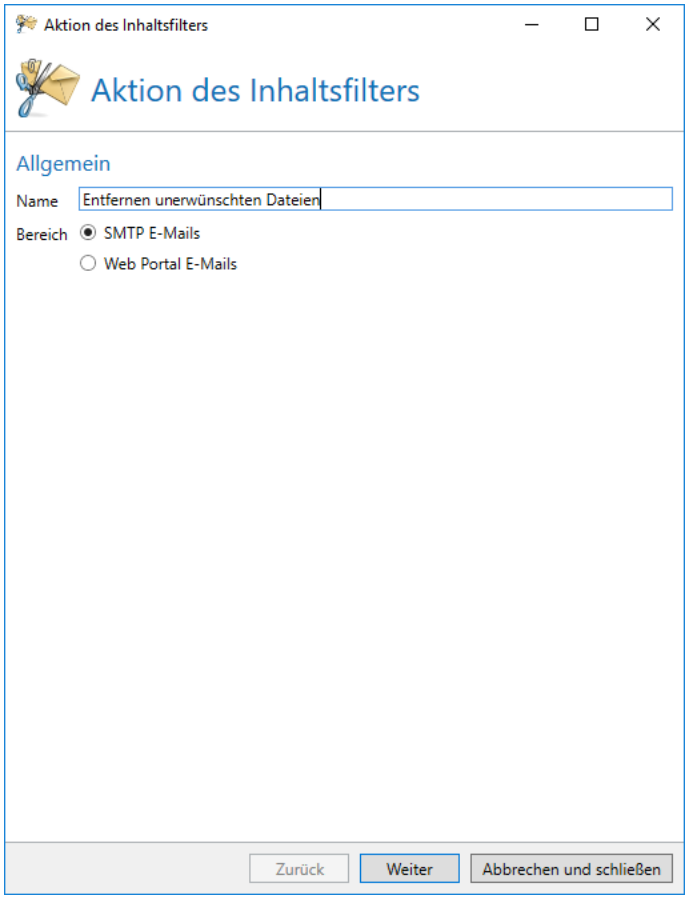


Bild 178: Der Typ der Aktion

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 179). 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.

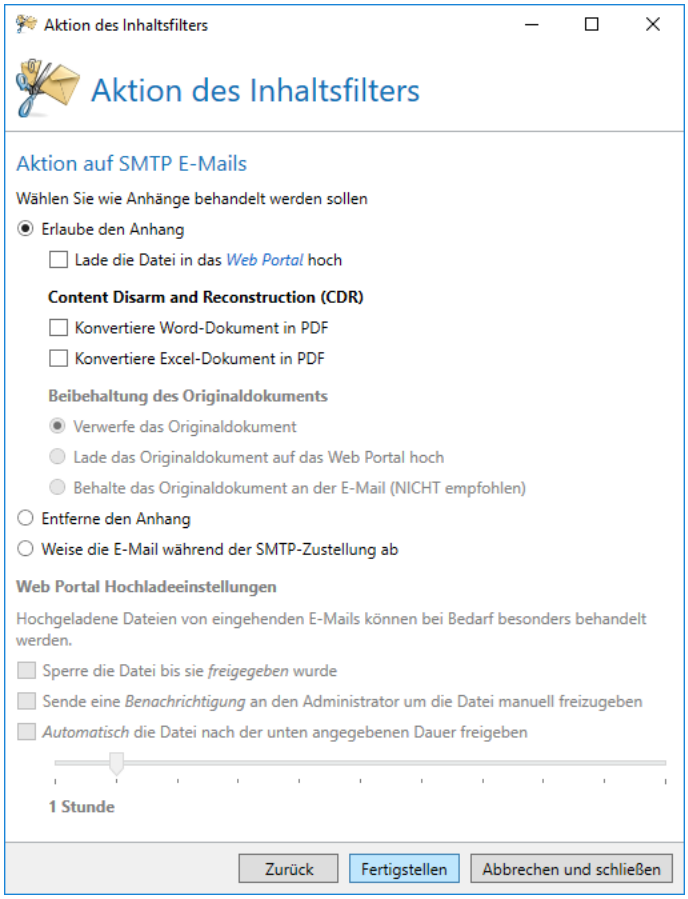


Bild 179: Aktionen auf SMTP-E-Mails

Die **Aktion auf Web Portal E-Mails** wird analog zu einer **Aktion auf SMTP-E-Mails** konfiguriert. (Bild 180)

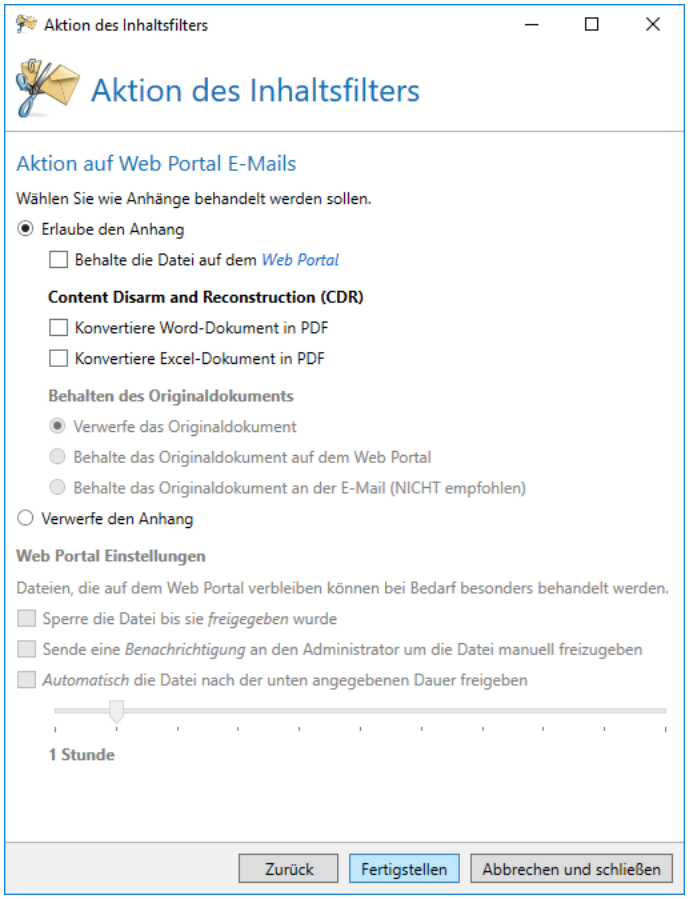


Bild 180: Aktion auf Web Portal E-Mails

NoSpamProxy Komponenten

Unter dem Menüpunkt **NoSpamProxy Komponenten** werden die Verbindungen zwischen den einzelnen Komponenten von NoSpamProxy konfiguriert (Bild 181).

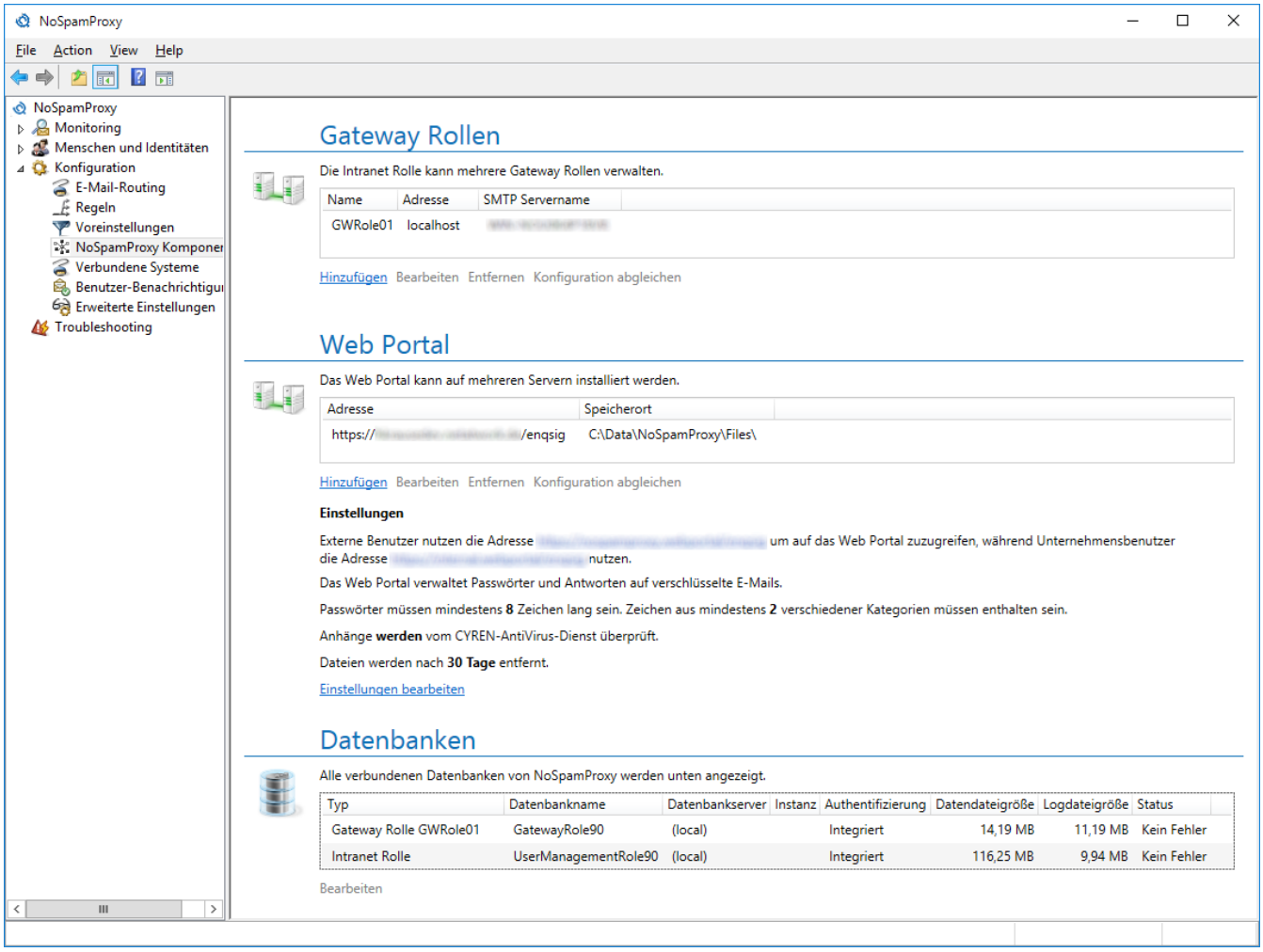


Bild 181: Die Verbindungen zu einzelnen Komponenten von NoSpamProxy

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 182).

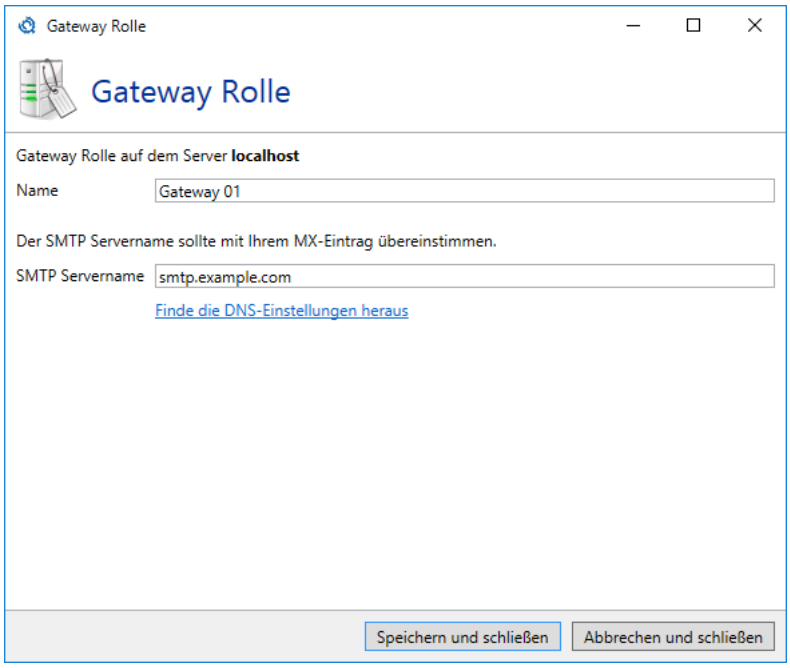


Bild 182: Die Server-Identität sollte dem "MX" Eintrag in Ihrem DNS entsprechen

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 angegeben Servernamen und Port verbinden**. Ansonsten wählen Sie **Die Management Konsole kann sich zur Gateway Rolle mit dem unten angegeben 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.

Web Portal Verbindungen

Im Dialog für eine Verbindung zum Web Portal (Bild 183) 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.

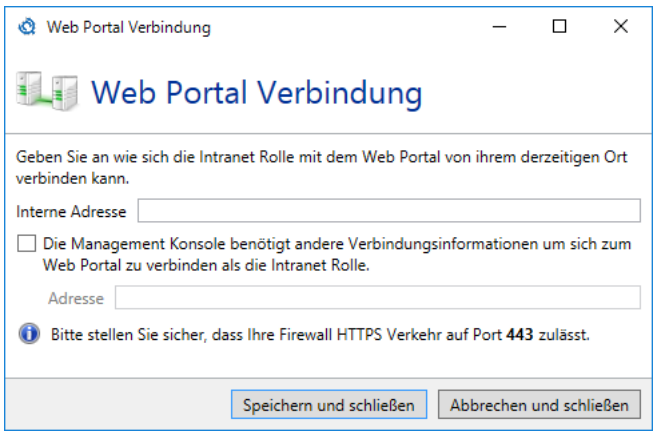


Bild 183: Die Einstellungen für eine Verbindung zu einem Web Portal

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 185):

- **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 184).
- **Microsoft Azure BLOB Storage**
  Durch die Angabe eines Azure Kontonamen und des dazugehörigen Kontoschlüssels werden alle Dateien im dazugehörigen Azure BLOB Storage gespeichert.

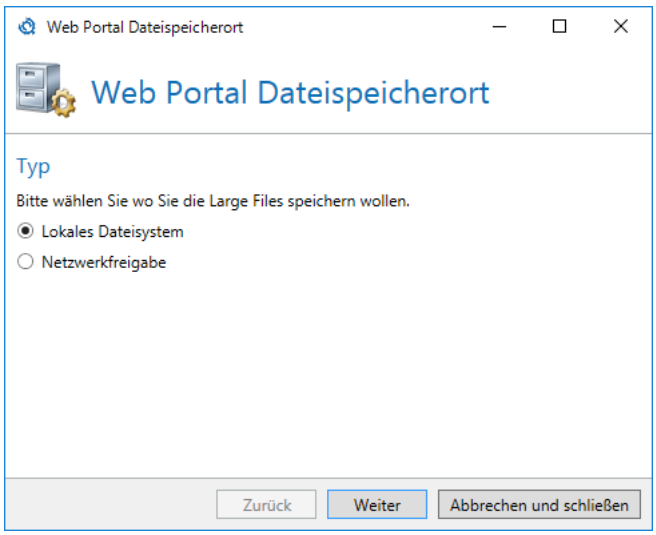


Bild 184: Speicherorte für die 'Large Files'

Je nach ausgewähltem Speicherort müssen Sie Speicherort und/oder Benutzerinformationen eingeben (Bild 185).

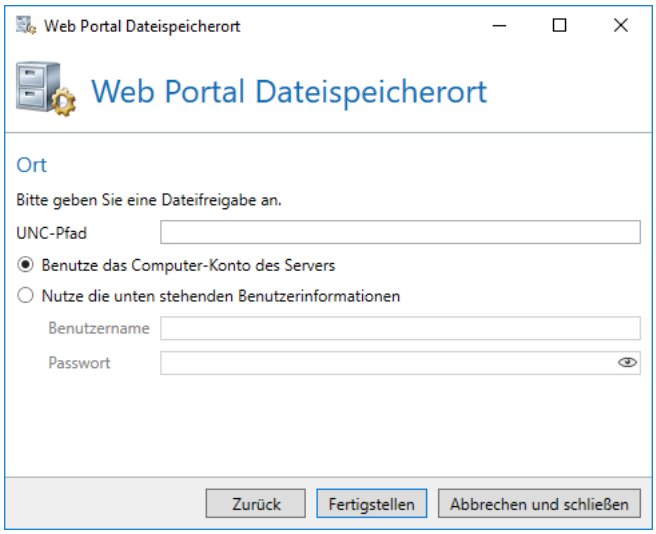


Bild 185: Die Verbindung zum Dateispeicherort des Web Portal am Beispiel der Netzwerkfreigabe

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 186). 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.

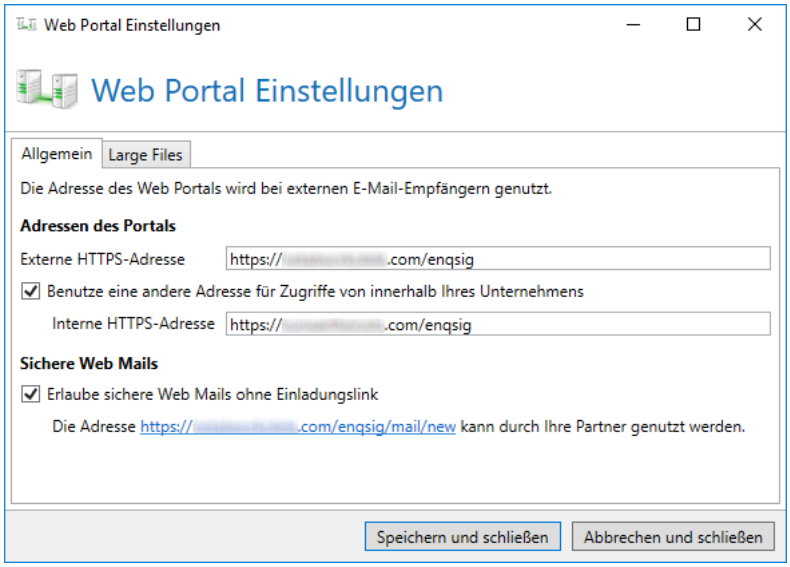


Bild 186: Allgemeine Einstellungen

Des Weiteren können Sie auf der zweiten Seite noch konfigurieren, welche Features Sie für 'PDF Mail' verwenden möchten (Bild 187):

- **Passworte verwalten**
  Aktivieren Sie dieses Feature, wenn Sie möchten, dass Kommunikationspartner ihre Passworte für PDF Mails selbst verwalten können. Hat ein Partner noch kein Passwort hinterlegt, so wird er von NoSpamProxy zunächst aufgefordert, eines zu hinterlegen, bevor eine E-Mail, die als "Automatisch verschlüsseln" markiert wurde, zugestellt wird. Wählen Sie hier außerdem noch aus, wie hoch Ihre Anforderungen an die Passwörter für PDF Mail sind. Über den Schieberegler können Sie bestimmen, wie lang und komplex das Passwort sein muss.
- **Antworten auf PDF Mails**
  Sobald dieses Feature aktiviert wird, können Kommunikationspartner auf PDF Mails über das Web Portal Antworten formulieren. Damit wird eine sichere Zwei-Wege-Kommunikation ohne Zertifikate ermöglicht.
- **Anhänge über das Web Portal verschicken**
  Wenn Sie diese Funktion aktivieren, werden Anhänge in PDF Mails immer in das Web Portal hochgeladen. In der PDF Mail verbleibt dann lediglich ein Link. Dies verbessert die Kompatibilität mit PDF-Readern z.B. auf Mobilgeräten, die keine Anhänge unterstützen.

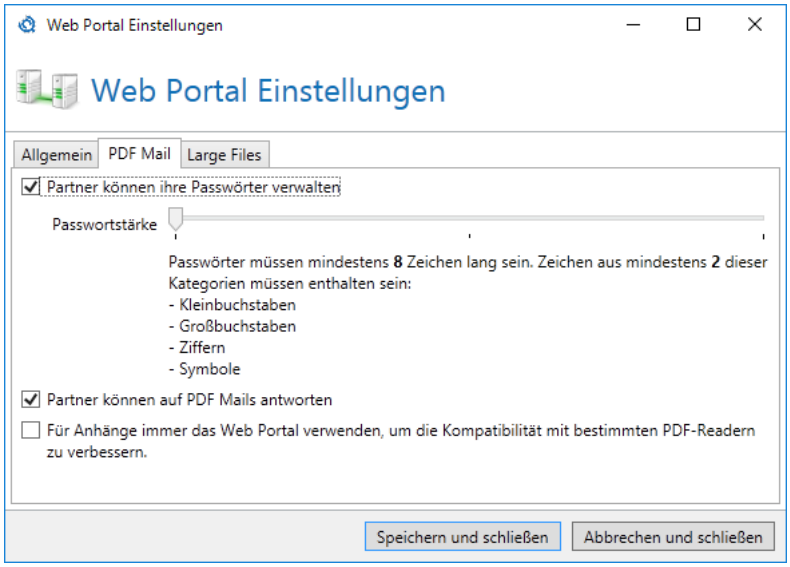


Bild 187: Einstellungen für PDF Mail

Wenn Sie Large Files aktivieren, müssen Sie auf der nächsten Seite noch einige weitere Einstellungen vornehmen (Bild 188). 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.

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

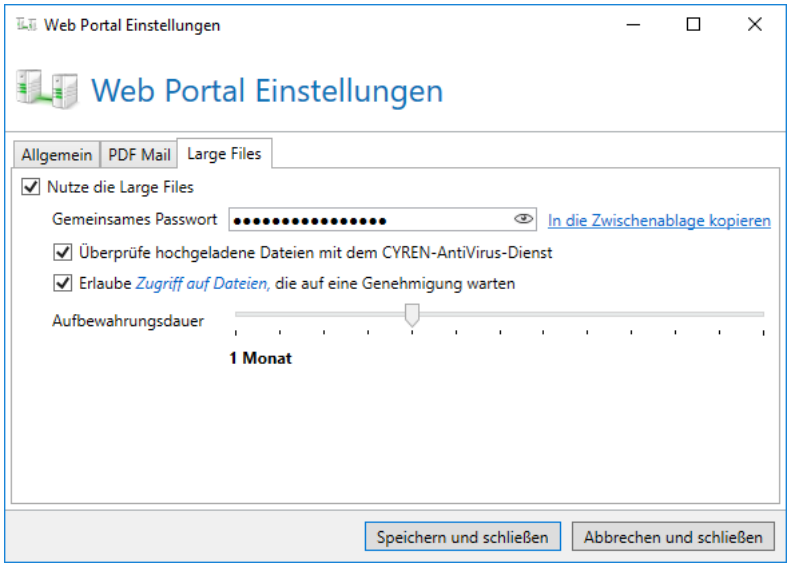


Bild 188: Einstellungen für Large Files

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 189).

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.

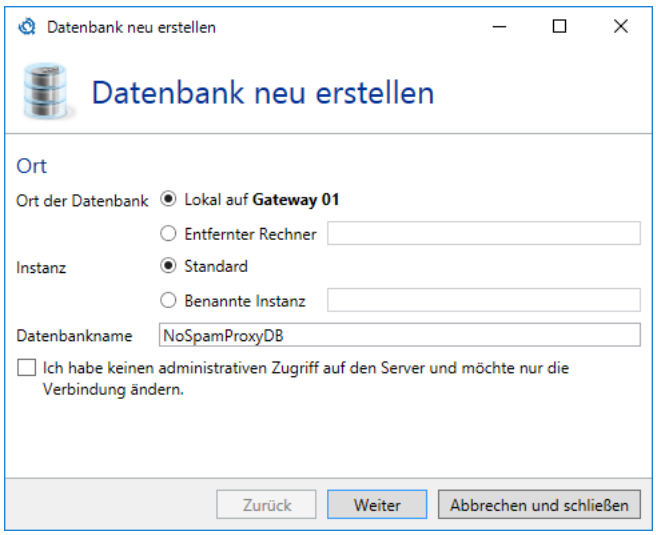


Bild 189: Die Verbindung zur Datenbank der entsprechenden Rolle

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 Domänennamen (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 190) 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.

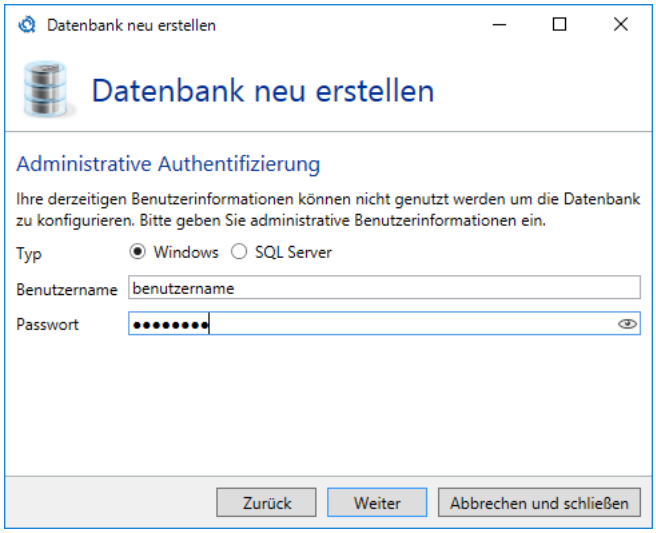


Bild 190: Die Verbindung zur Datenbank der entsprechenden Rolle

Die Einstellung **Service Authentifizierung** (Bild 191) 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 192).

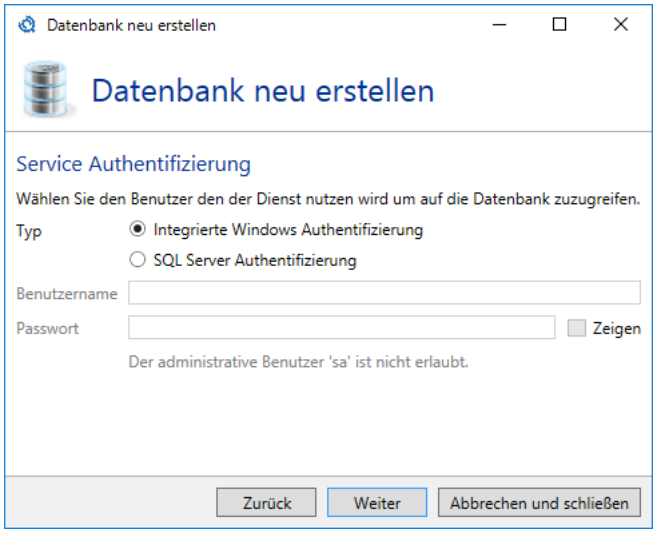


Bild 191: Dienstanbindung an die Datenbank.

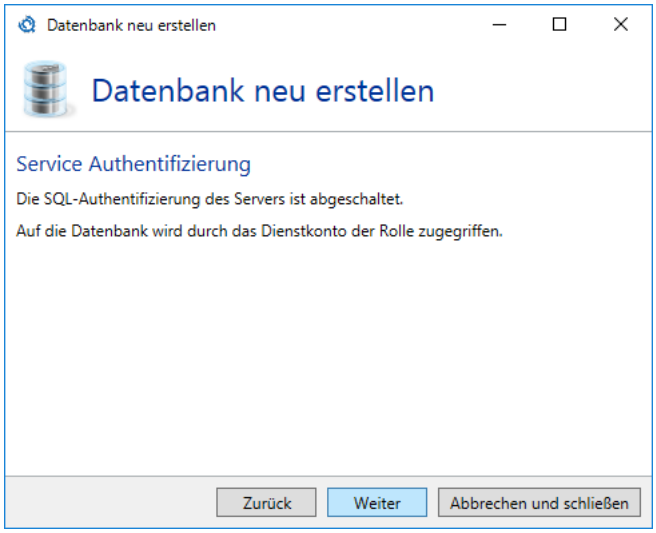


Bild 192: Keine SQL-Authentifizierung verfügbar.

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 193).

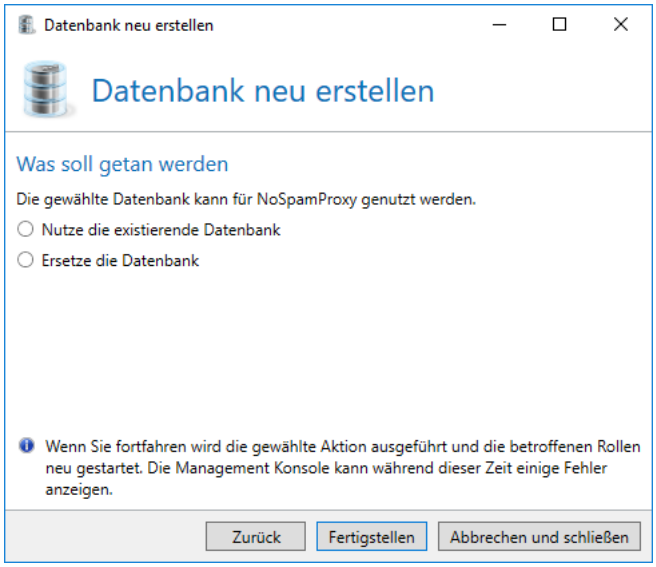


Bild 193: Wählen Sie ob die alte Datenbank gelöscht oder erhalten werden soll

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 194).

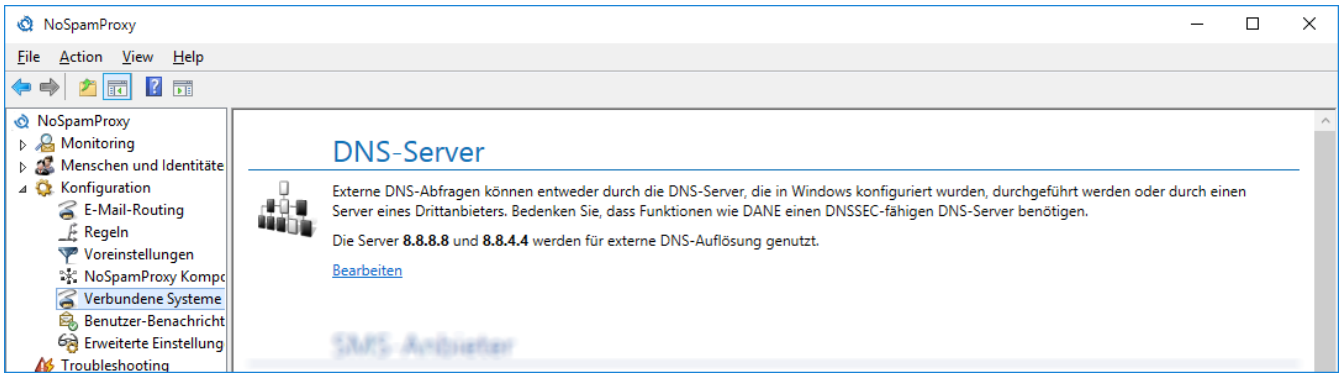


Bild 194: Anbindung an einen DNSSEC fähigen Server

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 195).

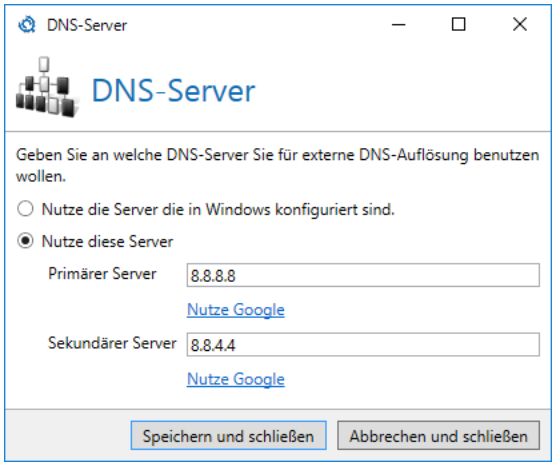


Bild 195: Konfiguration eines DNSSEC fähigen Server

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.

SMS-Anbieter

Bei der Verschlüsselung von PDF-Dokumenten kann eine SMS mit dem Passwort an den Empfänger der E-Mail gesendet werden. Um diese Funktion zu nutzen, ist es notwendig, mindestens ein Profil in dem Abschnitt **SMS-Anbieter** (Bild 196) zu konfigurieren.

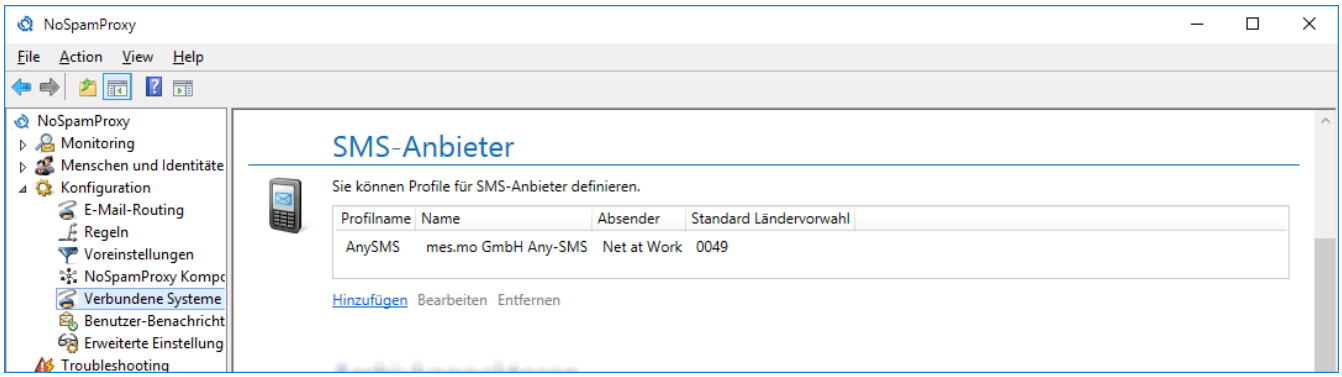


Bild 196: Die Liste der konfigurierten SMS-Anbieter

Derzeit werden folgende SMS Provider unterstützt:

- **mes.mo GmbH Any-SMS**- http://www.any-sms.de
- **MindMatics AG**- http://www.mindmatics.de
- **tyntec**- http://www.tyntec.com
- **Whatever Mobile GmbH**- http://www.whatevermobile.com
- **CM Telecom**- http://www.cmtelecom.com

In dem Dialog zum Erstellen eines neuen Profils wählen Sie zunächst Ihren SMS-Anbieter aus (Bild 197). Unterhalb des Provider-Namens werden technische Details über den Provider angezeigt, z.B. der Servername. In der Regel brauchen Sie diese Einstellungen nicht zu ändern.

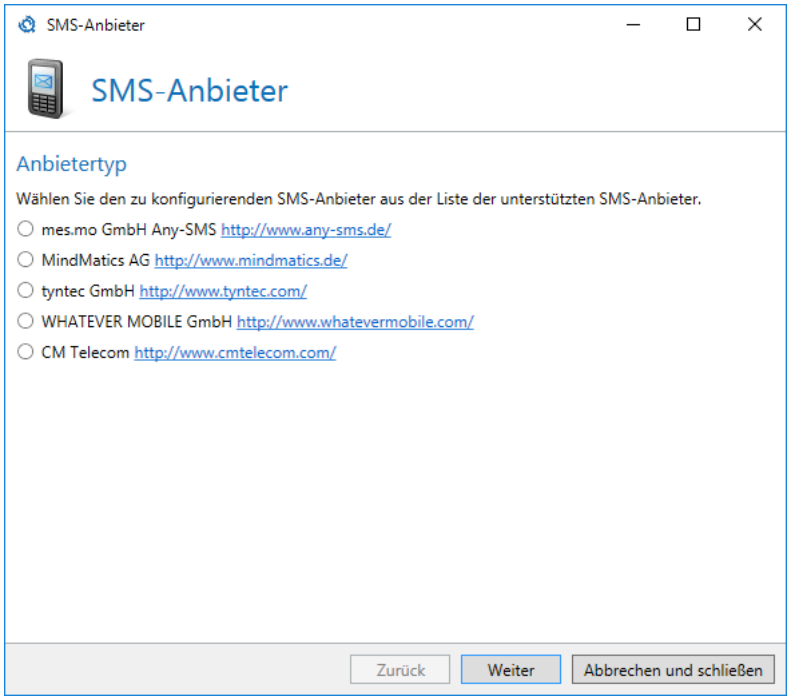


Bild 197: Auswahl des SMS Providers für ein neues Profil

Nach der Auswahl wird die Konfiguration der Verbindung zum Anbieter angezeigt (Bild 198).

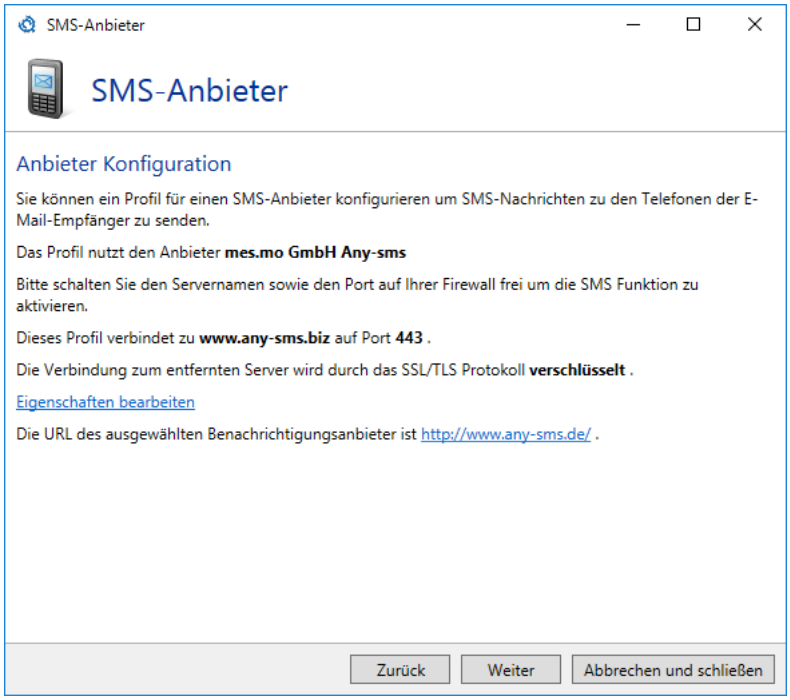


Bild 198: Die Verbindungseigenschaften des gewählten Providers

Im nächsten Schritt geben Sie dem Profil einen Namen (Bild 199). Außerdem legen Sie hier den Absender fest, mit dem die SMS Nachrichten gesendet werden sollen. Sie können hier entweder die Telefonnummer eines Mobiltelefons angeben oder eine Alphanumerische Zeichenkette mit einer maximalen Länge von 11 Zeichen, z.B. den Namen Ihrer Firma. Im dritten Feld müssen Sie noch eine Standard Landesvorwahl angeben. Diese wird verwendet, wenn beim Versenden eine Telefonnummer ohne Landesvorwahl verwendet wurde.

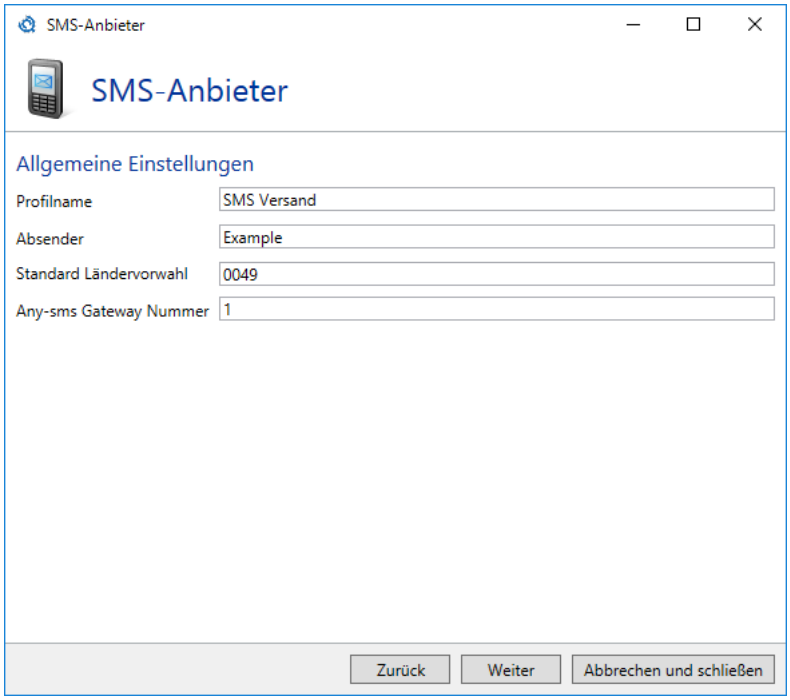


Bild 199: Profilname und weitere Optionen

Im letzten Schritt geben Sie Ihre Zugangsdaten ein, die Sie von dem Anbieter bekommen haben (Bild 200).

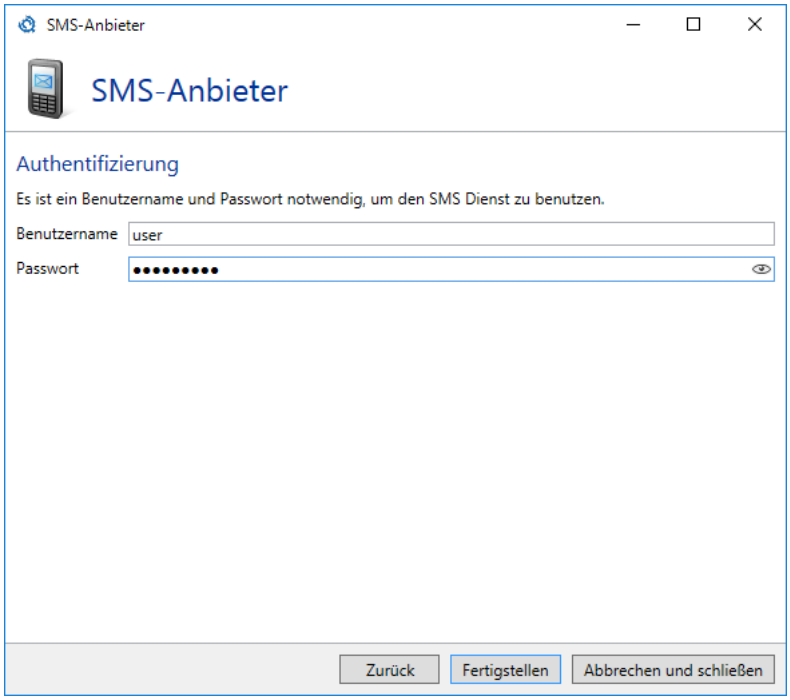


Bild 200: Benutzername und Kennwort festlegen

Die Konfiguration des Profils ist damit abgeschlossen. Es kann nun in den Regeln von der Aktion Anhänge mit einem Passwort schützen verwendet werden.

Archivschnittstelle

Über die Archivschnittstelle können E-Mails und qualifiziert signierte Dokumente an ein externes Archivsystem übergeben werden (Bild 201). Unterstützt werden derzeit das Dateisystem, ein Archivpostfach sowie d.velop d.3. Es können auch mehrere Archivsysteme parallel verwendet werden.

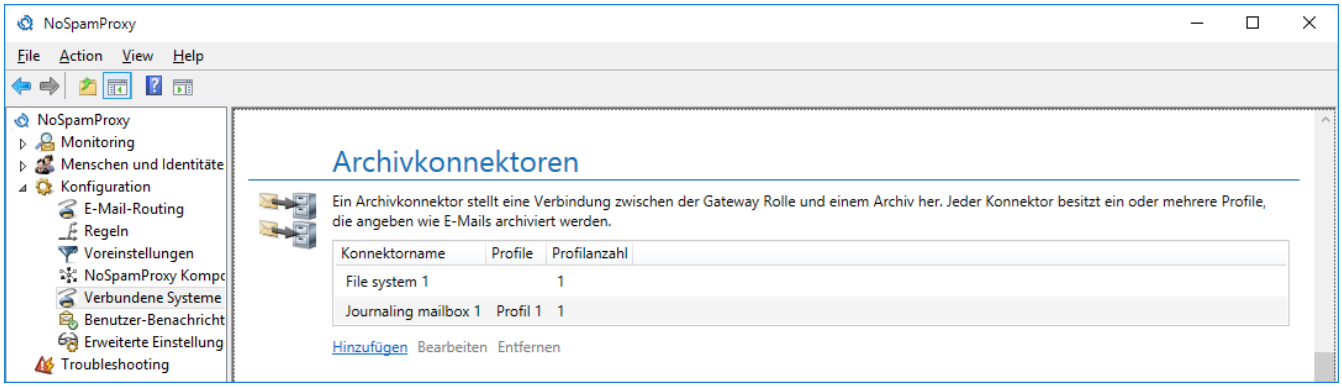


Bild 201: Die Liste der konfigurierten Archivschnittstellen

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 202).

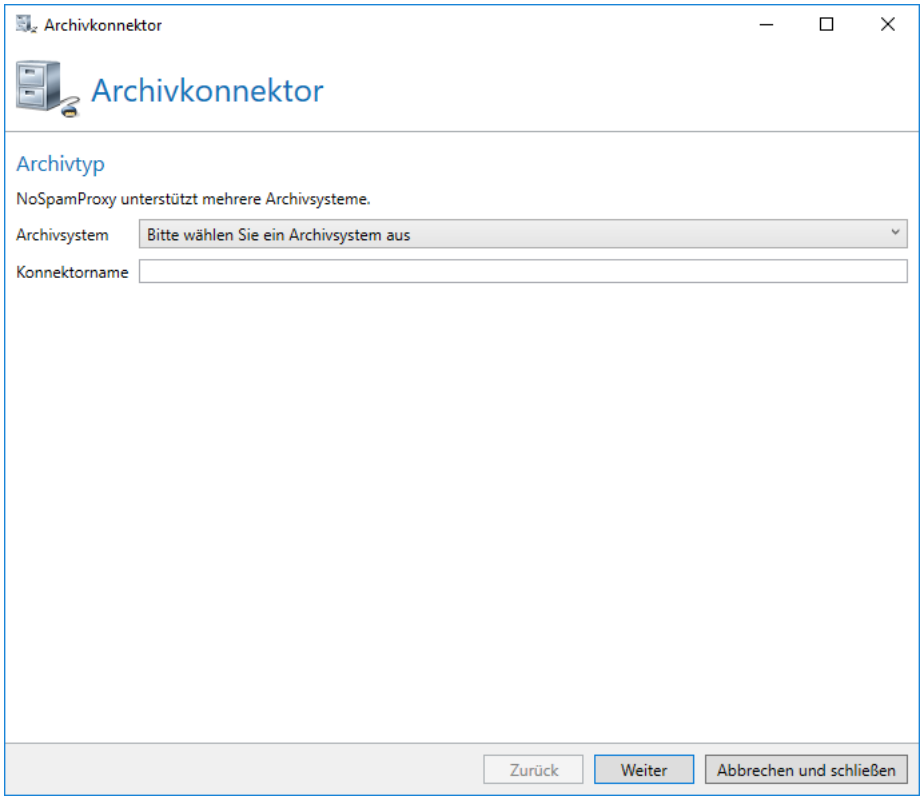


Bild 202: Allgemeine Einstellungen des Archivkonnektors

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 203).

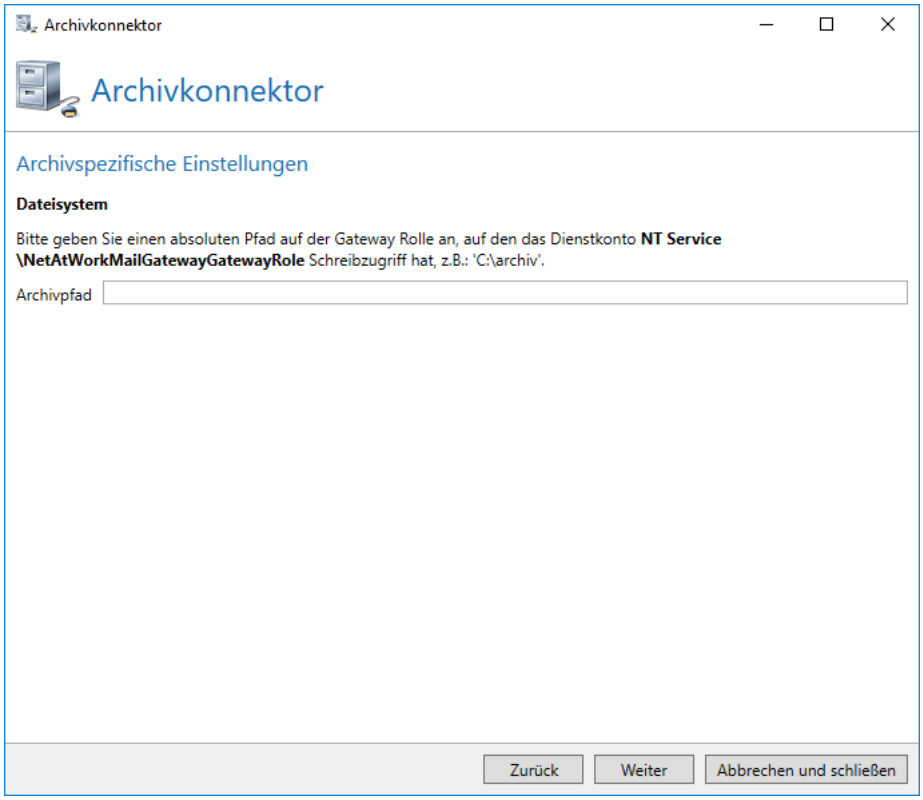


Bild 203: Eigenschaften für die Ablage im Dateisystem

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 204). E-Mails und Dokumente werden in dieses Verzeichnis geschrieben und von dort durch das d.velop d.3 System abgeholt.

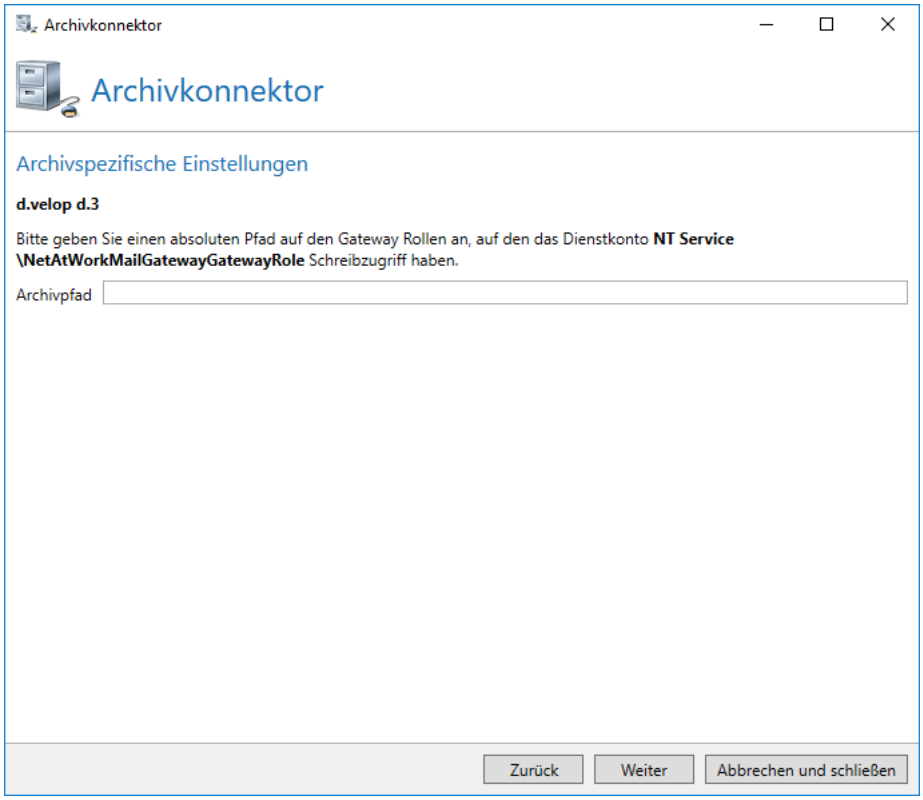


Bild 204: d.velop d.3-spezifische Eigenschaften

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 205). Außerdem wählen Sie hier aus, welche E-Mails durch dieses Profil archiviert werden. Dabei ist zu beachten, dass E-Mails mit einem qualifiziert signierten Anhang immer archiviert werden. Sie können optional auch alle anderen E-Mails archivieren.

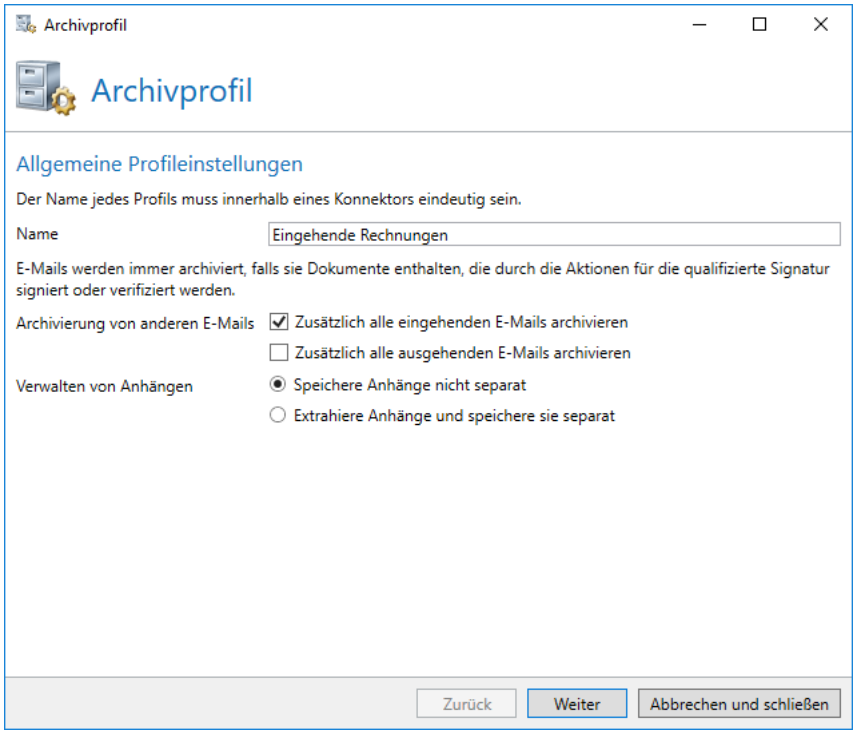


Bild 205: Allgemeine Einstellungen des Profils

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.

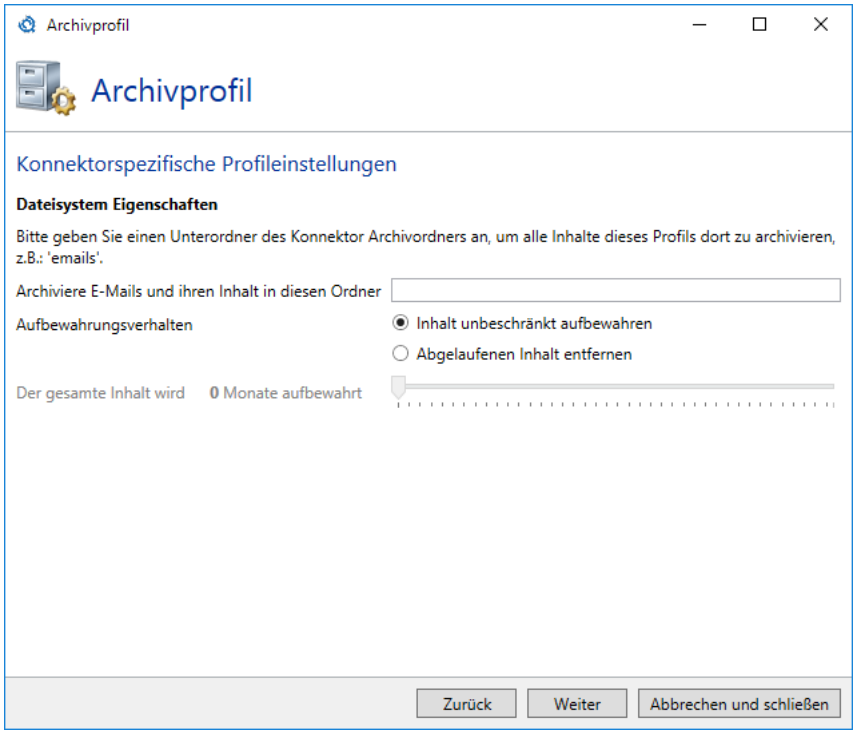


Bild 206: Eigenschaften für die Ablage im Dateisystem

Im Falle eines **Archivpostfachs** wird die E-Mail-Adresse des Zielpostfachs benötigt (Bild 207).

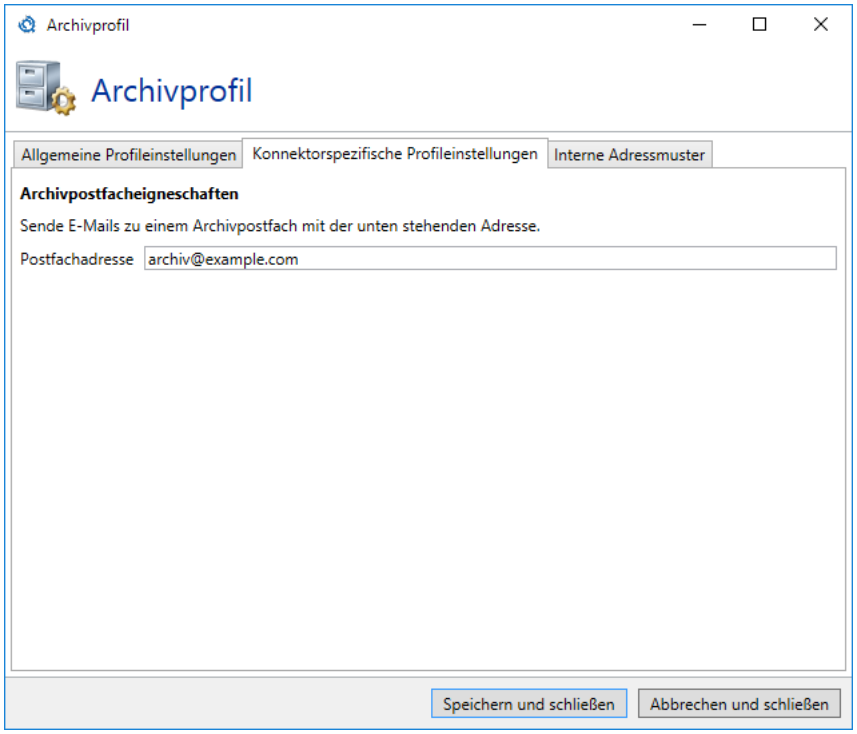


Bild 207: Eigenschaften für die Ablage in einem Archivpostfach

Bei einer Verbindung zu einem d.velop d.3 System ist keine weitere Konfiguration erforderlich. Der Dialog ist in diesem Fall leer (Bild 208).

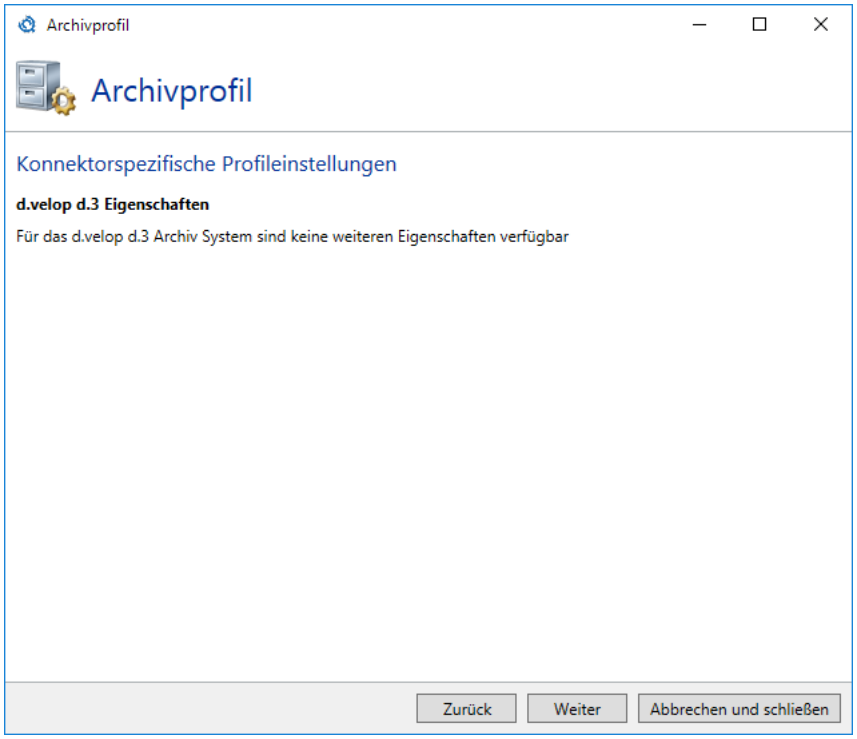


Bild 208: Eigenschaften für die Ablage in einem d.velop d.3 System

Im nächsten Schritt legen Sie fest, für welche lokalen E-Mailadressen dieses Profil zuständig ist. (Bild 209). 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 210) 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.

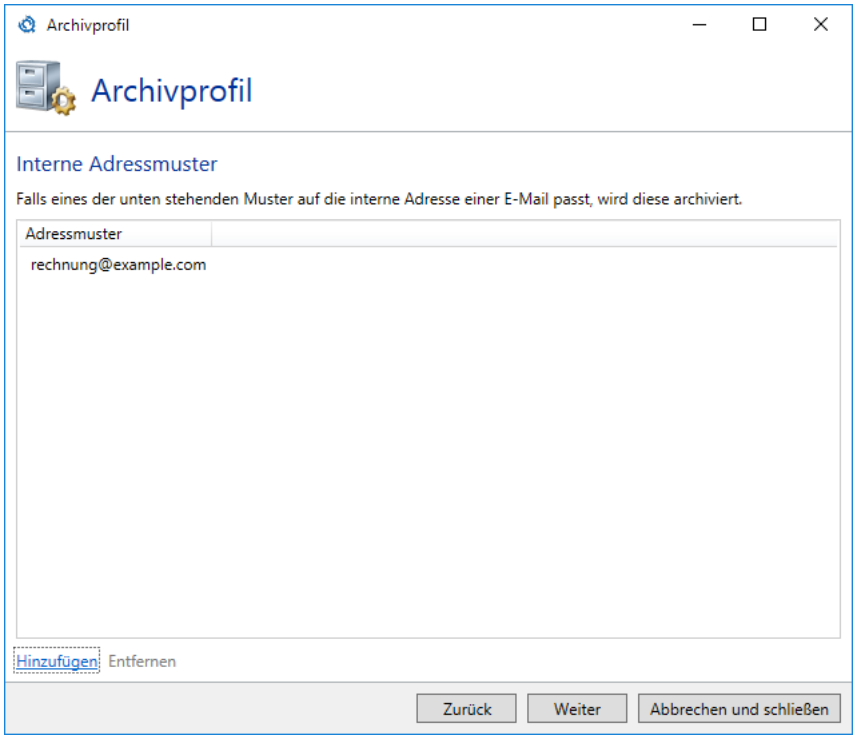


Bild 209: Zuordnung von Profilen zu internen E-Mail-Adressen

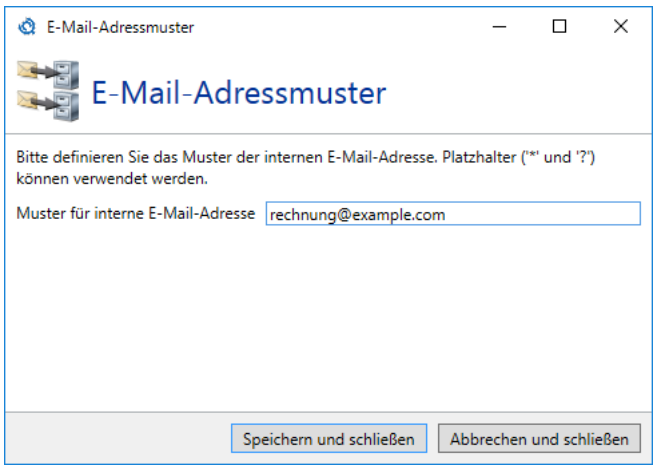


Bild 210: Neue Zuordnung erstellen

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 211).

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.

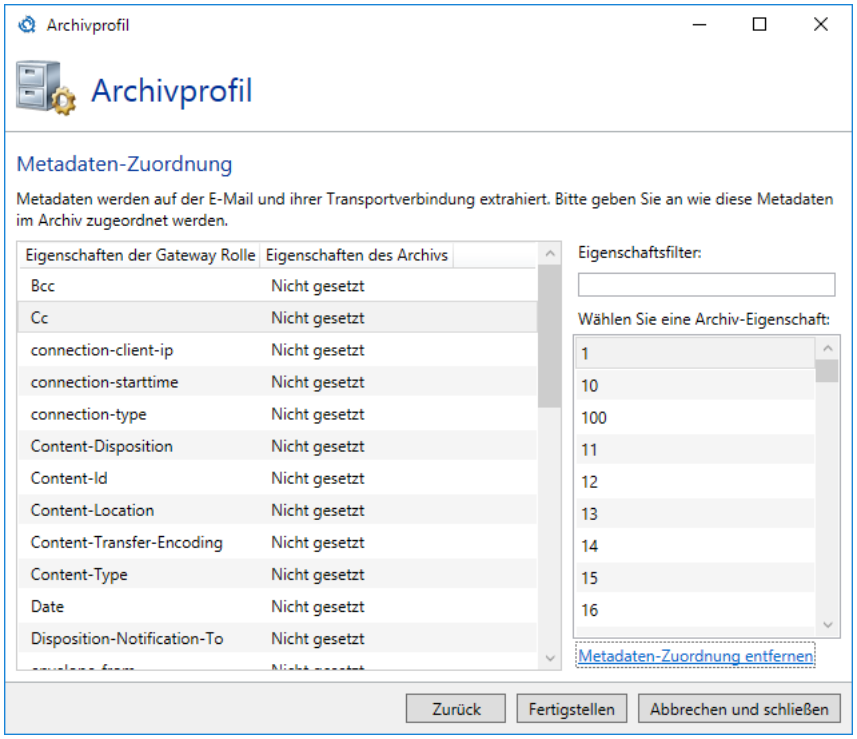


Bild 211: Metadaten-Zuordnung

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 212).

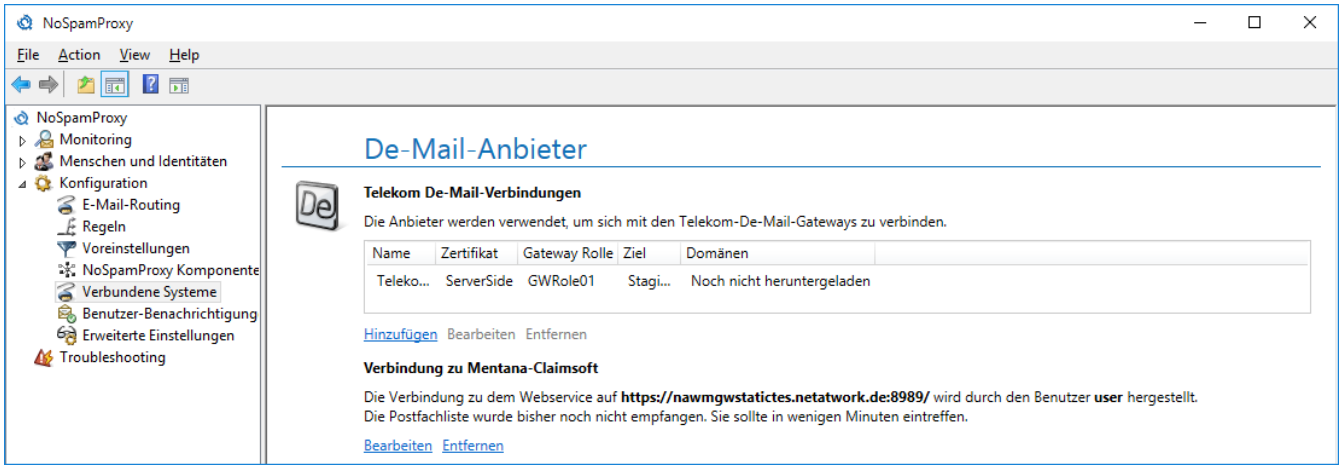


Bild 212: Die Liste der konfigurierten De-Mail-Verbindungen

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 213).

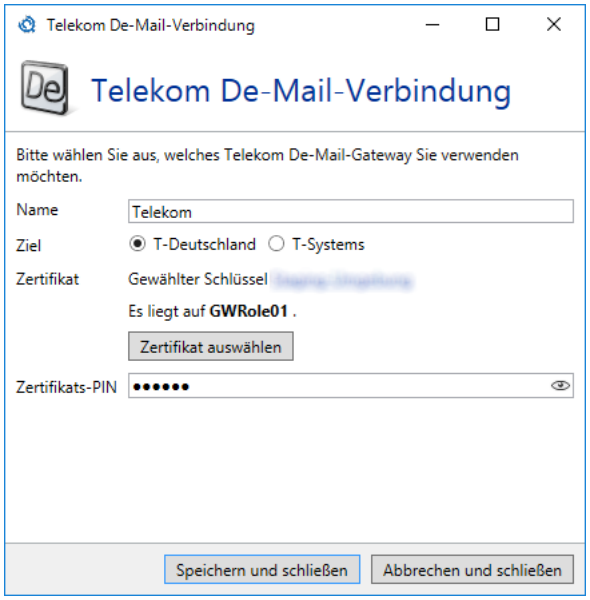


Bild 213: Konfigurieren Sie die Verbindung zum Telekom De-Mail-Anbieter

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 214).

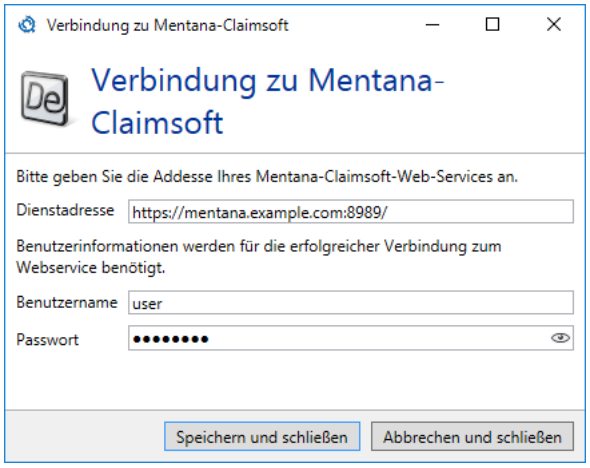


Bild 214: Verbinden Sie sich zum Mentana-Claimsoft-Webservice

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.

Verbindung zum digiSeal server

Bei der Nutzung der digiSeal-server-Dienste für die qualifizierte Dokumentensignatur benötigt NoSpamProxy Encryption die Verbindungsinformationen zu diesem Server (Bild 215). Konfigurieren Sie

die Verbindung über **Bearbeitung der digiSeal-server-Verbindungsinformationen**. In dem Dialog (Bild 216) können Sie nun die **Unterstützung für die digiSeal server Dienste** ein oder ausschalten. Wenn Sie die Dienste einschalten, müssen Sie in das Feld **Servername** den Namen des Zielsystems eingeben und unter **Port** den Netzwerk-Port, unter dem die digiSeal server Dienste erreichbar sind.

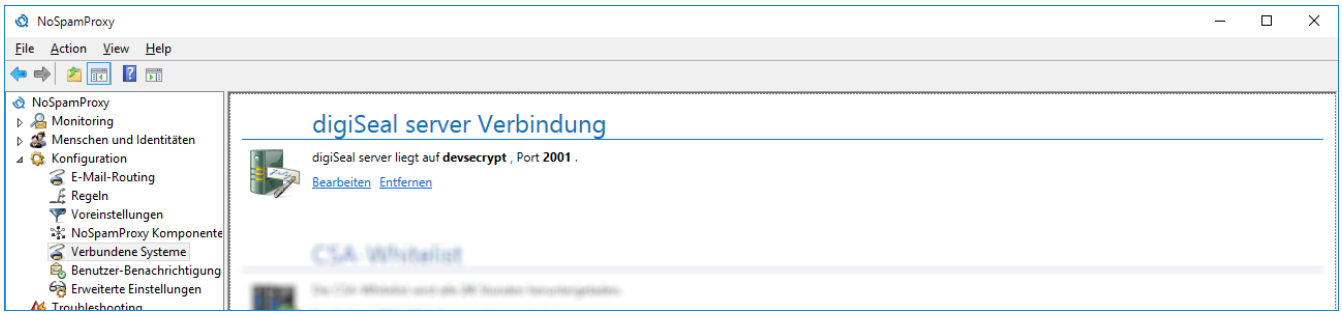


Bild 215: Die Verbindung zum digiSeal server

Um die Anbindung an den digiSeal server vollständig durchzuführen, halten Sie sich an die Schritte aus dem Handbuch Anbindung digiSeal server

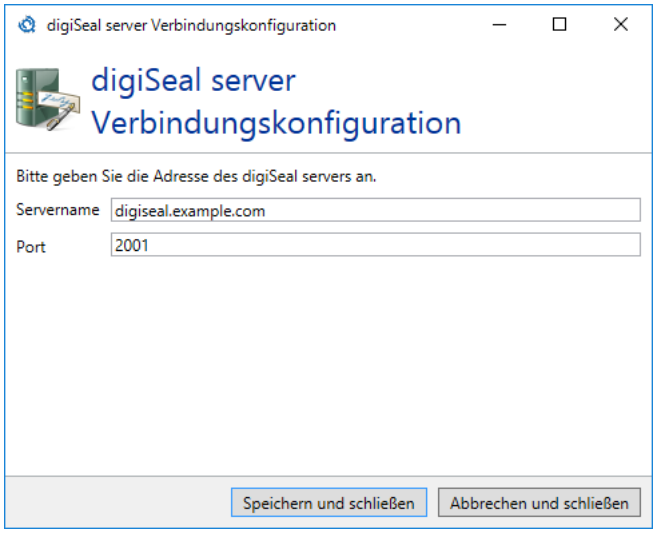


Bild 216: Verbinden Sie sich zu Ihrem digiSeal server

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 217).

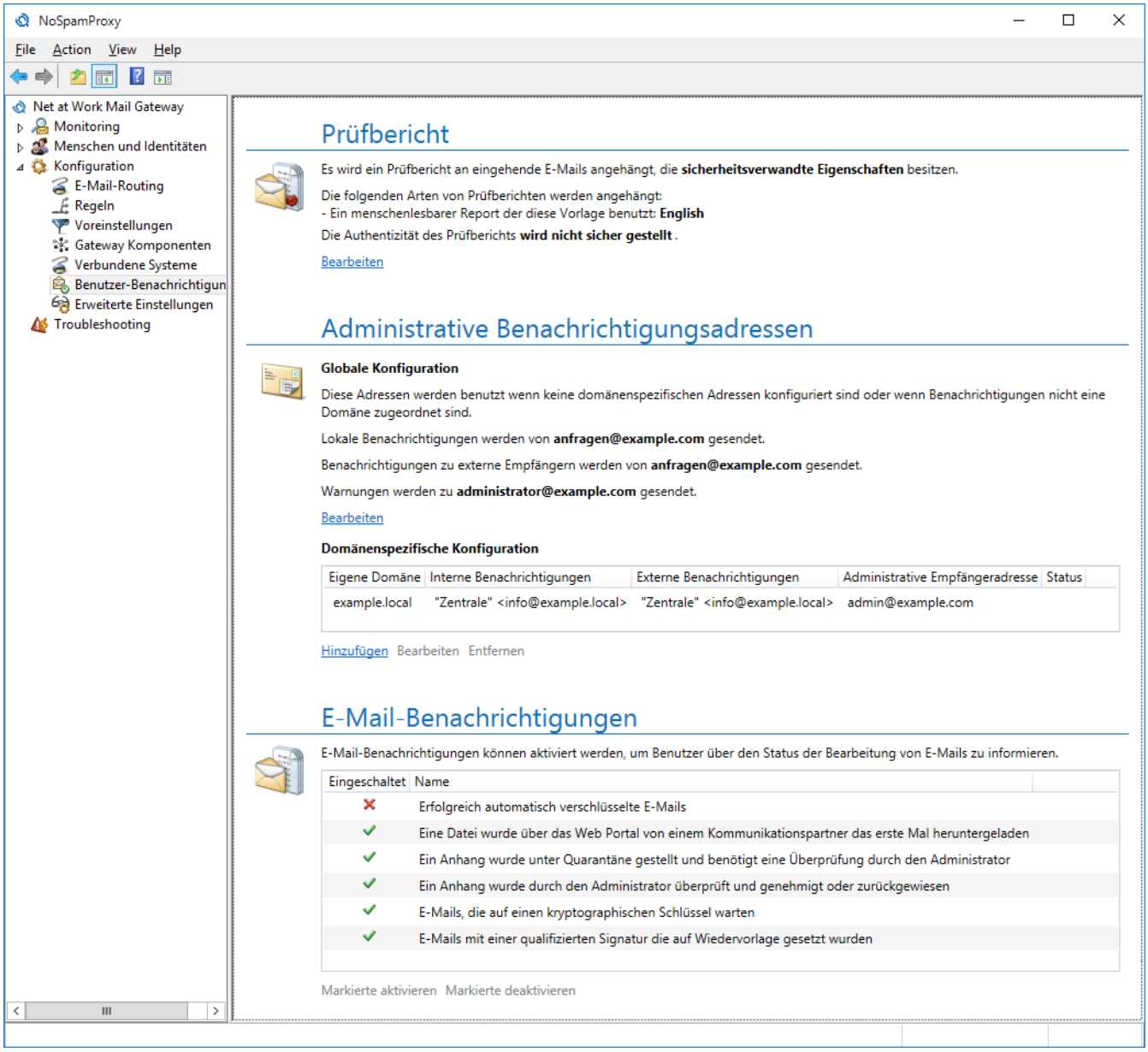


Bild 217: Benutzerbenachrichtigungen

Prüfbericht

Der Prüfbericht enthält Informationen über sicherheitsrelevante Eigenschaften und Vorgänge einer E-Mail. Er kann an E-Mails an lokale Adressen angehängt werden. Die aktuell eingestellten Werte werden in dem Knoten **Prüfbericht** angezeigt.

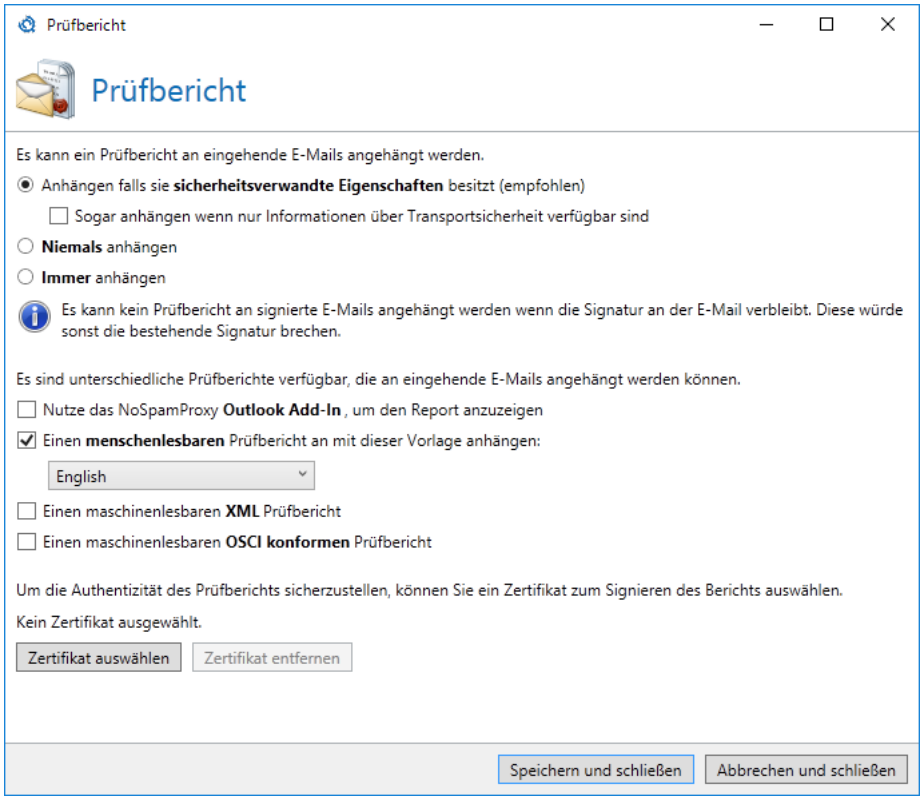


Bild 218: Der Prüfbericht

In der Konfiguration für den Prüfbericht wählen Sie zuerst aus, an welche E-Mails der Bericht angehängt werden soll. Anschließend wählen Sie die Art des anzuhängenden Prüfberichts.

- **Menschenlesbarer Prüfbericht**
  Der Textuelle Prüfbericht stellt die Informationen in für Menschen lesbarer Form dar. Wählen Sie für den Bericht eine Vorlage, die für die Darstellung des Berichts verwendet werden soll. Standardmäßig gibt es zwei Vorlagen (eine deutsche und eine englische). Die Vorlagen liegen in dem Konfigurationsverzeichnis der Gateway Rolle und haben die Erweiterung `HtmlProcessCardTemplate`. Falls Sie die Vorlagen anpassen wollen, dann ändern Sie bitte nicht die Standardvorlagen, da diese bei Updates der Software überschrieben werden. Legen Sie stattdessen eine Kopie einer bestehenden Vorlage an und arbeiten Sie damit.
- **OSCI konformer Prüfbericht**
  Der OSCI konforme Prüfbericht erstellt einen OSCI-Laufzettel. Dieser dient der automatischen Weiterverarbeitung durch OSCI konforme Drittsysteme. Dieser Prüfbericht muss zwingend mit einem Zertifikat signiert werden.
- **XML Prüfbericht**
  Der XML Prüfbericht dient der automatischen Weiterverarbeitung der Prüfberichtsdaten durch eine weitere Anwendung.
- **Prüfbericht für das Outlook Add-In**
  Dieser Prüfbericht wird als X-Header in die E-Mail eingebettet. Diese eingebetteten Daten können vom **Outlook Add-In** von NoSpamProxy angezeigt werden.

Der Prüfbericht kann digital signiert werden, um die Authentizität sicher zu stellen. Dazu können Sie ein privates E-Mail-Zertifikat auswählen. Diese Signatur ist für den OSCI-Laufzettel zwingend erforderlich, für alle anderen Prüfberichte ist sie optional.

Administrative E-Mail-Adressen

In diesem Abschnitt werden Adressen für Benachrichtigungen von NoSpamProxy hinterlegt (Bild 219). 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.

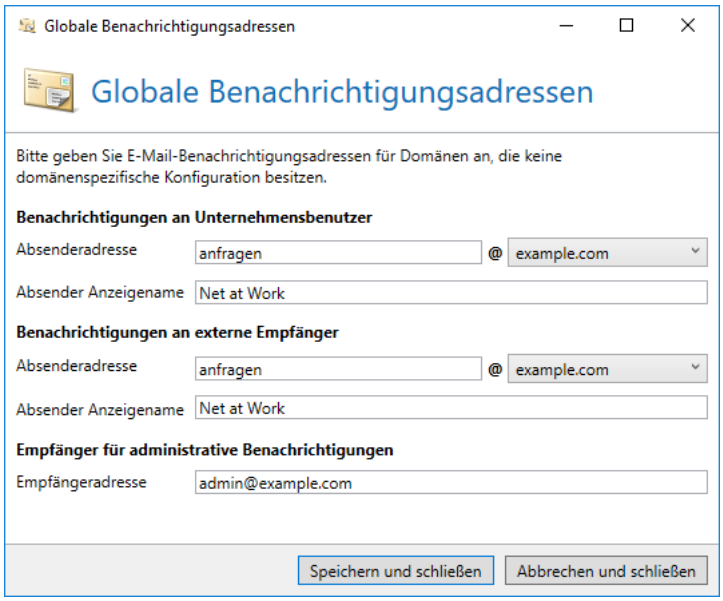


Bild 219: Die globalen Benachrichtigungsadressen

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 220).

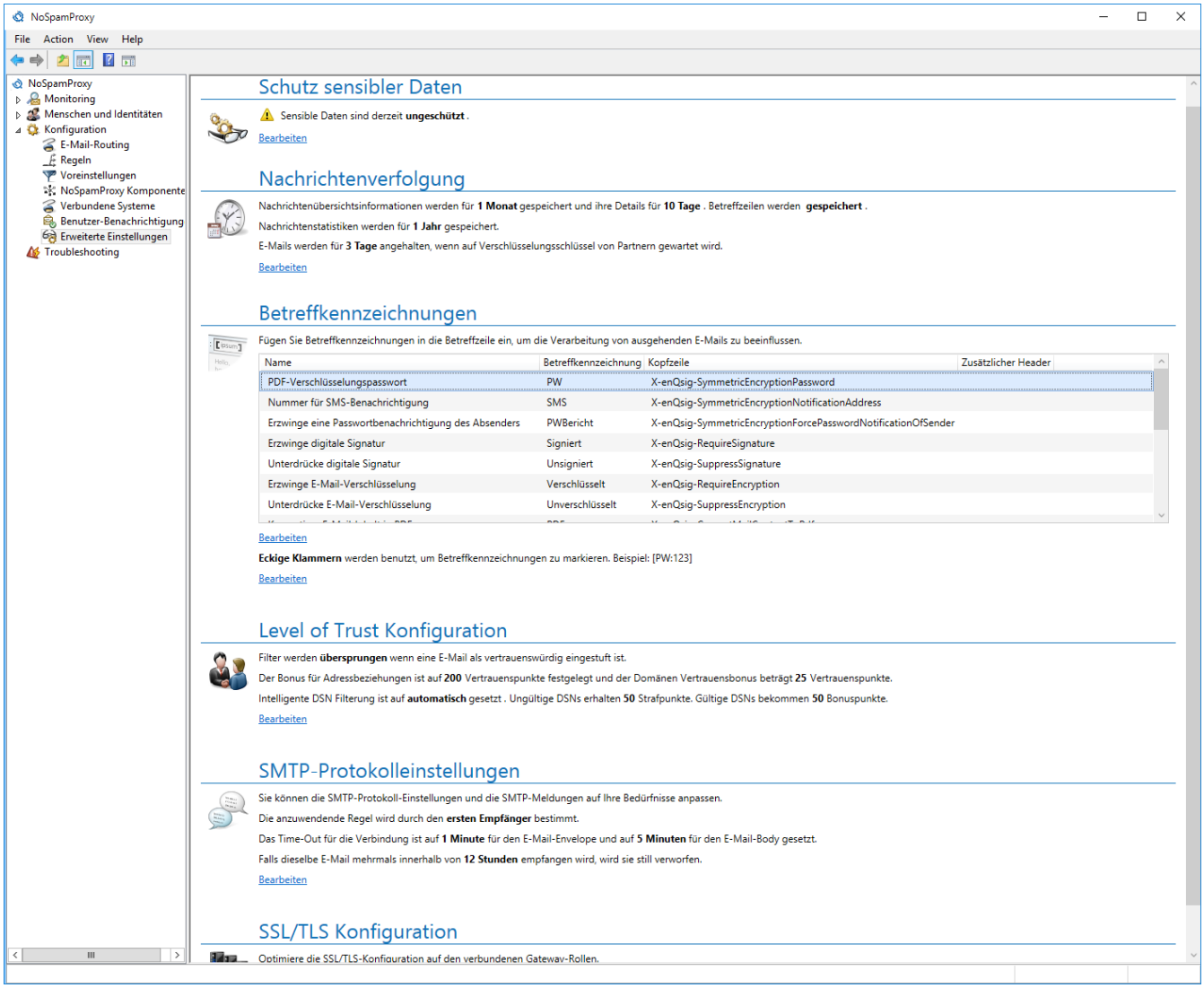


Bild 220: Die erweiterte Einstellungen von NoSpamProxy

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 221). 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.

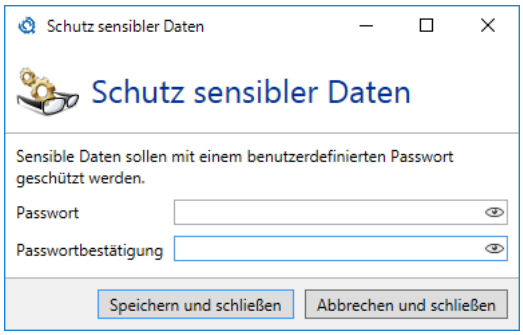


Bild 221: Das Passwort zum Schutz Ihrer Daten

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 222).

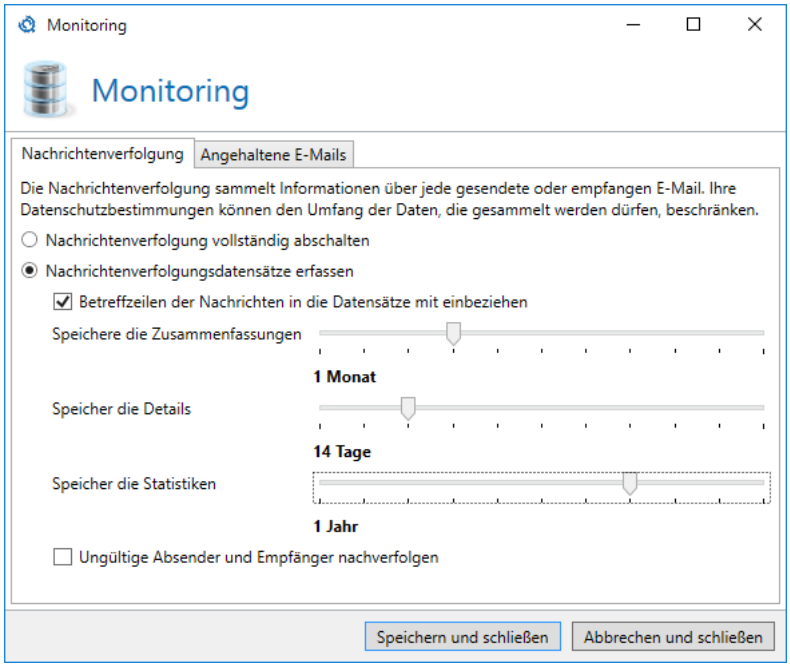


Bild 222: Anpassung der Aufbewahrungsfristen

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 Nachrichtenverfolgungsdatensätze 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.

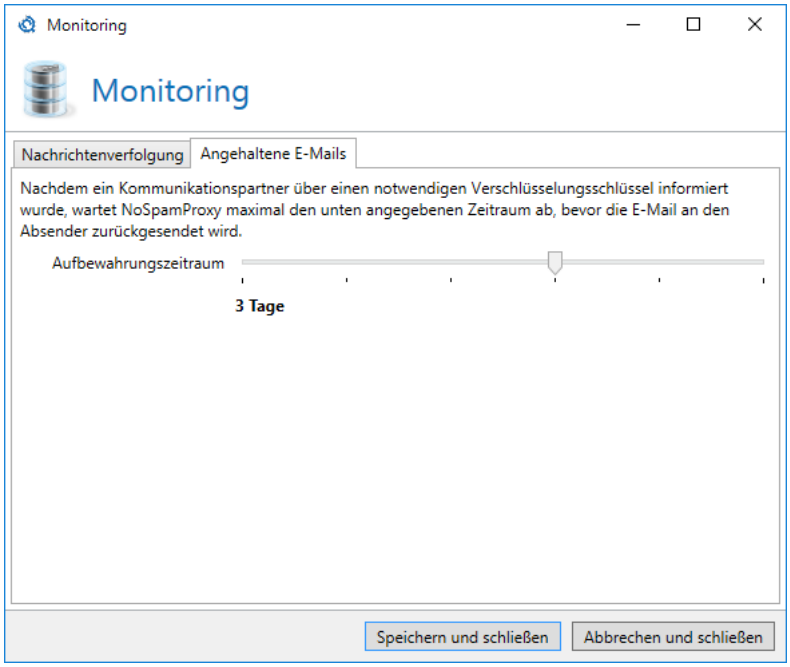


Bild 223: Anpassung der Aufbewahrungsfrist für angehaltene E-Mails

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 Schlüsselworte werden vor dem Versand von NoSpamProxy aus der Betreffzeile entfernt.

Nutzen Sie die Betreffkennzeichnungen, in dem Sie am Anfang oder Ende der Betreffzeile in Klammern die Schlüsselworte 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 224).

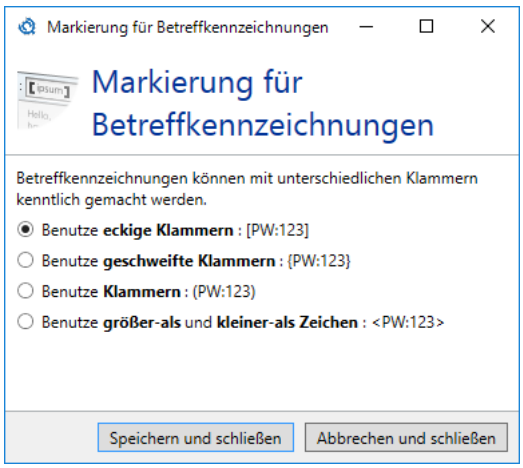


Bild 224: Konfigurieren Sie die Marker für Betreffkennzeichnungen

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:

- **[Versandbestätigung]**

De-Mail: Fordert eine Versandbestätigung von De-Mail an. Entspricht einen Einschreiben bei Briefen.

- **[Eingangsbestätigung]**
  De-Mail: Fordert eine Empfangsbestätigung von De-Mail an. Entspricht einem Einwurf-Einschreiben bei Briefen.
- **[Abholbestätigung]**
  De-Mail: Fordert eine Abholbestätigung von De-Mail an.
- **[Absenderbestätigt]**
  De-Mail: Setzt den Status 'Absenderbestätigt' in De-Mails.
- **[Persönlich]**
  De-Mail: Setzt den Status 'Privat' in De-Mail. Entspricht einem Einschreiben Eigenhändig bei Briefen.
- **[Autoverschlüsseln]**
  Automatische Verschlüsselung: Benutzt kryptographische Schlüssel um die E-Mail zu schützen oder sichert den E-Mail-Inhalt und alle Anhänge durch **PDF Mail**, falls keine kryptographischen Schlüssel verfügbar sind.
- **[PW]**
  Verschlüsselt angehängte PDF-Dokumente. `[PW]` für ein automatisch generiertes Passwort oder `[PW:geheim4937]` für z.B. das Passwort 'geheim4937'.
- **[SMS:Nr]**
  SMS-Benachrichtigung: Die Telefonnummer wird in der Aktion Anhänge mit einem Passwort schützen genutzt, um ein ggf. eingegebenes PDF-Passwort durch einen der konfigurierten SMS-Anbieter direkt an das Mobiltelefon des Empfängers per SMS zu senden. Sollte kein Passwort vergeben sein, wird diese Nummer ignoriert.
- **[PWBericht]**
  Erzwinge Passwortbenachrichtigung: Das gesetzte oder generierte Passwort der Aktion Anhänge mit einem Passwort schützen wird bei der Benutzung dieser Betreffkennzeichnung in jedem Fall auch an den Absender der E-Mail versandt.
- **[Signiert]**
  Erzwinge Signatur: Erzwingt eine digitale Signatur durch kryptographische Schlüssel. Sollte 'Autoverschlüsseln' angefordert sein, wird diese Option ignoriert.
- **[Unsigniert]**
  Unterdrücke Signatur: Unterdrückt eine digitale Signatur durch kryptographische Schlüssel. Sollte 'Autoverschlüsseln' angefordert sein, wird diese Option ignoriert.
- **[Verschlüsselt]**
  Erzwinge Verschlüsselung: Erzwingt eine E-Mail-Verschlüsselung mit Hilfe von kryptographischen Schlüsseln. Sollte 'Autoverschlüsseln' angefordert sein, wird diese Option ignoriert.
- **[Unverschlüsselt]**
  Unterdrücke Verschlüsselung: Unterdrückt eine E-Mail-Verschlüsselung mit Hilfe von kryptographischen Schlüsseln. Sollte 'Autoverschlüsseln' angefordert sein, wird diese Option ignoriert.
- **[PDF]**
  PDF Konvertierung: Konvertiert den gesamten E-Mail-Inhalt in ein PDF Dokument

- **[PasswortZurücksetzen]**
  Versendet statt der aktuellen E-Mail eine Aufforderung an den Empfänger sein Kennwort für PDF Mail neu zu vergeben.
- **[LFT]**
  Diese Kennzeichnung wird nur vom Outlook Add-In für die **Large Files** verwendet.

Sie können die Betreffkennzeichnungen an Ihre Bedürfnisse anpassen (Bild 225) 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.

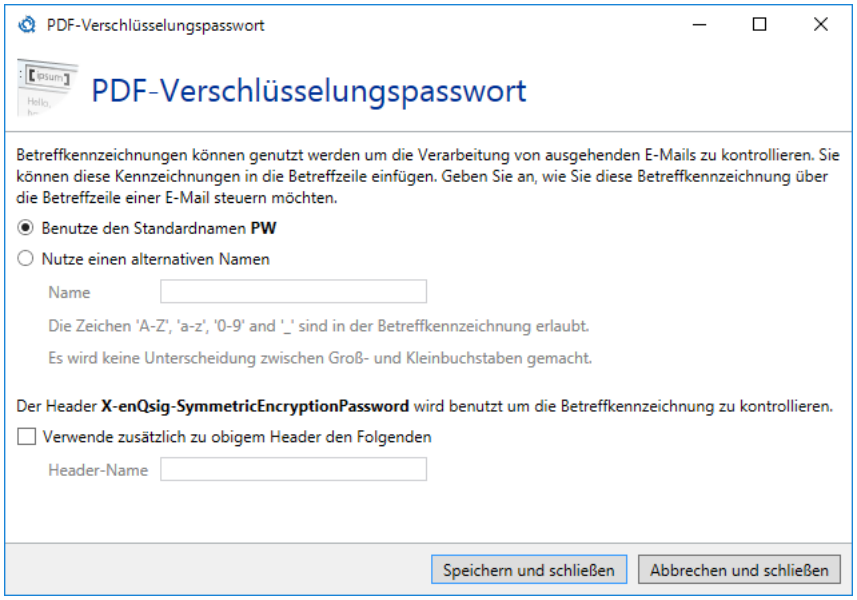


Bild 225: Betreffkennzeichnungen bearbeiten

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.

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 226).

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.

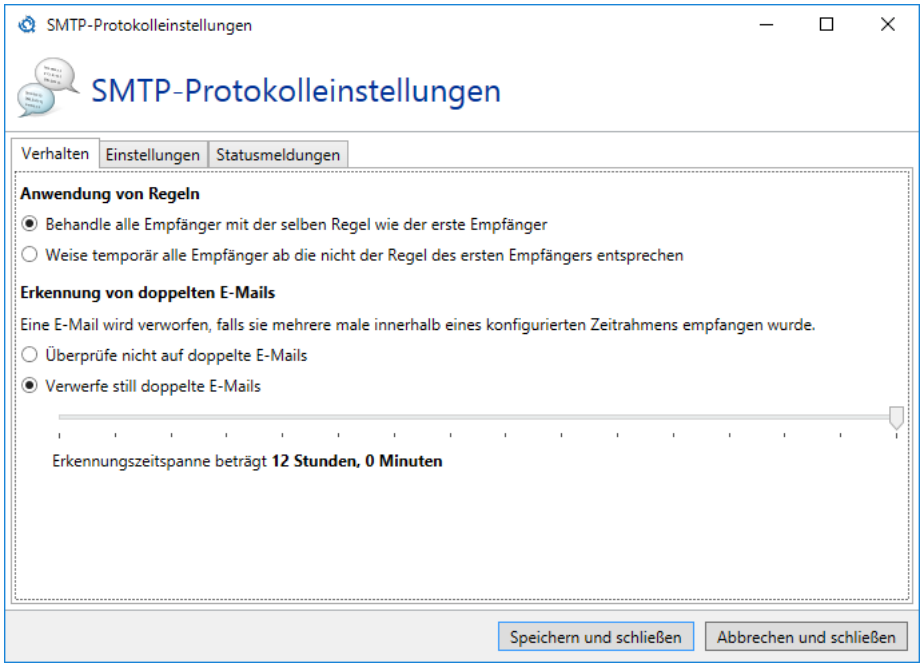


Bild 226: Verhalten beim Empfang von Nachrichten

Einstellungen

Das Anpassen der Timeouts (Bild 227) 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.

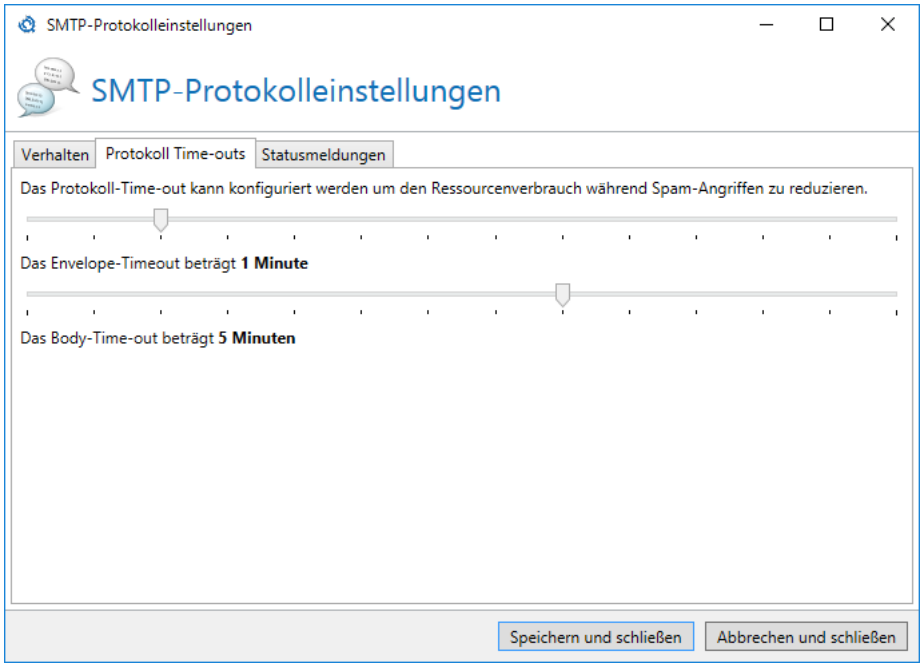


Bild 227: Timeouts

Statusmeldungen

Die Statusmeldungen (Bild 228) 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.

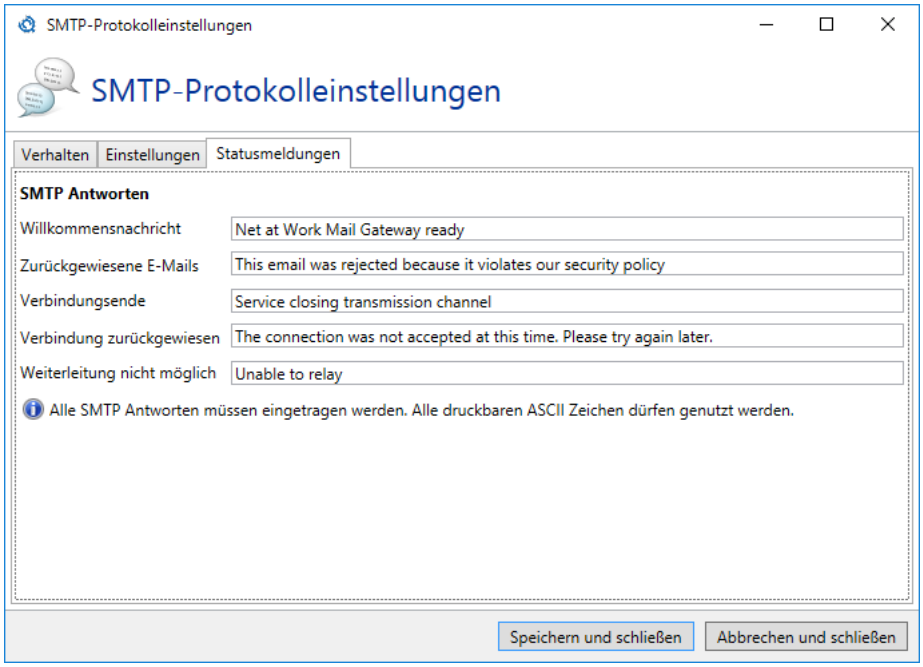


Bild 228: Textuelle SMTP-Statusmeldungen von NoSpamProxy an andere Server

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 229). 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.

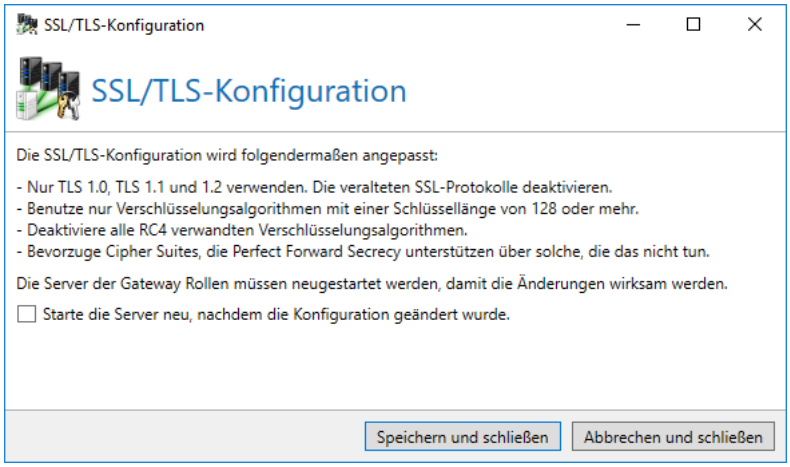


Bild 229: Empfohlene Einstellungen für die SSL/TLS-Konfiguration von Windows anwenden

Sie haben in diesem Bereich außerdem die Möglichkeit, die Standardwerte von Windows wiederherzustellen (Bild 230). Auch hier ist wieder ein Neustart des Servers notwendig, den Sie über den Dialog veranlassen können.

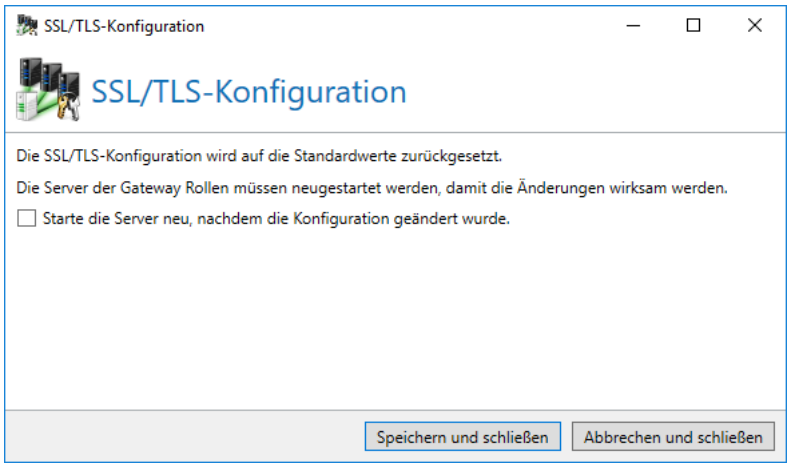


Bild 230: Auf Standardwerte für die SSL/TLS-Konfiguration zurückfallen

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 231). Das erneute Erstellen einer Datenbank kann notwendig werden, falls die alte Datenbank Schaden genommen hat.

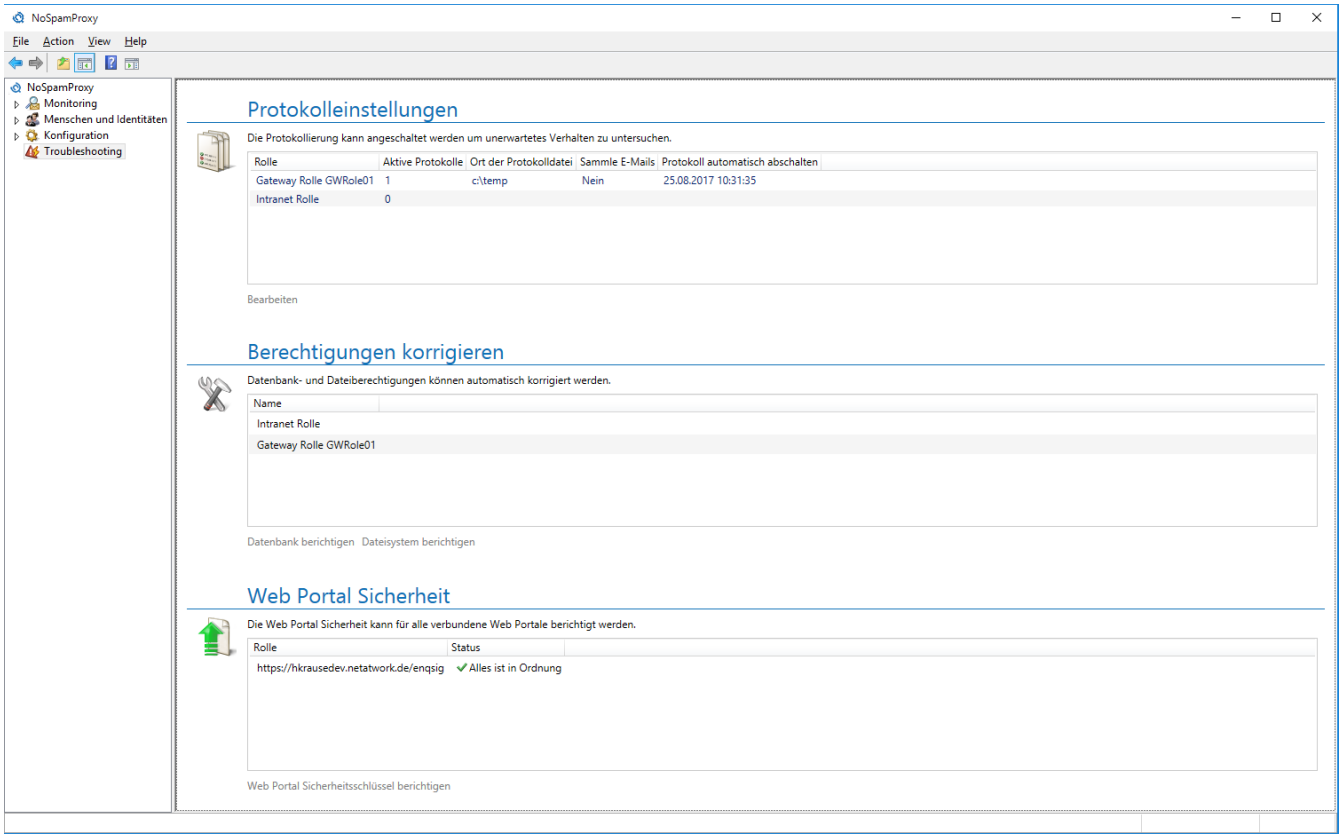


Bild 231: Werkzeuge für das Troubleshooting

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 232).

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.

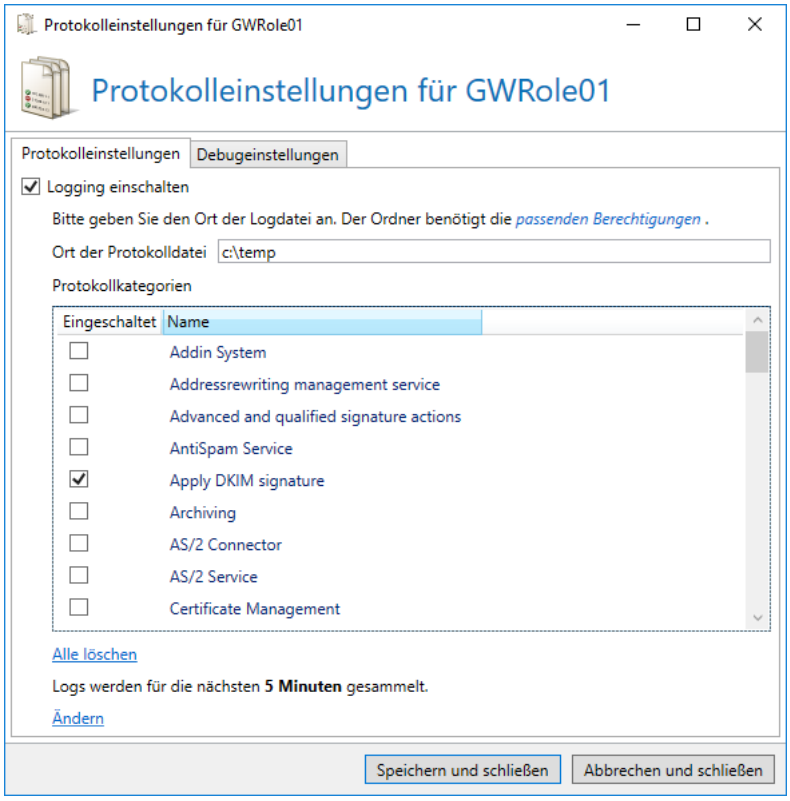


Bild 232: Konfigurieren Sie die Protokolleinstellungen

Zusätzlich ist es möglich, das Log auch nur für eine festgelegte Zeitspanne erstellen zu lassen (Bild 233). Nach dieser Zeit wird das Logging automatisch ausgeschaltet und Sie können die Logdateien für eine Analyse direkt benutzen.

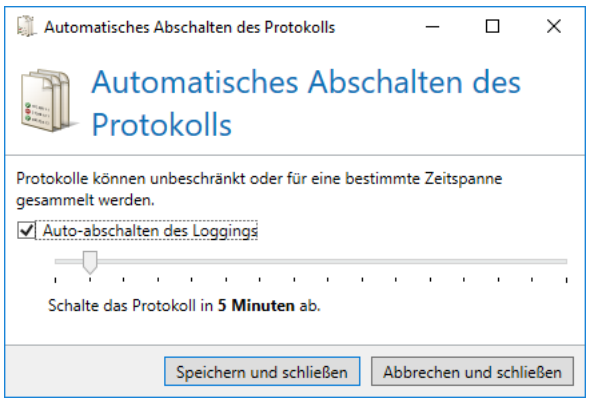


Bild 233: Automatisches Abschalten des Loggings

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 234). Dieser Reiter ist nur bei Gateway Rollen vorhanden. Auf der Intranet Rolle können Sie dies nicht konfigurieren.

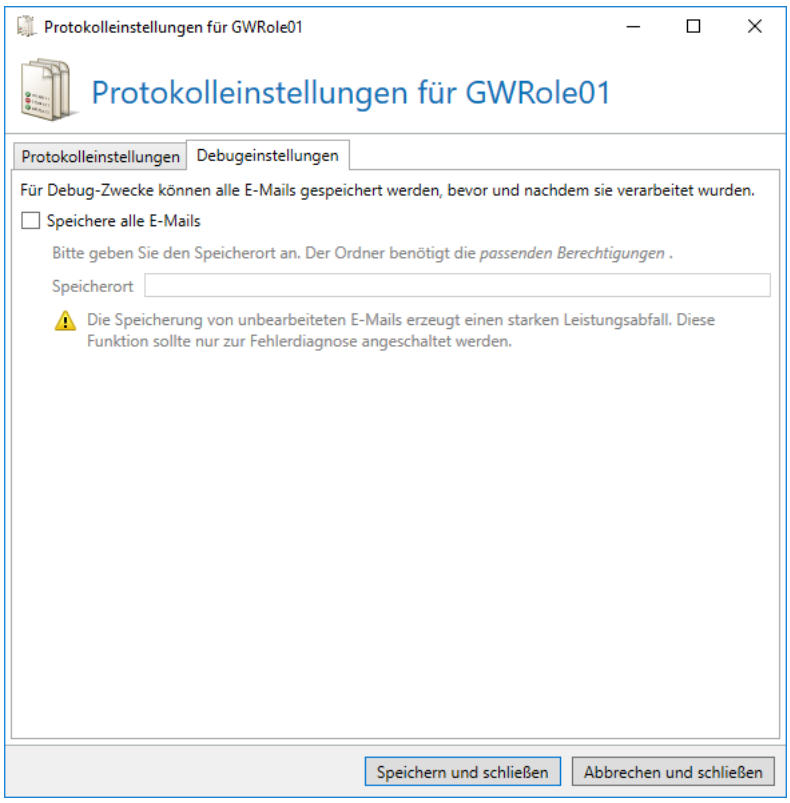


Bild 234: Speichern von E-Mails zur Fehlerdiagnose

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.

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 235) sowie auf der verwendeten Datenbank (Bild 236) korrigiert werden.

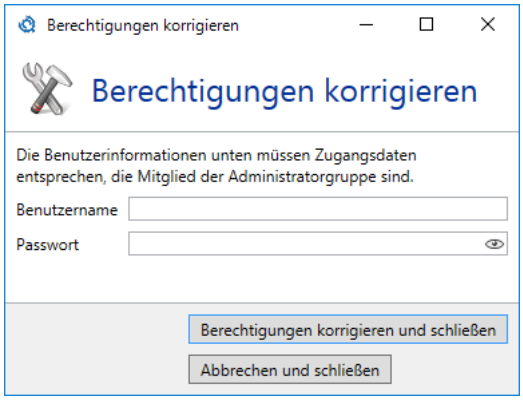


Bild 235: Lassen Sie Berechtigungen im Dateisystem korrigieren

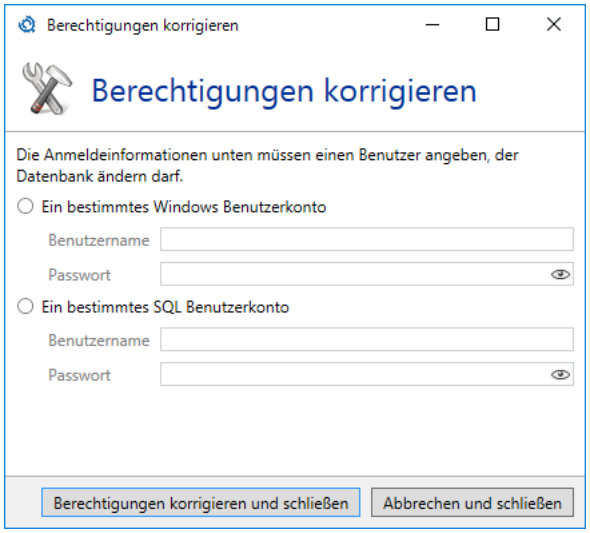


Bild 236: Lassen Sie Berechtigungen in der Datenbank korrigieren

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 stellt Ihren Kommunikationspartnern mehrere Funktionen zur Verfügung:

- Hinterlegung eines Kennworts für PDF Mail bei automatischer Verschlüsselung
- Sicheres Beantworten von PDF Mails ohne eigene Verschlüsselungsmöglichkeit des Beantwortenden
- Übertragung großer Dateien an interne und externe Benutzer

Hinterlegung eines Kennworts für PDF Mail

Haben Sie einem Kommunikationspartner eine E-Mail geschickt und dabei die Funktion "Autoverschlüsseln" verwendet, dann bekommt der Empfänger beim ersten Mal eine Aufforderung ein Kennwort zu hinterlegen. Erst nachdem er ein Konto auf dem Web Portal registriert hat, wird die eigentliche Nachricht zugestellt.

Wurde das Kennwort erfolgreich gespeichert, erscheint eine entsprechende Meldung. Die E-Mail des Absenders wird nun mit dem hinterlegten Kennwort verschlüsselt und zugestellt.

Beantworten von PDF Mails

Hat Ihr Kommunikationspartner eine PDF Mail erhalten, so kann er über das Web Portal dem Absender auf sichere Art und Weise eine Antwort zukommen lassen (Bild 237).

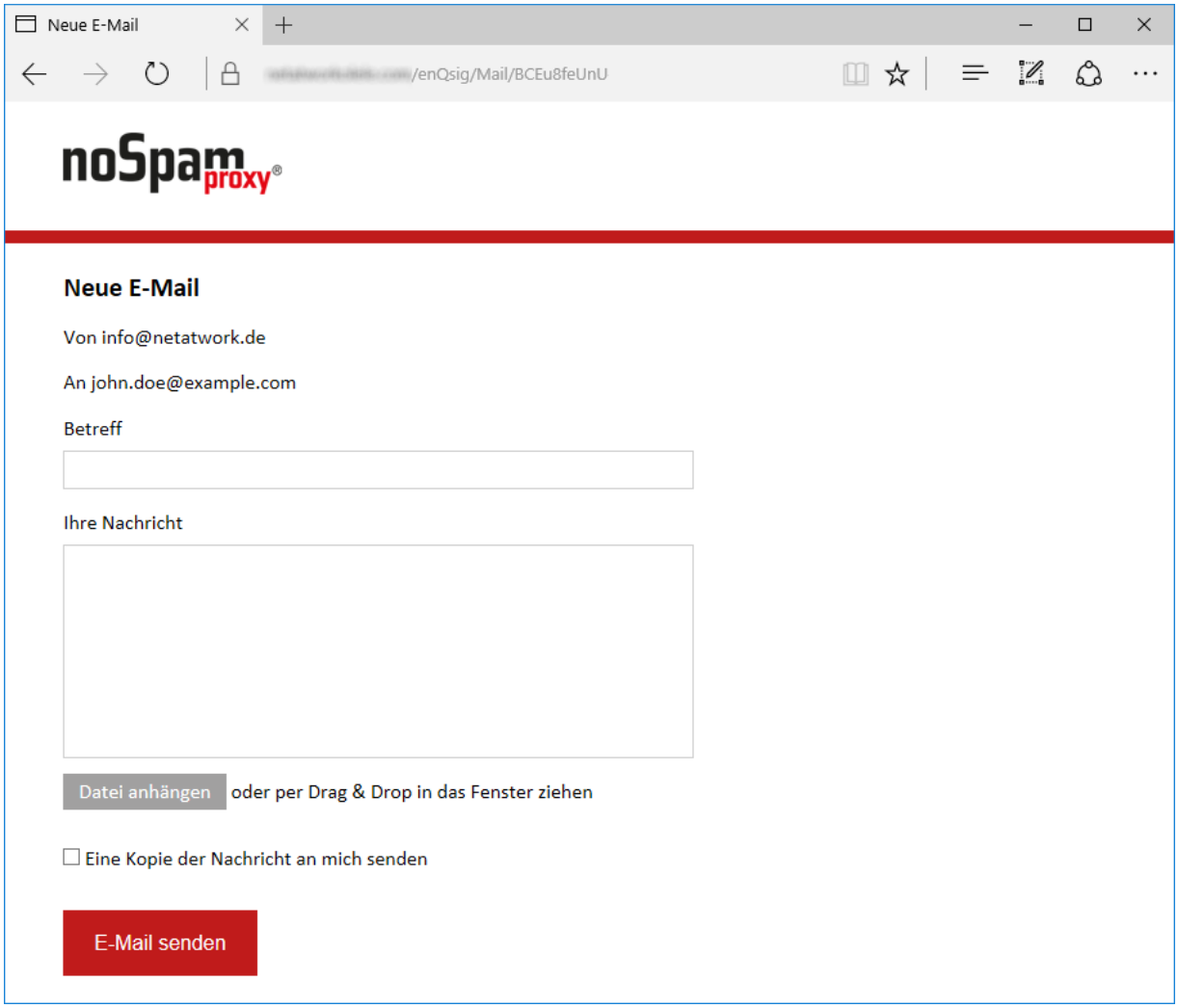


Bild 237: Sicher antworten über das Web Portal

Da es sich um eine Antwort handelt, sind Empfänger und Betreff festgelegt und können nicht geändert werden. Es ist dem Kommunikationspartner möglich, neben einem Antworttext eine oder mehrere Dateien anzuhängen. Wurde das Feature "Large Files" lizenziert, dann können beliebig große Dateien angehängt werden. Ansonsten können nicht mehr als 20 MB anhängt werden. Der Kommunikationspartner hat außerdem die Möglichkeit, sich eine Kopie der Nachricht zuschicken zu lassen. Diese wird dann wieder als PDF Mail zugestellt werden.

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.

Die Eingabemaske ist dieselbe wie beim Beantworten von PDF Mails. Allerdings sind die Größenbeschränkungen nun andere. Ein weiterer Unterschied besteht in der Funktion "Eine Kopie der Nachricht an mich senden". Die Antwort wird in diesem Fall nicht als PDF Mail zugestellt.

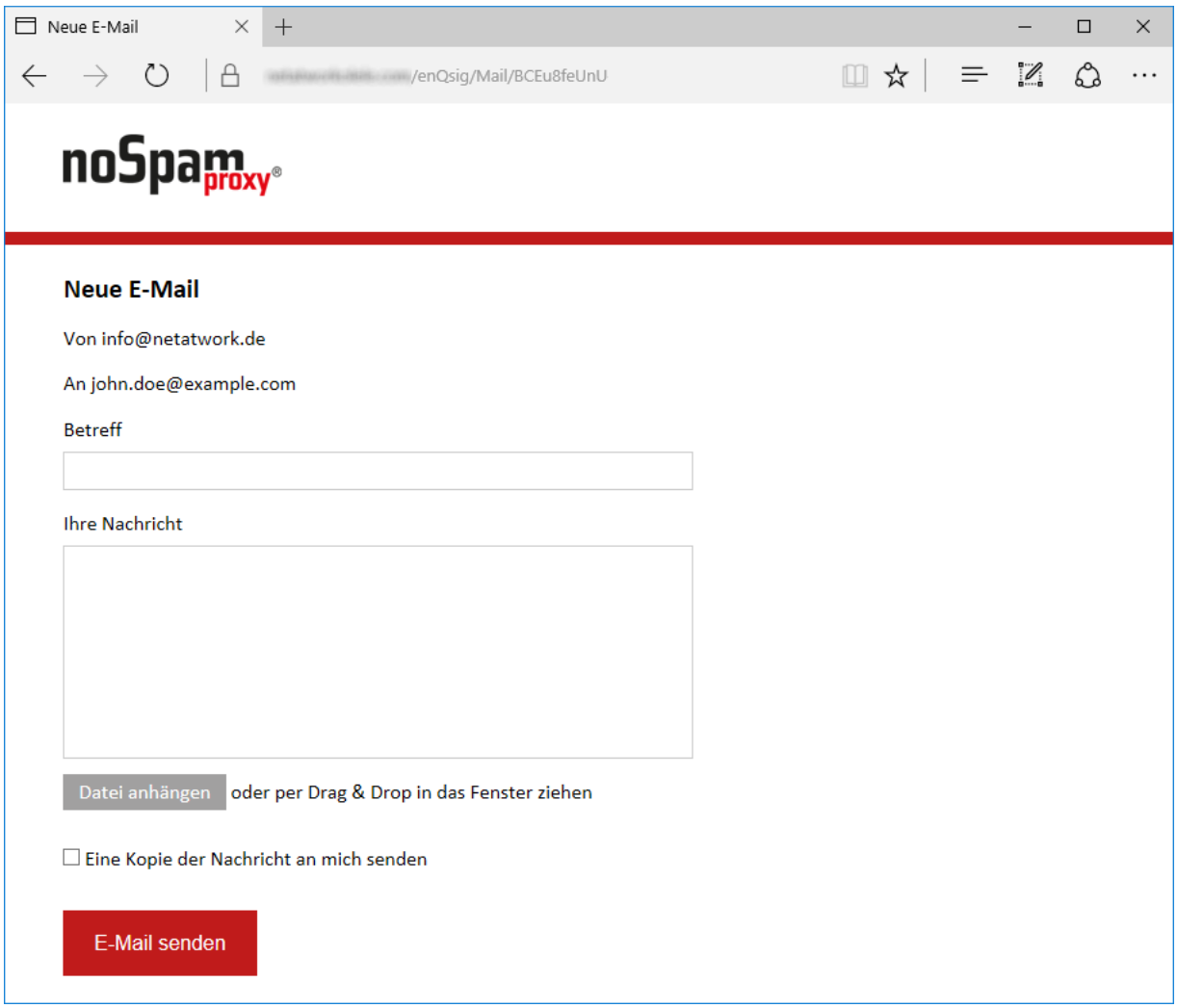


Bild 238: Dateien sicher übertragen über das Web Portal

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 239).

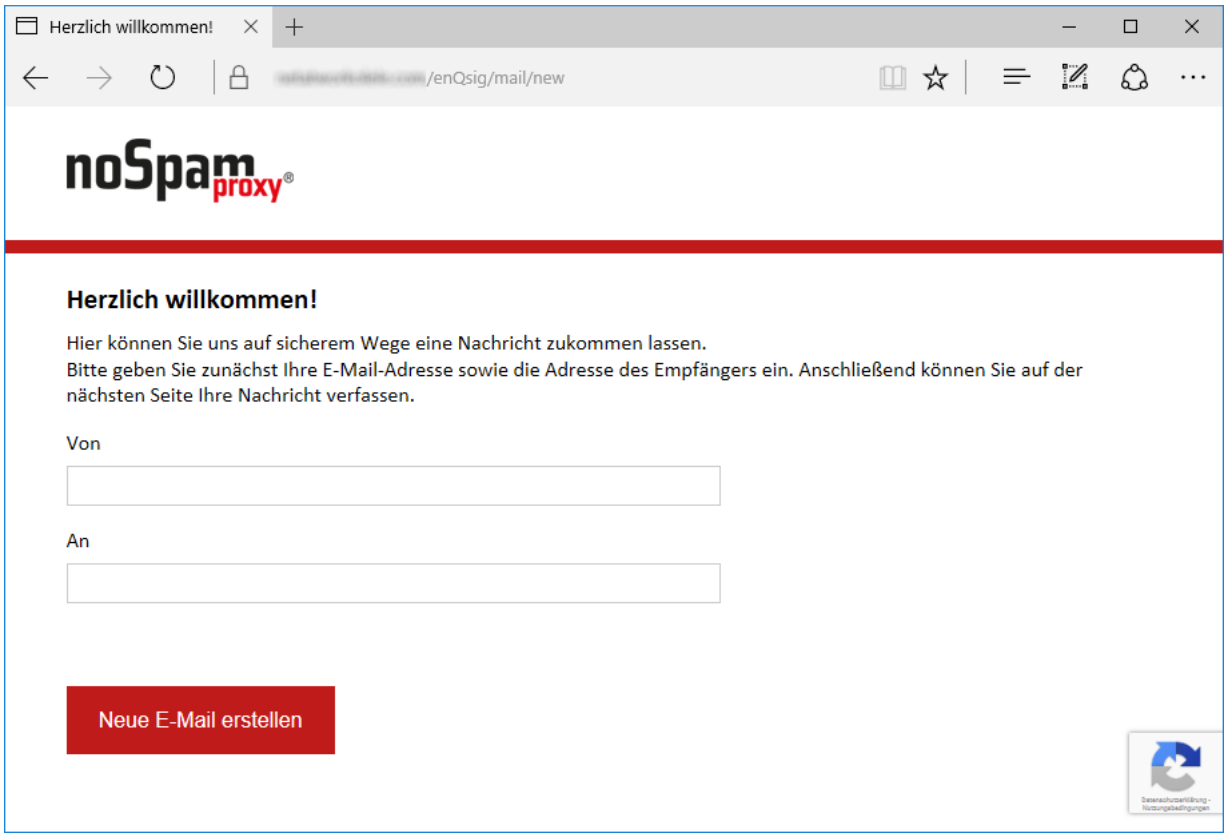


Bild 239: Maske für neue E-Mails ohne Einladungslink

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 240).

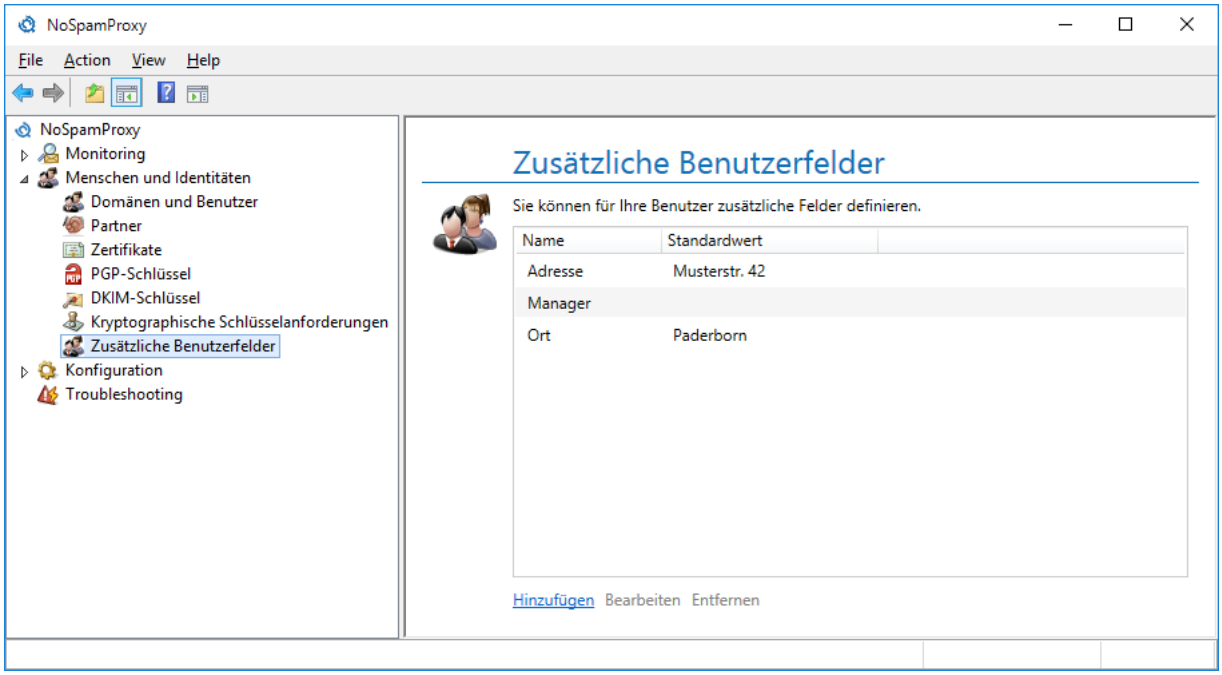


Bild 240: Die Übersicht über alle verfügbaren zusätzlichen Benutzerfelder

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 241).

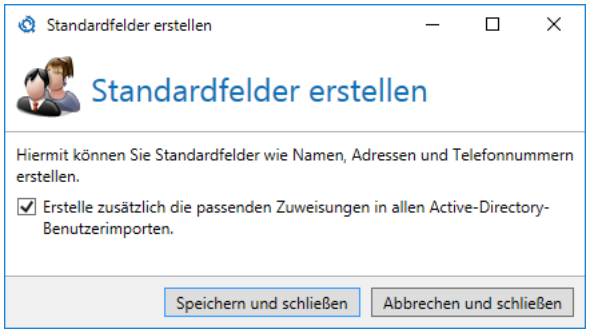


Bild 241: Das Erstellen von häufig genutzten Standardfeldern

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 242).

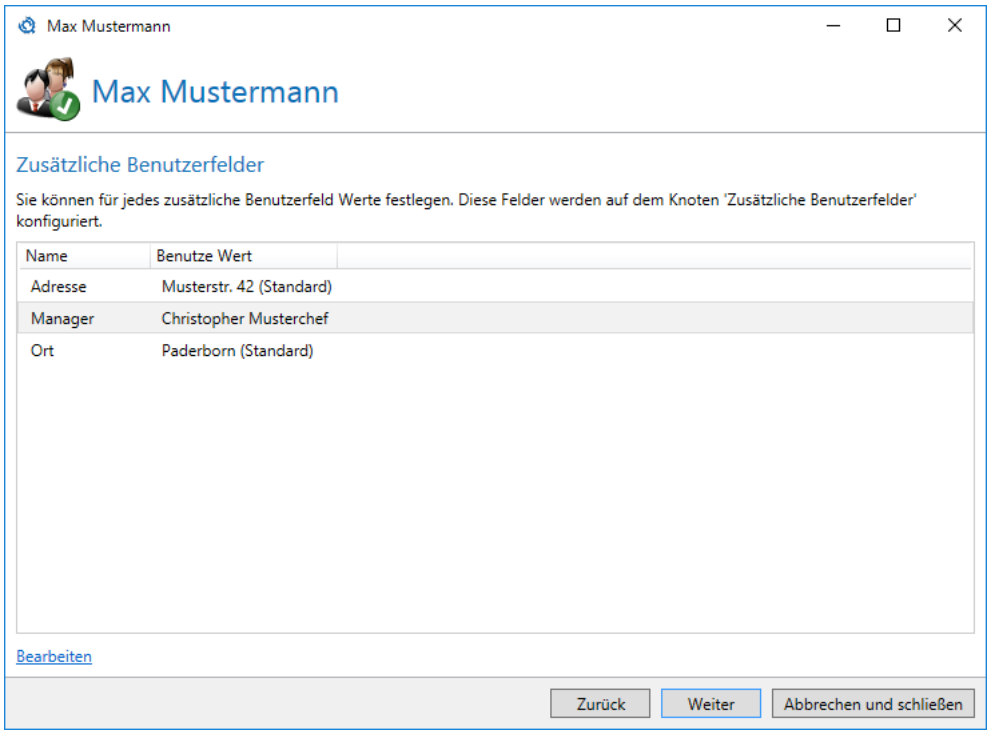


Bild 242: Zusätzliche Benutzerfelder

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 243).

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.

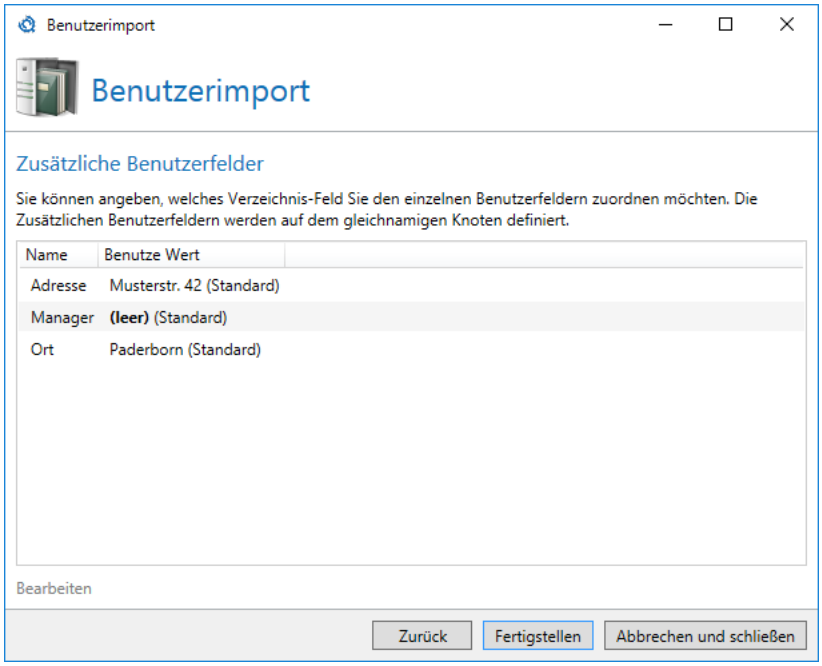


Bild 243: Konfiguration zusätzlicher Benutzerfelder

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 244). 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 244: 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 Passworten 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 Passworte 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 Verschlüsselungspasswörten der externen Partner verwendet.

Auswahl von Zertifikaten

Bei der Auswahl von Zertifikaten erscheint der Dialog mit dem Titel **Wählen Sie ein Zertifikat aus** (Bild 245).

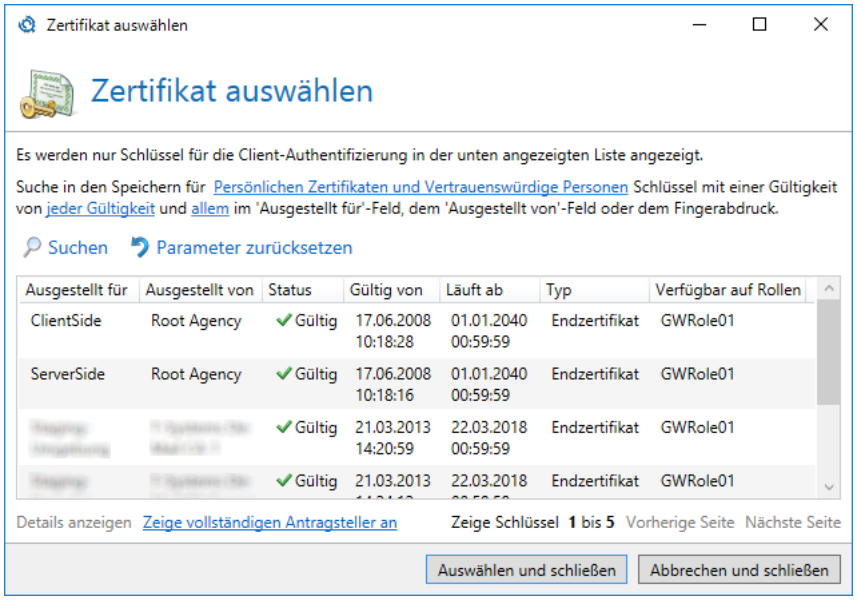


Bild 245: Die Liste der verfügbaren Zertifikate

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 Antragstellername 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 Kundenummer 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 246).

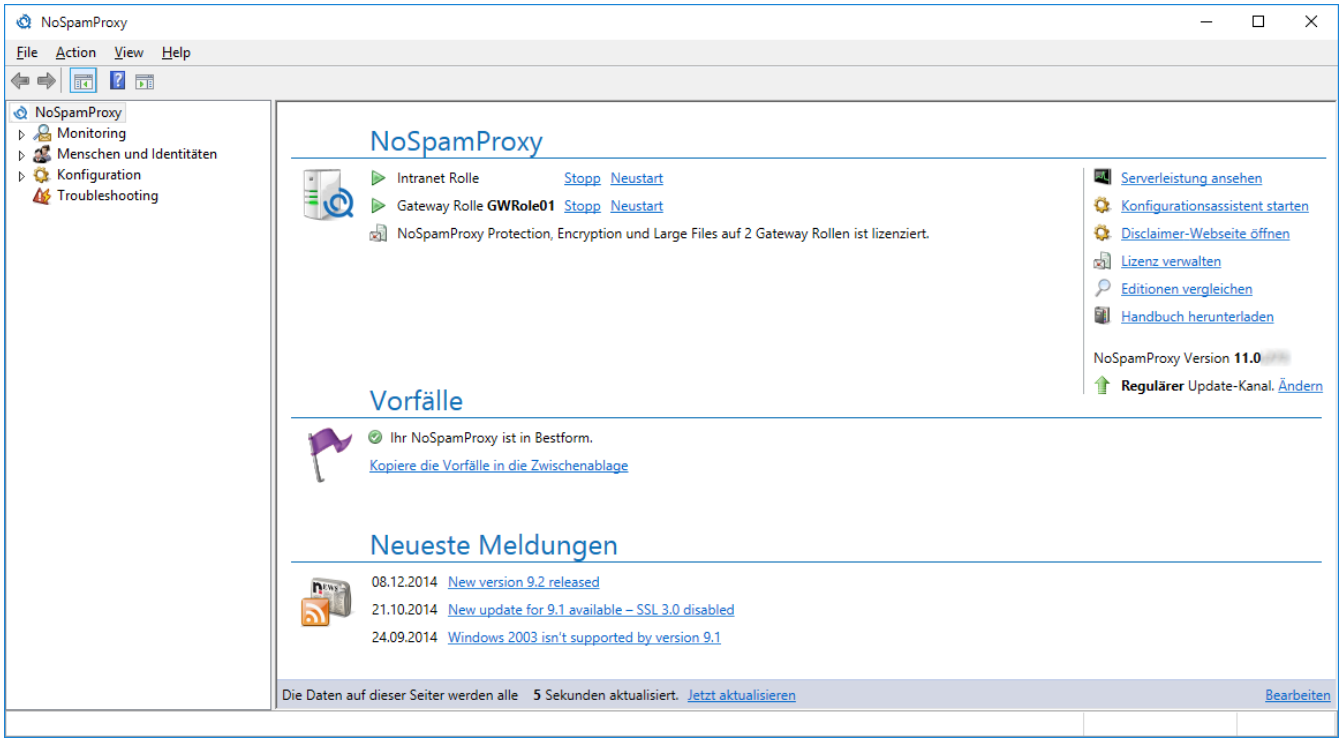


Bild 246: Die Übersicht zeigt eine vollständige Konfiguration von NoSpamProxy an

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 247). 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.

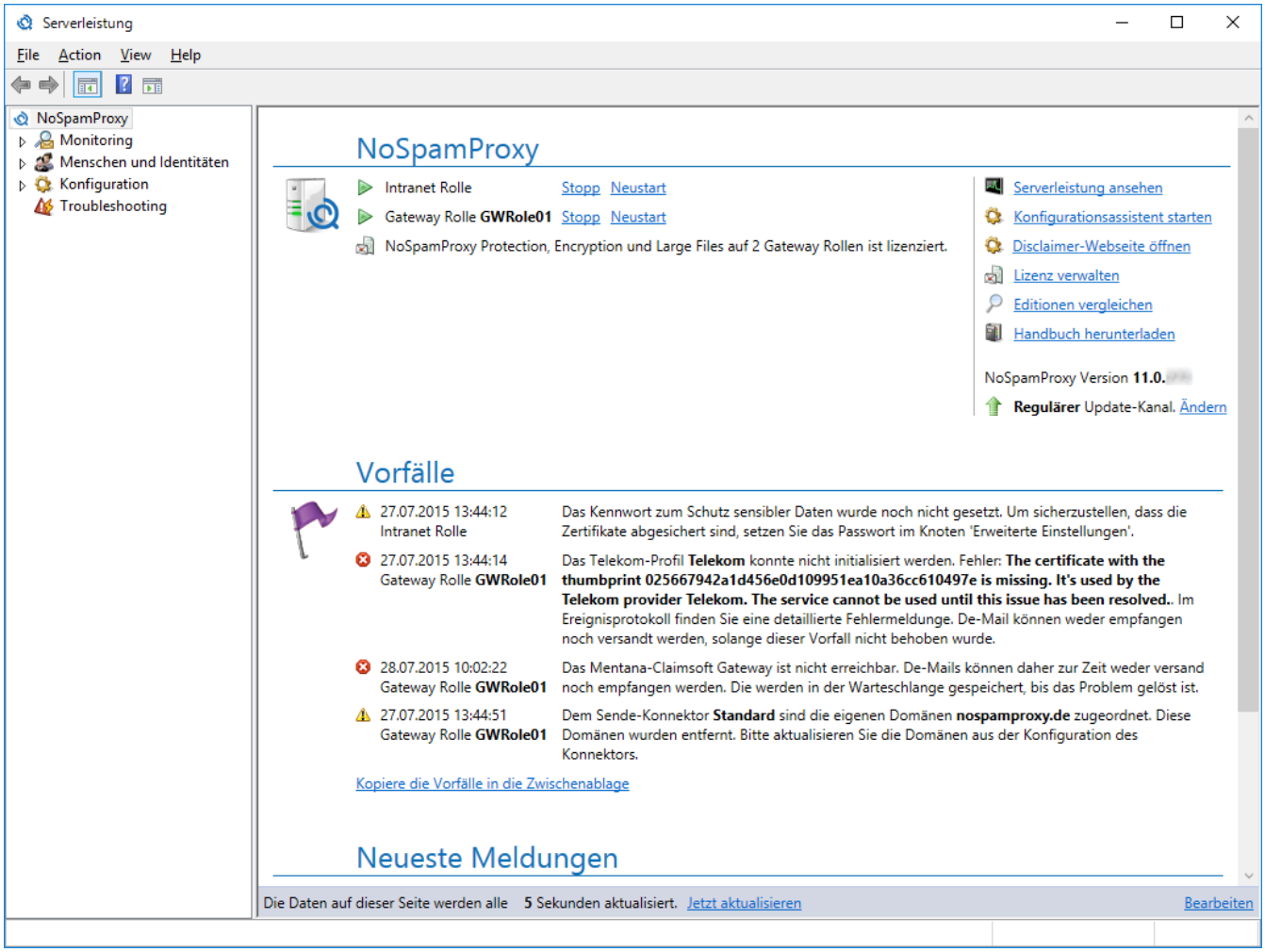


Bild 247: Fehler in den Konfigurationen von NoSpamProxy

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 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.

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 248). Wählen Sie in der Karteikarte **Erweitert** / **Advanced** die Schaltfläche **Umgebungsvariablen...** / **Environment Variables...**.

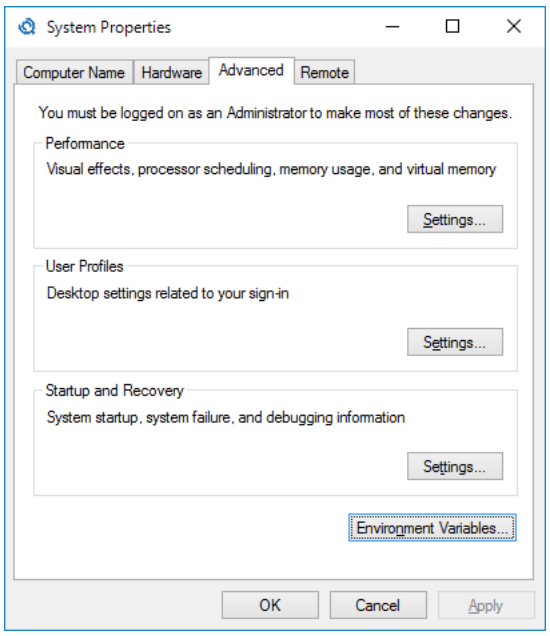


Bild 248: Die erweiterten Systemeinstellungen

Es öffnet sich das Fenster mit den 'Umgebungsvariablen' (Bild 249).

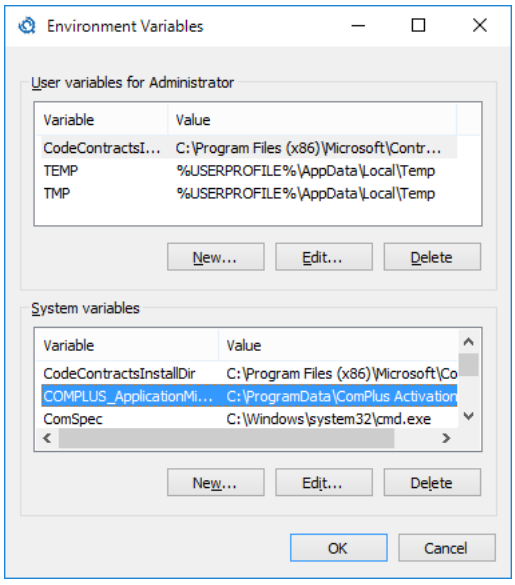


Bild 249: Die Umgebungsvariablen des Systems und des angemeldeten Benutzers

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 Zielserver 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