noSpam proxy® SERVER

Benutzerhandbuch

Suite

Version 14

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

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

DIESES DOKUMENT WURDE ZULETZT AM 27. NOVEMBER 2023 ÜBERARBEITET.

Inhalt

Die Benutzeroberfläche

NoSpamProxy wird über das NoSpamProxy Command Center verwaltet. Es ist folgendermaßen unterteilt:

- **Monitoring**| Dieser Bereich bietet eine Übersicht über den Empfang und die Zustellung von E-Mails. Zusätzlich können Sie die Ereignisanzeige von allen verbundenen Rollen einsehen.
- **Identitäten**| Dieser Bereich dient der grundlegenden Konfiguration von NoSpamProxy. Sie definieren Sende- und Empfangskonnektoren für E-Mails, Ihre Regeln und Benachrichtigungen sowie die Verbindungen zu Komponenten.
- **Konfiguration**| Dieser Bereich dient der grundlegenden Konfiguration von NoSpamProxy. Sie definieren Sende- und Empfangskonnektoren für E-Mails, Ihre Regeln und Benachrichtigungen sowie die Verbindungen zu Komponenten.
- **Troubleshooting**| Diesen Bereich nutzen Sie zur Diagnose. Sie erstellen Log-Dateien der einzelnen NoSpamProxy-Komponenten oder lassen Einstellungen automatisch korrigieren.

Aktionen auf der Übersichtsseite

In der linken unteren Ecke werden die verfügbaren Aktionen angezeigt.

Aktualisieren

Klicken Sie hier, um die auf der Übersichtsseite angezeigten Daten zu aktualisieren.

Konfigurationsassistent

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 Gatewayrolle| Wenn noch keine Gatewayrolle verbunden wurde, können Sie hier Ihre Gatewayrolle verbinden. Legen Sie nach dem Hinzufügen der Rolle den DNS Namen für die Server-Identität dieser Gatewayrolle fest.

Unternehmensdomänen| Konfiguration der Unternehmensdomänen. Falls das Gateway beim Ausführen des Assistenten noch keine Unternehmensdomänen eingetragen hat, wird in diesem Schritt die primäre Domäne der Lizenz in die Liste der Unternehmensdomänen 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. Siehe **Zertifikate und PGP-Schlüssel**.

Die Durchführung dieser Schritte stellt die Funktion von NoSpamProxy sicher.

Server ändern

Hier können Sie einen Server auswählen, auf den Sie per NCC zugreifen.

Sprachauswahl

Hier können Sie die Anzeigesprache ändern.

Weitere Verknüpfungen

Disclaimer-Website öffnen

Klicken Sie hier, um Vorlagen und Regeln für Ihre Disclaimer zu bearbeiten.

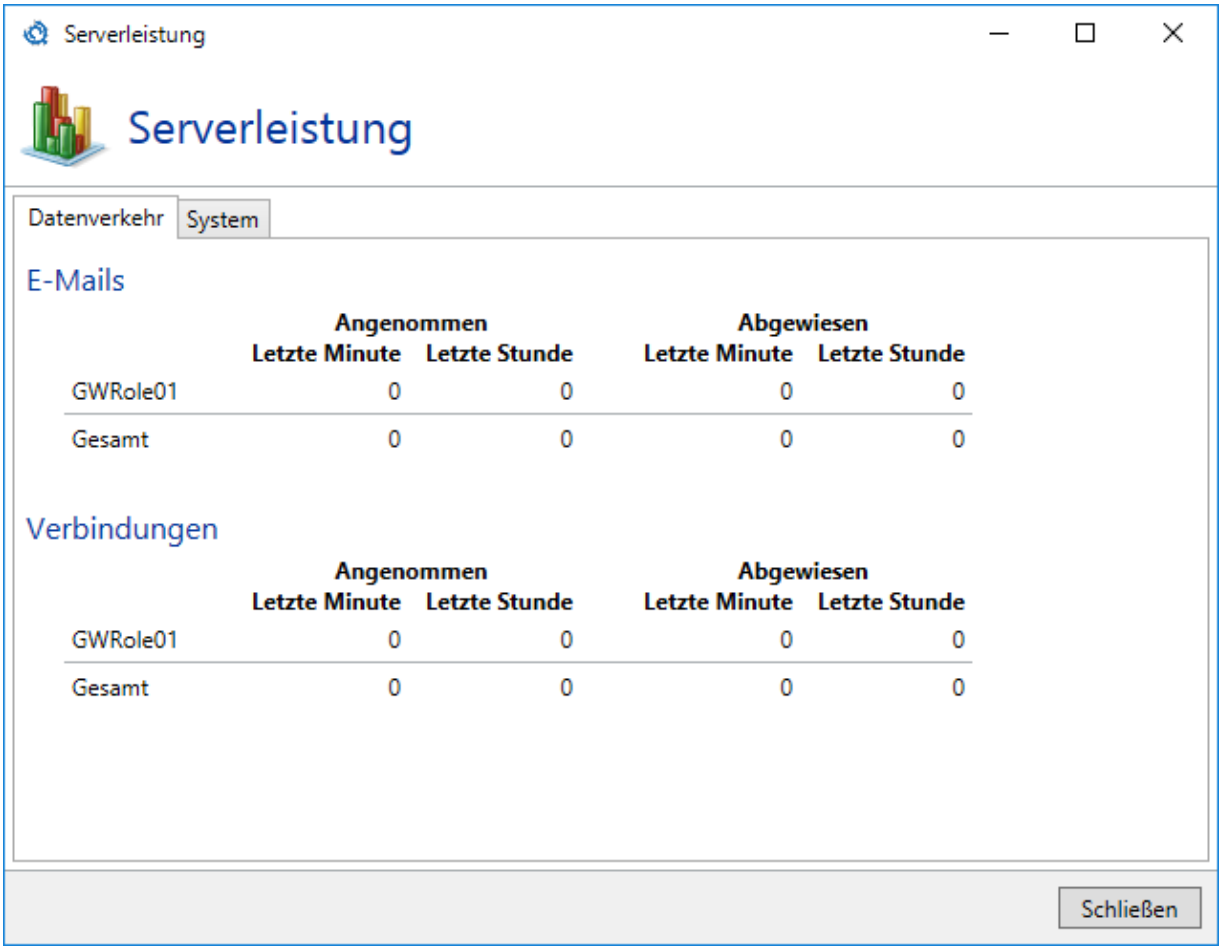
Dokumentation öffnen

Öffnet die NoSpamProxy-Dokumentation.

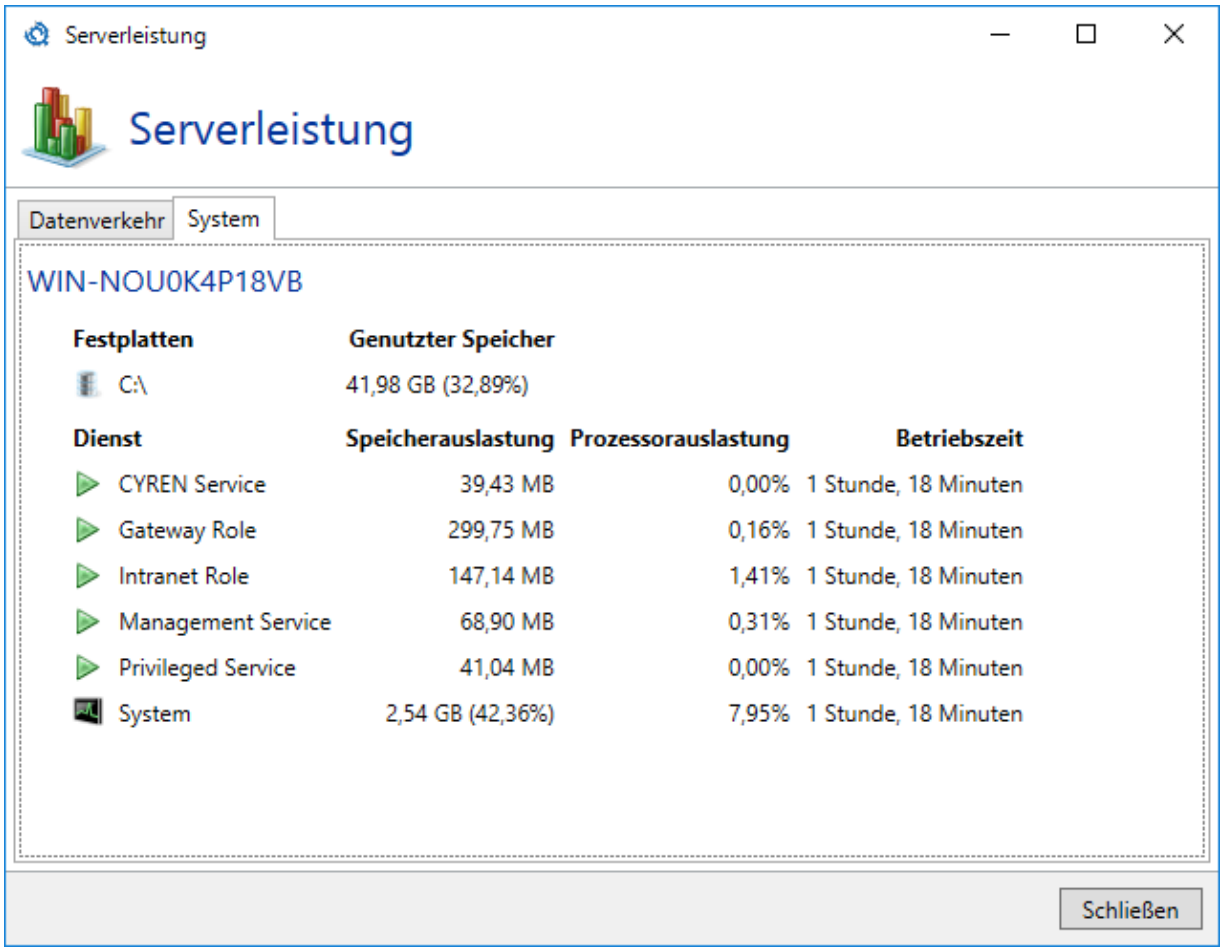
Serverleistung ansehen

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

Datenverkehr| Diese Registerkarte zeigt einen gleitenden Durchschnitt der verarbeiteten E-Mails der letzten Minute beziehungsweise Stunde. Die Seite wird automatisch aktualisiert und zeigt Ihnen zudem, ob NoSpamProxy aktuell E-Mails empfängt.



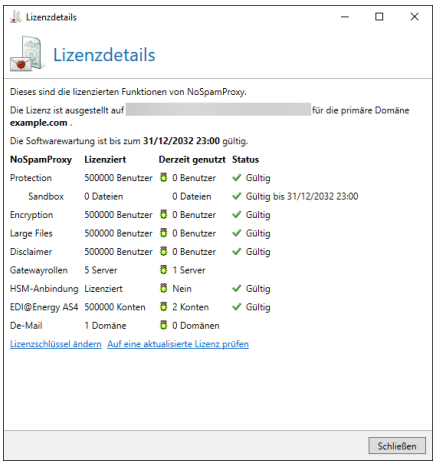
System| Diese Registerkarte zeigt für jedes System mit Intranet- oder Gatewayrollen die installierten Dienste, deren Status und die verwendeten Ressourcen.



Zusätzlich zu dieser Ansicht stehen Ihnen auf dem Server außerdem die Leistungsindikatoren zur Verfügung.

Lizenz verwalten

Diese 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.



Sie sehen hier Ihre C-Nummer, Domäne sowie alle lizenzierten Funktionen und deren Gültigkeitszeitraum.

Lizenzschlüssel ändern 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.

Auf eine aktualisierte Lizenz prüfen| Prüfen, ob Änderungen an der aktiven Lizenz vorliegen.

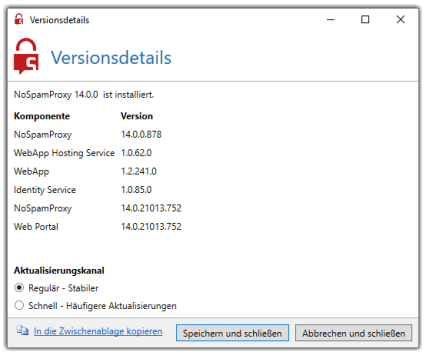
Auswahl des Aktualisierungskanals

- Klicken Sie auf die angezeigte Versionsnummer, um Details zur Version Ihrer NoSpamProxy-Instanz anzuzeigen und den Release-Kanal zu ändern.

Updates für NoSpamProxy werden über zwei Kanäle angeboten:

Regulärer Kanal| Der reguläre Kanal ist die Standardeinstellung und bietet Aktualisierungen an, die bereits lange getestet wurden und die höchste Stabilität für NoSpamProxy erreichen.

Schneller Kanal| 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.



> **HINWEIS:** 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.

Monitoring

Dieser Bereich bietet Ihnen Zugriff auf alle Informationen zu Empfang und Versand Ihrer E-Mails. Er enthält auch Statusinformationen bezüglich System und E-Mail-Verkehr.

Nachrichtenverfolgung

Dieser Bereich zeigt detaillierte Informationen über die Verarbeitung von E-Mails an. Sie können einsehen, welche E-Mails geblockt oder durchgelassen wurden sowie das Vorgehen von NoSpamProxy® und das Funktionieren der Regeln nachvollziehen.

> **TIPP:** Die NoSpamProxy Web App bietet zusätzliche Suchoptionen für die Nachrichtenverfolgung. Siehe **Nachrichtenverfolgung (Web App)**.

Nachrichtenverfolgung aktivieren

1. Gehen Sie zu **Konfiguration > Erweiterte Einstellungen > Monitoring**.
2. Klicken Sie **Bearbeiten**.
3. Aktivieren Sie die Option **Nachrichtenverfolgungsdatensätze erfassen** auf der Registerkarte **Nachrichtenverfolgung**.
4. Konfigurieren Sie die folgenden Optionen:
   - **Speichere die Zusammenfassungen|** Der Zeitraum, für den Sie E-Mails zurückverfolgen können. 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.
   - **Speichere die Details|** Die Vorhaltezeit für die dazu gehörenden Nachrichtendetails. In den Details 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.

- **URL Safeguard**| Der Zeitraum, für den die Besuche der Ziele von URLs gespeichert werden.
- **Speichere die Statistiken**| Der Zeitraum, für den Sie Reports erstellen können. Um einen aussagekräftigen Report erstellen zu können, empfehlen wir eine Mindestaufbewahrungsfrist von 12 Monaten.

5. Konfigurieren Sie auf der Registerkarte **Angehaltene E-Mails** den Aufbewahrungszeitraum für E-Mails, für die auf einen Verschlüsselungsschlüssel gewartet wird.
6. Klicken Sie **Speichern und schließen**.

Suchergebnisse filtern

Sie können die folgenden Suchkriterien einzeln oder kombiniert anwenden, um die Ergebnisse zu filtern.

Versandzeitraum| Durch die Auswahl unter Zeiträume können oft benötigte Suchen schnell gewählt werden.

> **HINWEIS:** Ein Zeitraum muss in jedem Fall angegeben werden. Standardmäßig wird die Startzeit auf die aktuelle Systemzeit - 1 Stunde und die Endzeit auf den aktuellen Tag um 23:59 Uhr gesetzt.

- **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**| Die interne Kennung der E-Mail.
- **Zustellergebnisse**| Der Status der Zustellung.
- **SCL-Wert**| Das errechnete Spam Confidence Level.
- **Regel**| Der Name der Regel, von der die Nachricht verarbeitet wurde.

> **TIPP:** Bei der Eingabe von Text können Sie immer den gesamten zu suchenden Text oder nur Teile davon eingeben.

Die Ergebnisse der Suche sind nach Datum aufsteigend sortiert.

Details zur Verarbeitung einer E-Mail anzeigen

Die Details enthalten Informationen zum Zustellstatus sowie zur Signierung beziehungsweise Verschlüsselung einer E-Mail.

1. Rechtsklicken Sie den Datensatz, dessen Details Sie einsehen möchten.
2. Klicken Sie auf **Details**.

oder

- Doppelklicken Sie den Datensatz.

Sie können hier alle Bearbeitungsschritte und Details einsehen, die vom Start bis zum Schließen der Verbindung für den entsprechenden Datensatz verfügbar sind, unter anderem:

- Verbindungsverschlüsselung
- Vom SMTP-Server beziehungsweise SMTP-Client verwendete Zertifikate
- Filterergebnisse
- Generelle Verarbeitungsfehler von NoSpamProxy
- Die Registerkarte **Überprüfung** zeigt unter anderem Details zur Validierung der E-Mail, zur Berechnung des Spam Confidence Level für die Level-of-Trust-Bewertung sowie zu den auf der E-Mail ausgeführten Filter und Aktionen.
- Die Registerkarte **URL Safeguard** enthält Informationen zu URLs, die durch den URL Safeguard verändert wurden.

Datensätze exportieren oder importieren

Sie können die Datensätze der Nachrichtenverfolgung als CSV-Datei auf Ihrer lokalen Festplatte abspeichern oder abgespeicherte Datensätze wieder mit allen Details anzeigen. Diese Funktion ist hilfreich, falls Sie Unterstützung bei der Analyse eines Datensatzes benötigen.

- Zum Exportieren klicken Sie **Nachrichtenverfolgung exportieren** in der linken unteren Ecke des Detaildialogs.
- Zum Anzeigen klicken Sie **Nachrichtenverfolgungsdatei laden** in der Liste aller gefundenen Datensätze.

Fehlklassifizierung melden

Sollten E-Mails fälschlicherweise als sicher beziehungsweise bösartig bewertet worden sein, können Sie diese an unsere cloudbasierten NoSpamProxy-Dienste melden.

Gehen Sie folgendermaßen vor:

- Klicken Sie **Fehlklassifizierung melden** unterhalb des Detaildialogs.

Die gemeldeten Fehlklassifizierungen werden genutzt, um die Erkennung durch 32Guards und durch die Core Antispam Engine zu verbessern.

Hinweise

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

HINWEIS: Um die Datenbankgröße der Nachrichtenverfolgung und der Reports nicht unkontrolliert wachsen zu lassen, räumt die Intranetrolle die Datenbank in einem regelmäßigen Intervall auf. Dabei werden alle Elemente, die ein vorgegebenes Alter überschritten haben, aus der Datenbank gelöscht.

HINWEIS: Wenn alle Nachrichtenverfolgungsdatensätze und die statistischen Daten verworfen werden sollen, wählen Sie bitte die Option **Nachrichtenverfolgung vollständig abschalten** unter dem **Erweiterte Einstellungen** der Gatewayrolle. In diesem Fall werden keinerlei 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.

HINWEIS: 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 kürzere Aufbewahrungsfristen der Nachrichtenverfolgungsdatensätze gewählt werden oder eine SQL-Server-Datenbank ohne diese Beschränkung installiert werden.

Nachrichtenverfolgung (Web App)

Die Web App bietet über ein webbasiertes Interface weitere Funktionen, beispielsweise zusätzliche Suchoptionen für die Nachrichtenverfolgung.

Monitoring

Übersicht

Unter **Monitoring > Nachrichtenverfolgung** finden Sie neben allgemeinen Informationen auch Informationen zum Nachrichtenfluss sowie zur Signierung und Verschlüsselung.

Verwendete Icons

| Die E-Mail wurde verschlüsselt übertragen.

| Die E-Mail wurde teilweise verschlüsselt übertragen.

| Die E-Mail wurde signiert.

| Die E-Mail wurde teilweise signiert.

| Die Signatur ist beschädigt.

| Die Verschlüsselung ist beschädigt.

| Die E-Mail wurde aus dem Internet empfangen.

| Die E-Mail wurde von einem E-Mail-Server des Unternehmens gesendet.

> **TIPP:** Eine Auflistung der Icons finden Sie auch unter **Legende** in der Übersicht der Nachrichtenverfolgung.

Spalten umsortieren

Um die Reihenfolge der angezeigten Spalten zu ändern, ziehen Sie die jeweilige Spalte und legen Sie diese am gewünschten Platz ab.

E-Mails filtern

Bedingungen hinzufügen

1. Klicken Sie **Bedingung hinzufügen** in der linken oberen Ecke der Nachrichtenverfolgung.

2. Wählen und konfigurieren eine oder mehrere Bedingungen.
3. Klicken Sie **Suchen**, um die Abfrage auszuführen.

Um eine Bedingung zu entfernen, klicken Sie **Bedingung entfernen** neben der jeweiligen Bedingung.

Suchen speichern

Um eine von Ihnen konfigurierte Suche nicht jedes Mal neu erstellen zu müssen, können Sie diese speichern. Im Drop-Down-Menü **Gespeicherte Suchen** können Sie diese dann auswählen.

- Klicken Sie nach dem Konfigurieren der Abfrage unter **Gespeicherte Suchen** auf **Aktuelle Suche hinzufügen**, um Sie zu speichern.

Suchen als Standard speichern

Standardsuchen werden bei jedem Öffnen der Nachrichtenverfolgung ausgeführt.

- Markieren Sie im Drop-Down-Menü **Gespeicherte Suchen** die gewünschte Suche mit 💙, um diese als Standardsuche zu speichern.

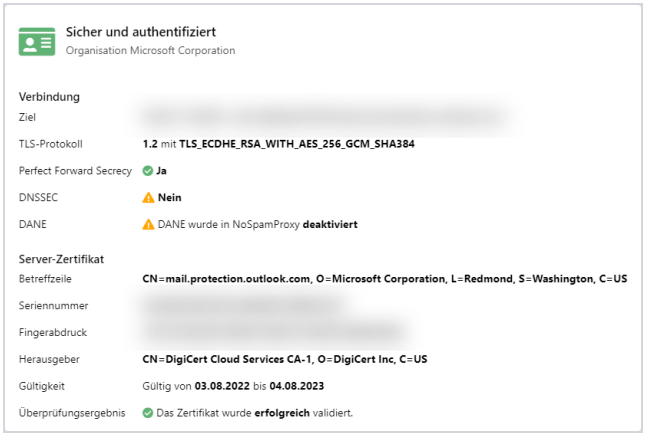
Details zu einer E-Mail anzeigen

- Klicken Sie die E-Mail, deren Details Sie anzeigen wollen. Die Detailansicht der jeweiligen E-Mail öffnet sich.
- Klicken Sie in der Detailansicht auf der Registerkarte **Allgemein** das Icon ⧉, um die Detailansicht in einem neuen Tab zu öffnen.
- Klicken Sie **Nachrichtenverfolgungsdatensatz herunterladen**, um den Datensatz als json-Datei auf Ihrem Computer zu speichern.

Registerkarte Allgemein

Hier finden Sie allgemeine Informationen zur E-Mail und deren Anhängen sowie zur Verbindung und Übertragung.

- Zur Ermittlung des Servernamens wird auf Basis der IP-Adresse ein Reverse DNS Lookup ausgeführt.
- Durch Klicken auf die Absendeadresse können Sie sowohl die MAIL FROM- als auch die Header-From-Adresse anzeigen lassen (sofern diese unterschiedlich sind).
- Durch Klicken auf die Empfängeradresse können Sie sämtliche Empfänger anzeigen lassen.
- Durch Klicken auf den Namen des TLS-Serverzertifikats können Sie Details zur Verbindungsverschlüsselung einsehen:



Für bestimmte E-Mails kann eine Aktion des Administrators erforderlich sein. Klicken Sie in diesem Fall **Aktion erforderlich**, um weitere Informationen und Optionen anzuzeigen:

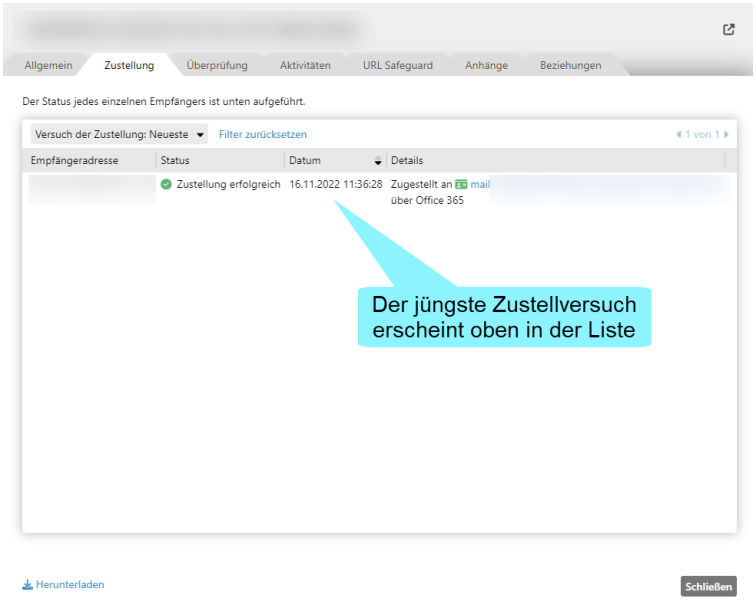
Angehaltene E-Mails| Die E-Mail wurde für mindestens einen Empfänger angehalten. Siehe **Angehaltene E-Mails**.

Gesperrte Anhänge| Mindestens ein Anhang erfordert eine Freigabe durch den Administrator.

> **TIPP:** Informationen zu den einzelnen Status-Typen finden Sie unter **Status-Typen**.

Registerkarte Zustellung

Hier finden Sie Informationen zu den einzelnen Zustellversuchen.

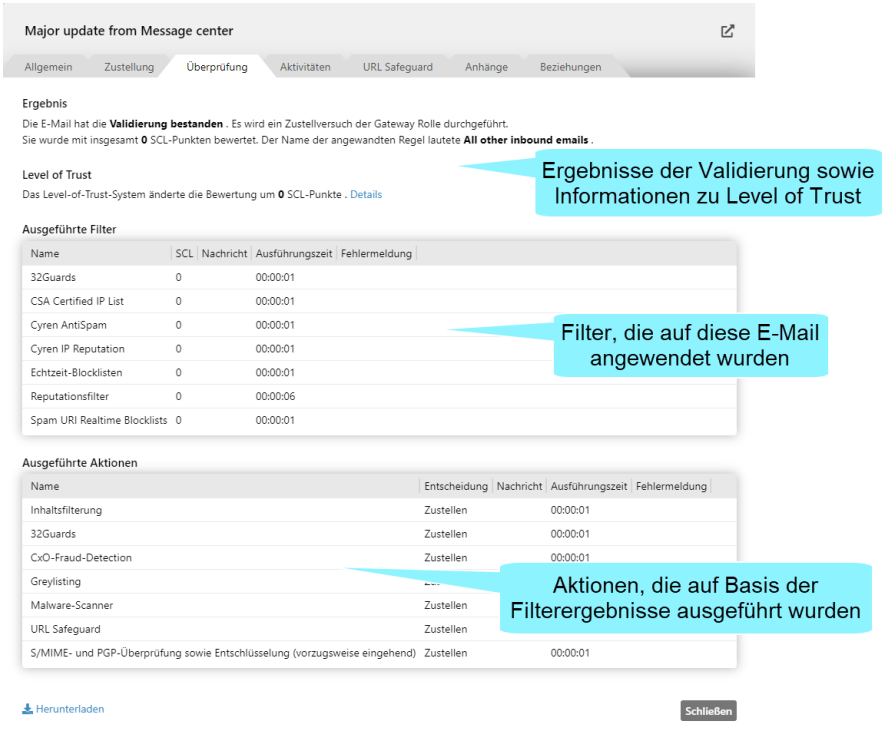


- Sollten initial nicht alle Zustellversuche für die einzelnen Empfänger angezeigt werden, klicken Sie **Alle anzeigen**, um sämtliche Zustellversuche anzuzeigen.

Registerkarte Überprüfung

Hier finden Sie Informationen zur Validierung sowie zu angewandten Filtern und ausgeführten Aktionen.

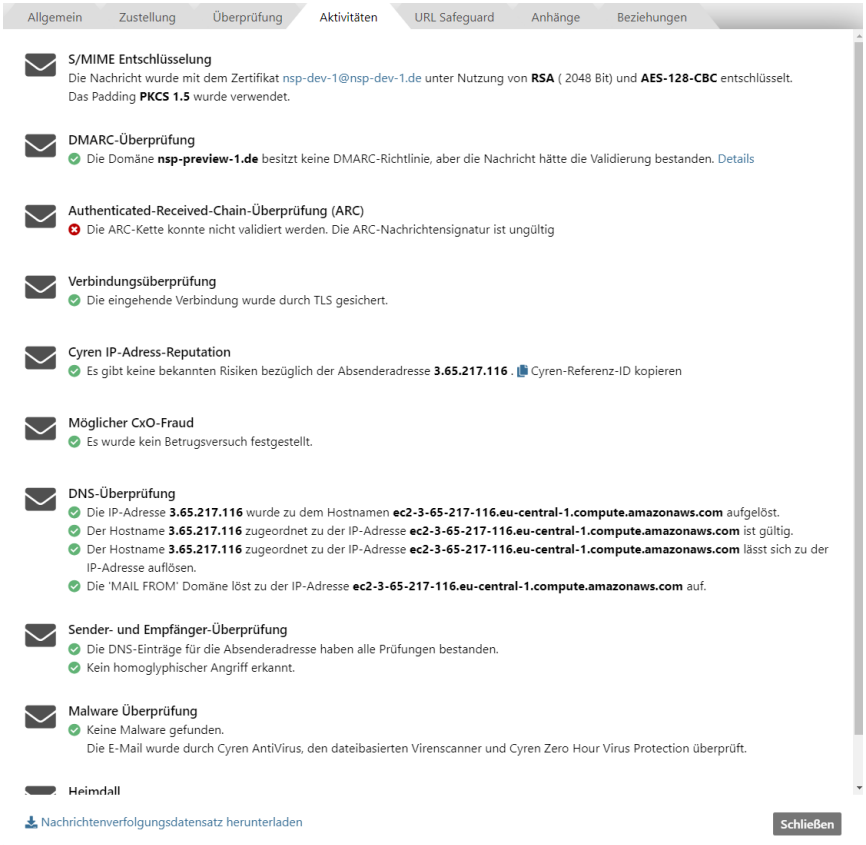
> **HINWEIS:** Einträge in den Listen **Ausgeführte Filter** und **Ausgeführte Aktionen** sind nach **Fehlermeldung (absteigend) > SCL (absteigend) > Name (aufsteigend)** sortiert.



Registerkarte Aktivitäten

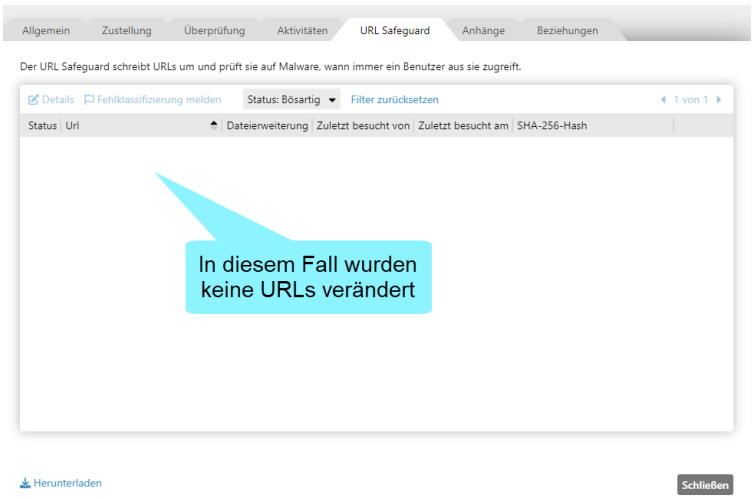
Hier finden Sie Informationen darüber, wie die E-Mail auf dem Server verarbeitet wurde. Dies sind beispielsweise Details zur angewandten Verschlüsselung, zur Reputationsprüfung sowie zum Einsatz von Content Disarm and Reconstruction oder PDF Mail.

Außerdem enthält diese Registerkarte Angaben zu den Konsequenzen, die sich aus den Ergebnissen bestimmter Prüfungen ergeben haben.



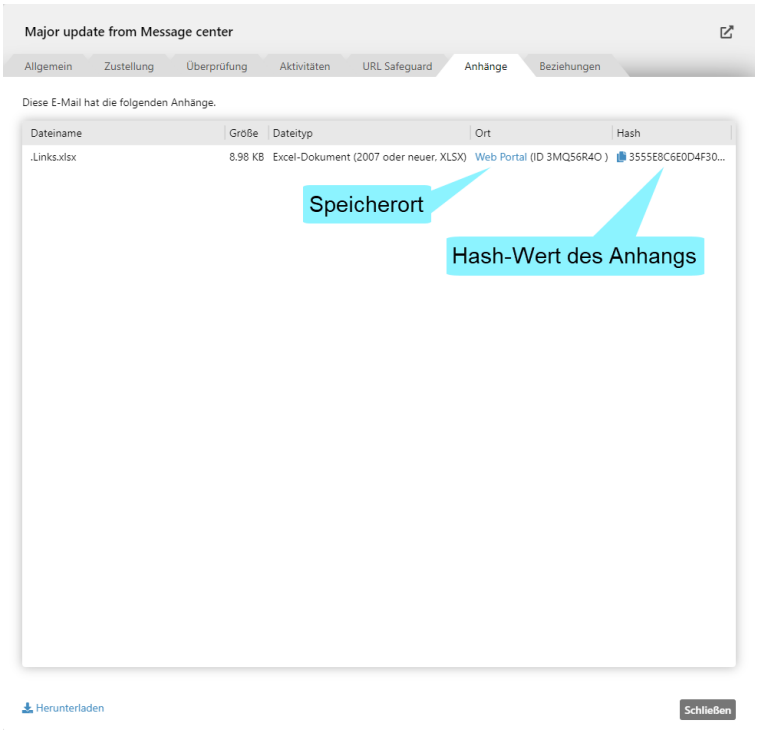
Registerkarte URL Safeguard

Hier finden Sie Informationen zu in der E-Mail oder in den Anhängen enthaltene URLs, die vom URL Safeguard umgeschrieben oder blockiert wurden.



Registerkarte Anhänge

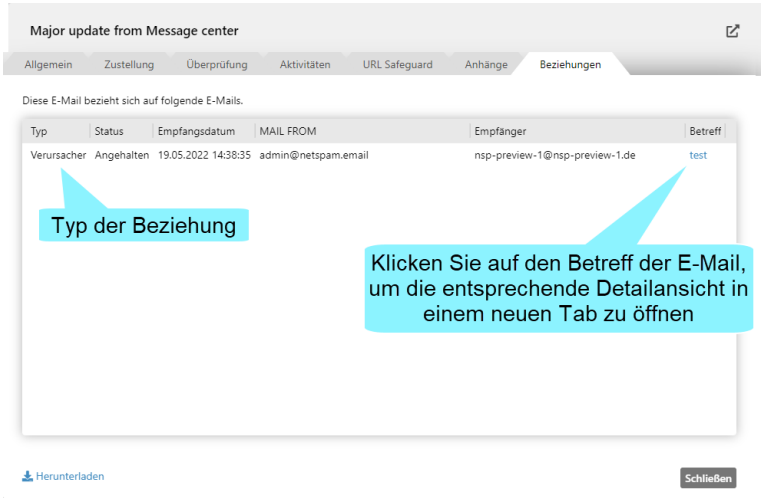
Hier finden Sie Informationen zu in der E-Mail enthaltenen Anhängen.



Informationen zu gesperrten Anhängen finden Sie unter **Gesperrte Anhänge**.

Registerkarte Beziehungen

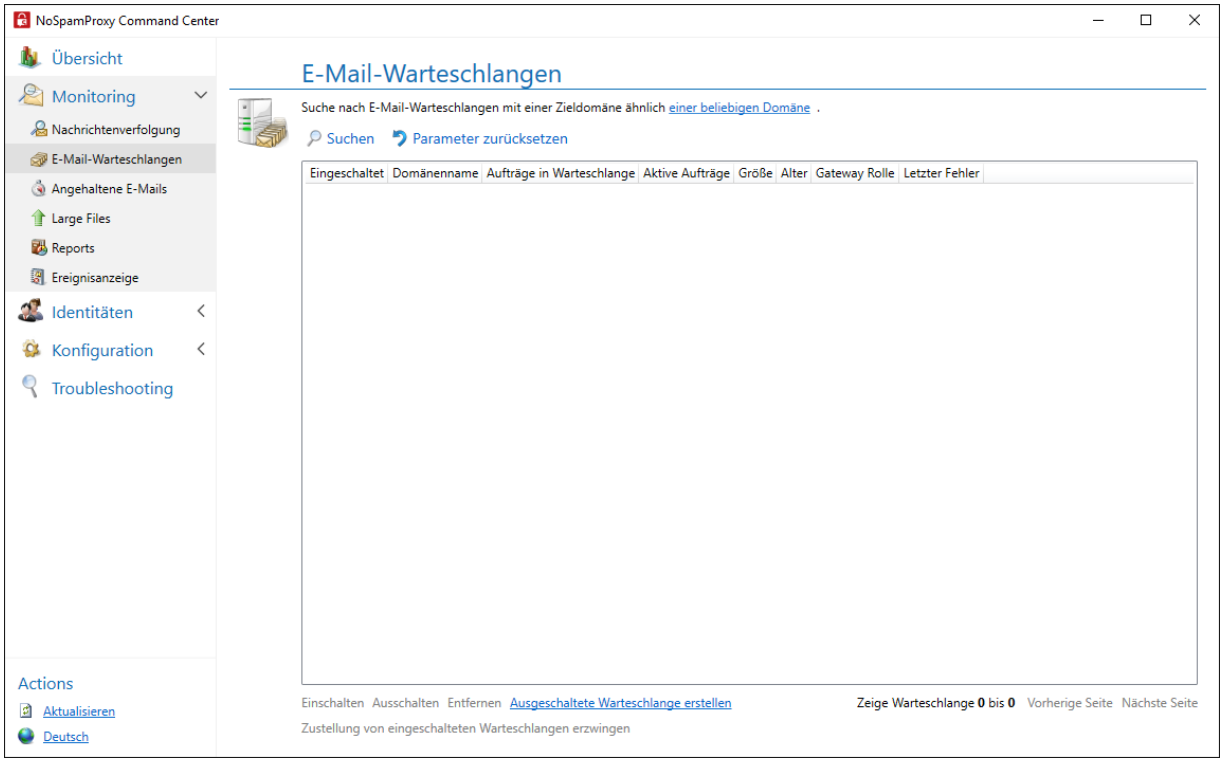
Hier finden Sie Verknüpfungen mit anderen Datensätzen der Nachrichtenverfolgung, die mit diesem Datensatz in Beziehung stehen.



E-Mail-Warteschlangen

E-Mails an externe Adressen werden Ihrer Domäne entsprechend Warteschlangen zugewiesen. Pro Domäne gibt es eine Warteschlange.

Unter **E-Mail-Warteschlangen** werden Ihnen sämtliche aktiven E-Mail-Warteschlangen angezeigt. 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.



Nach bestimmten Warteschlangen suchen

1. Geben Sie den Suchbegriff in das Suchfeld ein.
2. Klicken Sie **Suchen**.

Es werden alle Warteschlangen angezeigt, die dem Suchbegriff entsprechen.

Die einzelnen Spalten enthalten detaillierte Informationen:

Eingeschaltet| Zeigt an, ob derzeit für diese Domäne E-Mails zugestellt werden.

Domänenname| Entspricht dem Namen der Zieldomäne.

Warteschlangenlänge| Die Anzahl der wartenden E-Mails.

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.

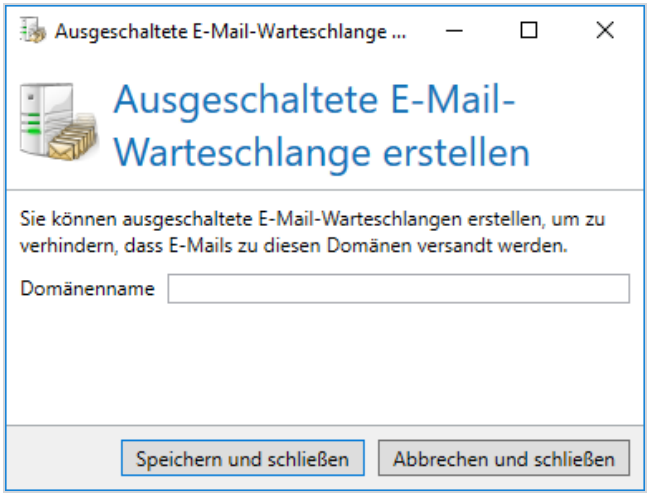
Zustellung über ausgewählte Domains starten oder pausieren

- Klicken Sie **Einschalten** beziehungsweise **Ausschalten**, um die Zustellung von E-Mails über eine bestimmte Domain zu starten oder zu pausieren.

Eine ausgeschaltete Warteschlange erstellen

Sie können eine ausgeschaltete Warteschlange erstellen, um die Verbindung zu einer bestimmten Domäne im Vorfeld zu unterbinden.

1. Wählen Sie **Ausgeschaltete Warteschlange erstellen**.



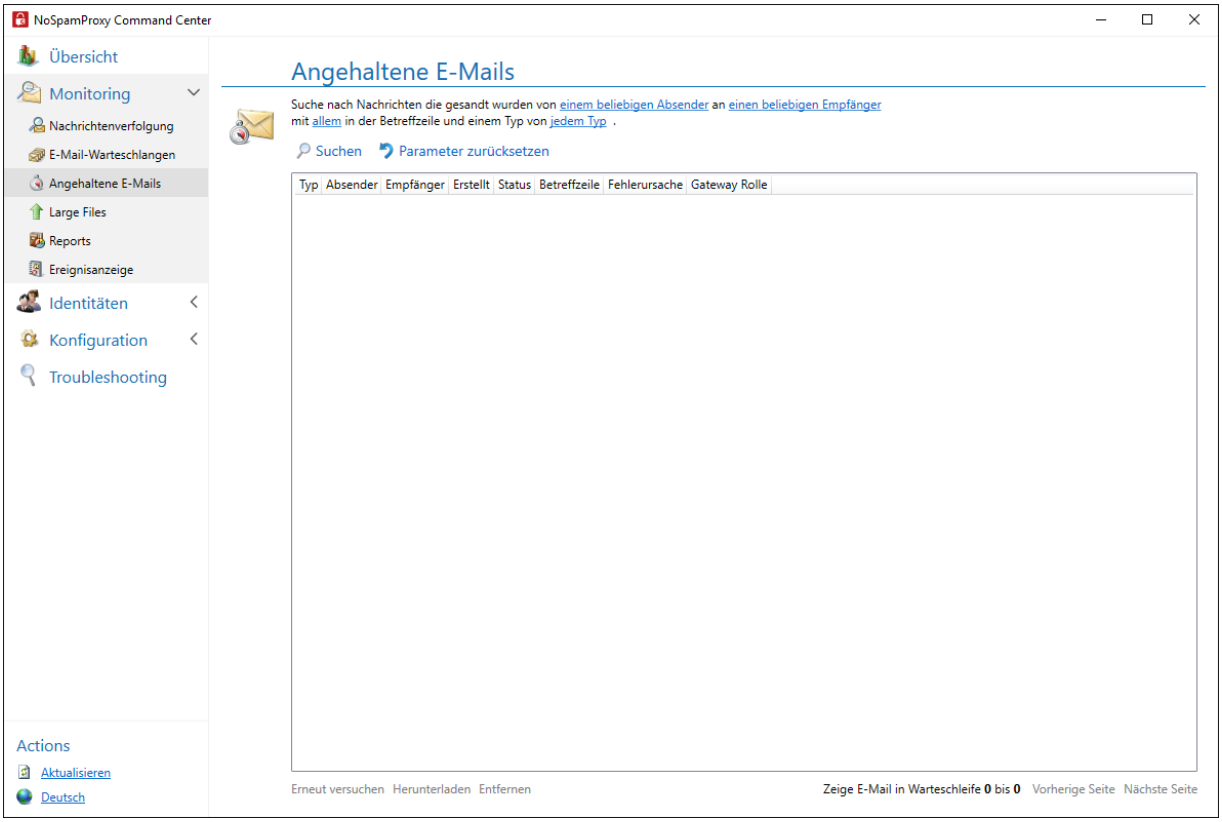
2. Geben Sie unter **Domänenname für Warteschlange** den Domänennamen an, also beispielsweise **netatwork.de**.
3. Speichern Sie die Einstellung, um die deaktivierte Warteschlange zu erstellen.

Es werden nun alle E-Mails an **netatwork.de** in den Warteschlangen von NoSpamProxy pausiert, bis Sie die Warteschlange wieder aktivieren.

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

Angehaltene E-Mails

Unter bestimmten Bedingungen können E-Mails 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.



Nach bestimmten angehaltenen E-Mails suchen

Bei der Suche nach angehaltenen E-Mails stehen Ihnen die Filterkriterien

- Richtung,
- Absender- und Empfängeradresse,
- Betreffzeile sowie der
- Status

der E-Mail zur Verfügung.

> **TIPP:** Für die Adressen und Betreffzeile müssen nur Teile des zu suchenden Textes eingegeben werden.

In welchen Fällen werden E-Mails angehalten?

- Falls Sie eine E-Mail über die Aktion **Anhänge mit einem Passwort schützen** verschlüsseln möchten, die in der Aktion angegebenen Passwortquellen aber keine Passworte bereitstellen.
- Falls bis zum angezeigten Ablaufdatum der E-Mail kein Passwort bereitgestellt wird oder keine signierte E-Mail vom ursprünglichen E-Mail-Empfänger eingeht. Die Zustellung wird abgebrochen und der Absender benachrichtigt.
- Falls E-Mails, die beim Hinzufügen oder Validieren von digitalen Dokumentensignaturen nicht automatisch bearbeitet werden können. Die E-Mails werden nicht zum eigentlichen Empfänger ausgeliefert, sondern mit Anzeige des aktuellen Status sowie der Ursache des Fehlschlags aufgelistet.
- Falls Fehler während des Zustellprozesses von De-Mails auftreten.
- Bei Nutzern von NoSpamProxy Large Files werden Dateien, bei denen das Hochladen fehlschlug, in der Liste angezeigt.

Verwandte Schritte

- **E-Mails erneut verarbeiten**| Eine erneute Verarbeitung von E-Mails lösen Sie aus, in dem Sie **Erneut versuchen** klicken. Sollten erneut Vorfälle auftreten, werden die betroffenen E-Mails erneut in die Liste eingetragen.
- **E-Mails lokal speichern**| Vollständige E-Mails mit allen zugehörigen Dokumenten speichern Sie lokal, indem Sie den jeweiligen Vorfall markieren und dann auf **Herunterladen** klicken.
- **E-Mails löschen**| Sie können angehaltene E-Mails löschen. Dabei können Sie wählen, ob der Absender hierüber benachrichtigt wird oder nicht.

Gesperrte Anhänge

Anhänge, die gesperrt wurden, werden auf dem Web Portal gespeichert. Auf der Registerkarte **Anhänge** in der Detailansicht der jeweiligen E-Mail haben Sie folgenden Optionen:

- Klicken Sie **Large Files**, um weitere Informationen zum Anhang zu erhalten, den Anhang herunterzuladen oder eine Malwareprüfung auszuführen.
- Klicken Sie **Anhänge freigeben**, um die jeweiligen Anhänge zu freizugeben.
- Klicken Sie **Anhänge verwerfen**, um die jeweiligen Anhänge zu löschen.

> **TIPP:** Um eine Übersicht zu allen E-Mails zu erhalten, die Dateien enthalten, die eine manuelle Freigabe erfordern, fügen Sie in der Nachrichtenverfolgung die Bedingung **Anhang erfordert Freigabe** hinzu.

Status-Typen

Im Folgenden werden die einzelnen Status-Typen an Hand von Beispielen erklärt.

> **HINWEIS:** Diese Informationen dienen einem grundsätzlichen Verständnis und decken nicht zwingend jeden Fall ab.

- **Erfolgreich|** Die E-Mail konnte erfolgreich an den Empfänger übermittelt werden.
- **Zustellung fehlgeschlagen|** Eine ausgehende E-Mail wurde von dem Empfangssystem abgelehnt. Im Reiter „Zustellung“ können Sie die Rückmeldung des Empfangssystem nachvollziehen.
- **Temporär abgewiesen|** Der einliefernde E-Mail-Server bekommt eine Rückmeldung und wird nach dem konfigurierten Intervall einen weiteren Zustellversuch durchführen.
    - **Greylisting|** Eine eingehende E-Mail hat mindestens 2 SCL-Punkte wegen Verstoß gegen unsere Filter erhalten.
    - **Empfänger entspricht nicht der Regel des ersten Empfängers|** Eine ausgehende E-Mail wird an unterschiedliche Empfänger versendet und nicht für jeden Empfänger liegt ein Zertifikat zum Verschlüsseln vor.
    - **32Guards|** Ein kürzlich neu gesichteter Host wird für einen kurzen Zeitraum temporär abgewiesen, um dessen Reputation zu ermitteln.
    - **Dienst nicht erreichbar|** Der Integrated Malware Scanner ist als einzig ausgewählter **Malware-Scanner** in der Regel konfiguriert, aber nicht erreichbar.

- **Permanent abgewiesen|** Die E-Mail wurde aufgrund von Verstoß gegen unsere Filter mit mindestens 4 SCL-Punkten bewertet oder durch **Aktionen in NoSpamProxy** abgewiesen.
- **Zustellung ausstehend|** Die E-Mail befindet sich noch in Zustellung und wird je nach Resultat in Kürze mit einem entsprechenden anderen Status vermerkt. Details finden Sie auf der Registerkarte **Zustellung**.
- **Mehrere Zustellzustände|** Eine E-Mail wurde an mehrere Empfänger versendet und mit unterschiedlichen Ergebnissen vermerkt. Details finden Sie im jeweiligen Eintrag auf der Registerkarte **Zustellung**.
- **Angenommen aber nicht zugestellt|** Die E-Mail wird empfangen, kann aber nicht verarbeitet werden.
    - **Ausgehende Inhaltsfilterung|** Der hinterlegte Inhaltsfilter verbietet den Anhang der E-Mail.
    - **Verschlüsselung|** Es wird eine Regel mit zwingender Verschlüsselung genutzt; dies war für den Empfänger nicht möglich
    - **Der Absender hat eine Verbindung aufgebaut, aber keinen Email Body übermittelt|** In diesem Fall sieht NoSpamProxy nur noch den Email Envelope mit Absender und Empfänger, kann die E-Mail aber nicht verarbeiten. Oftmals wird solch eine Verbindung erzeugt, um eine E-Mail-Adresse einer zuvor ausgehenden E-Mail zu validieren und soll als Anti-Spam-Maßnahme dienen. Das Verfahren ist bekannt als **Callback verification**.
    - **De-Mail|** Es wird versucht, eine E-Mail, für die in NoSpamProxy keine Konfiguration vorliegt, an einen De-Mail-Empfänger zuzustellen.
- **Doppelt|** Eine E-Mail wurde doppelt an NoSpamProxy zugestellt. Die Schleife (Email Loop) wird verhindert und die E-Mail wird nicht zugestellt.

- Eine eingehende E-Mail wird von NoSpamProxy an den hinterlegten E-Mail-Server zugestellt. Diese E-Mail landet jedoch nicht im Postfach des Empfängers, sondern der E-Mail-Server sendet wenige Sekunden nach Empfang der E-Mail diese erneut an NoSpamProxy zurück.
- Eine eingehende E-Mail wurde doppelt mit der gleichen Nachrichten-ID vom selben oder von unterschiedlichen einliefernden Systemen versendet. Jede E-Mail muss eine eindeutige Mail ID haben.
- Eine ausgehende E-Mail an Office 365 wird zurück in den eigenen Mandanten geholt. In diesem Fall stellt der eigene Office-365-Konnektor das Problem dar.

Office 365 agiert nach dem Prinzip, dass es mehrere Zugangspunkte für E-Mails gibt. Konfigurieren Sie einen Konnektor, so wird dieser an die für Ihren Mandanten zuständigen Systeme übermittelt.

Falls ein Kommunikationspartner über das selbe System wie Sie E-Mails empfängt, gilt natürlich auch Ihr Konnektor (eingehend).

Beachten Sie dabei, dass Office 365 zwei Arten von Konnektoren kennt: **Partnerorganisation an Office 365** und **E-Mail-Server der Organisation an Office 365**. Der entscheidende Unterschied hierbei ist, dass der Partnerkonnektor nur dann aktiv wird, wenn eine Ihrer eigenen Domänen als E-Mail-Empfänger angegeben ist. Der Konnektor **E-Mail-Server der Organisation an Office 365** greift, wenn Ihre Domäne als Absender auftritt und holt dann die E-Mail zurück in Ihren Mandanten.

Aus Sicht von NoSpamProxy wird die E-Mail korrekt an das im MX angegebene System abgeliefert. Aus Microsoft-Seite ist jedoch der Unterschied zum erwarteten Verhalten, dass Ihr Mandant die E-Mail auf Grund des zuvor erwähnten Konnektors statt dem eigentlichen Empfänger-Mandangten empfängt und sie dann entsprechend der Regeln wieder an NoSpamProxy zustellen will. Die E-Mail wurde dann aus Sicht von NoSpamProxy zugestellt, aber in Office 365 falsch eingeordnet.

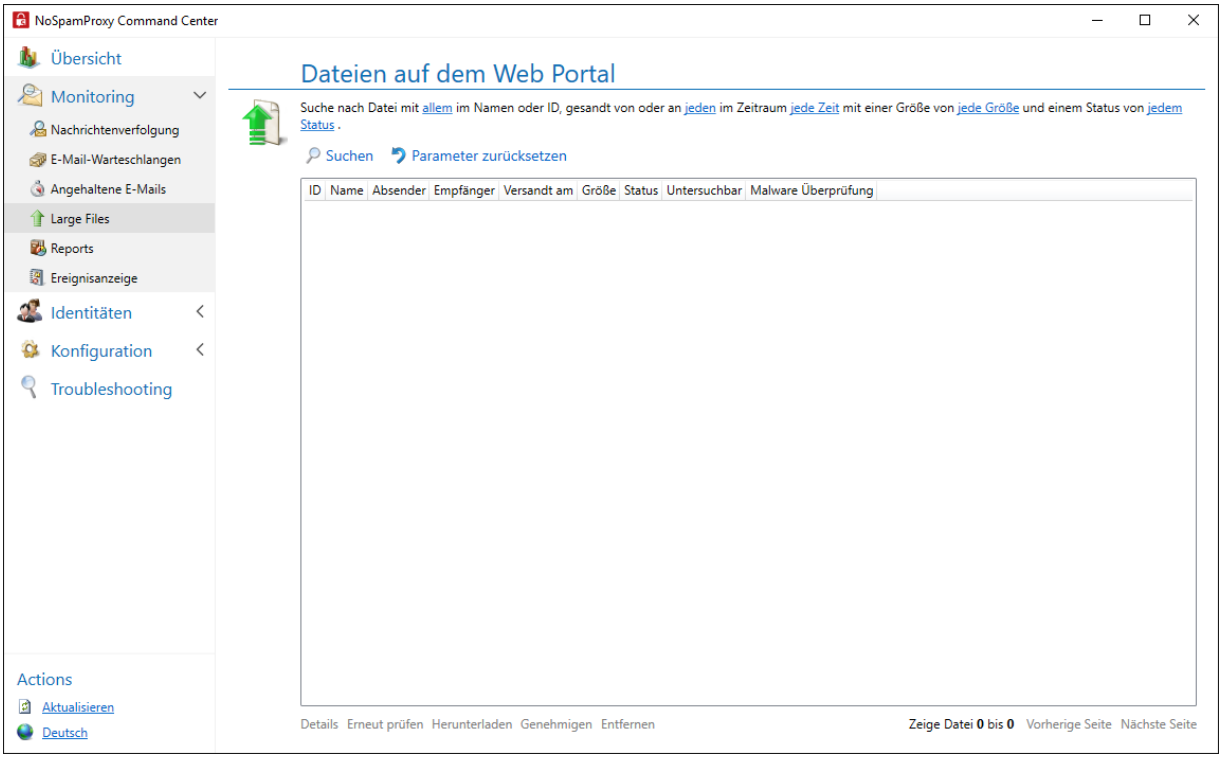
Lösungen gibt es hier mehrere. Alle haben das Ziel, zwischen E-Mails von Ihnen und E-Mails, die zu Ihnen kommen, zu unterscheiden. Dies können Sie entweder mit Hilfe eines erneuten Anlegens des eingehenden Konnektors in Office 365

> **(Partnerorganisation an Office 365)** oder durch Umstellung auf unterschiedliche TLS-Identitäten bei ein- und ausgehenden Sendekonnektoren in NoSpamProxy erreichen.Wir empfehlen hier, im ausgehenden Sendekonnektor keine TLS-Identität zu übermitteln.

- **Angehalten**| Es sind weitere Aktionen notwendig, damit die E-Mail erfolgreich zugestellt wird.
  - **Inhaltsfilter**| Die E-Mail wird zur Verarbeitung der angehängten Dateien angehalten und anschließend mit einem zweiten Message Track als erfolgreiche E-Mail zugestellt. Die durchgeführte Aktion lässt sich im Message Track auf der Registerkarte **Aktivitäten** nachvollziehen. Den Nachfolger der angehaltenen E-Mail können Sie im Message Track auf der Registerkarte **Beziehungen** nachvollziehen.
  - **PDF-Mail**| Die ausgehende E-Mail wird in ein PDF-Dokument konvertiert und verschlüsselt, da kein S/MIME-Zertifikat für den Empfänger vorliegt. Der Empfänger muss ein Passwort auf dem Webportal vergeben; solange verbleibt die E-Mail in diesem Status.
  - **Dienst nicht erreichbar**| Der Integrated Malware Scanner kann Dateien, die zum Webportal hochgeladen werden sollen, nicht erreichen.

Large Files

Hier erhalten Sie einen Überblick über alle Dateien, die derzeit auf dem Web Portal gespeichert sind.



Verwandte Schritte

- Dateien löschen, die nicht mehr benötigt werden.
- Dateien zum Herunterladen freigeben, die die Freigabe eines Administrators benötigen.
- Noch nicht freigegebene Dateien durch den Administrator herunterladen, um deren Inhalt zu überprüfen (falls Sie als **Untersuchbar** in der Liste markiert sind).

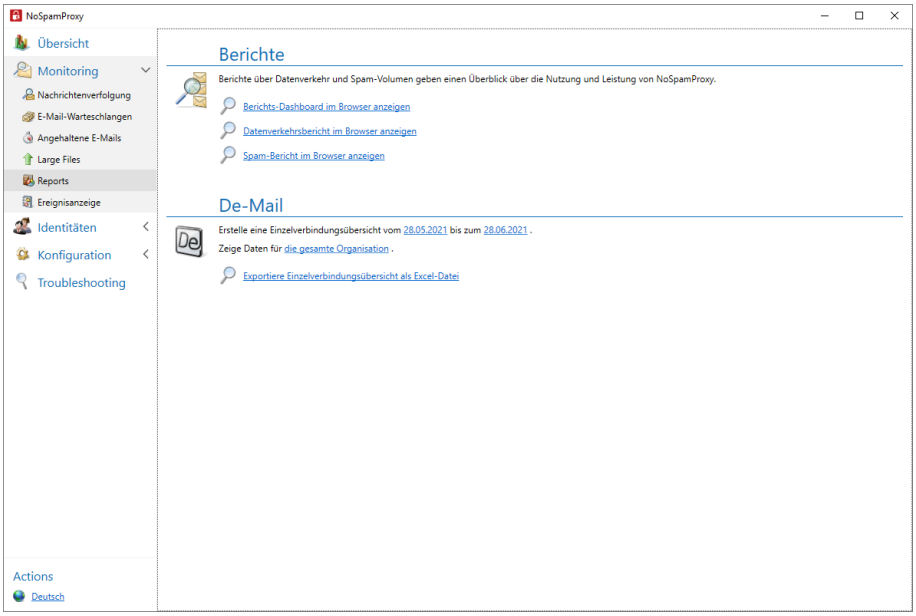
- Untersuchbare Dateien über **Erneut prüfen** auf Malware untersuchen. Wird Malware gefunden, wird die Datei gelöscht und der Empfänger über das Ergebnis informiert. Die Spalte **Malware Überprüfung** zeigt den Zeitpunkt der letzten Überprüfung an.

Filteroptionen bei der Suche

- **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, beispielsweise **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. Klicken Sie **Details**, um weitere Empfänger sowie eventuell aufgetretene Probleme während des Malwarescans anzuzeigen.

Reports

Die Reports von NoSpamProxy geben Ihnen einen Überblick über den Verlauf Ihres E-Mail-Verkehrs und darüber, wie sich das Spam-Aufkommen über die Monate verändert hat. Sie erhalten auch Informationen zu den E-Mail-Adressen und Domänen, die das höchste Spam-Aufkommen hatten.

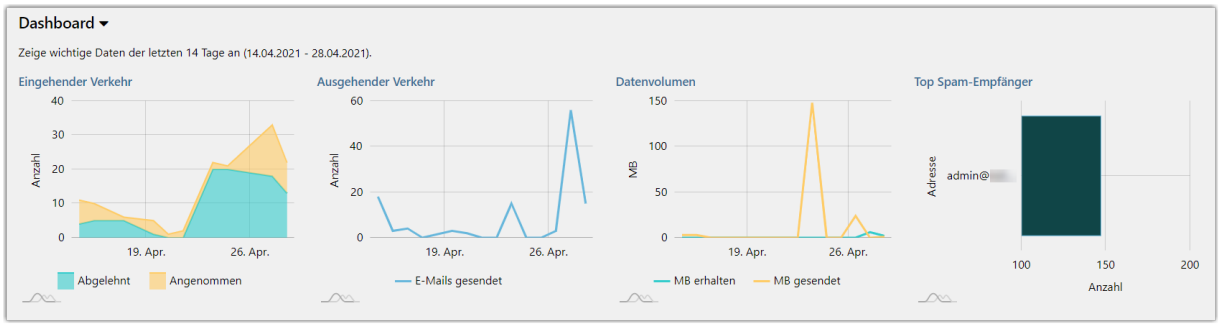


Reports

Mit den Reports in NoSpamProxy haben Sie eine Übersicht des eingehenden und ausgehenden E-Mail-Verkehrs sowie der Top-Spam-Empfänger.

> **TIPP:** Sie können in allen Ansichten mit der Maus über einem Datum hovern, um genaue Angaben anzuzeigen.

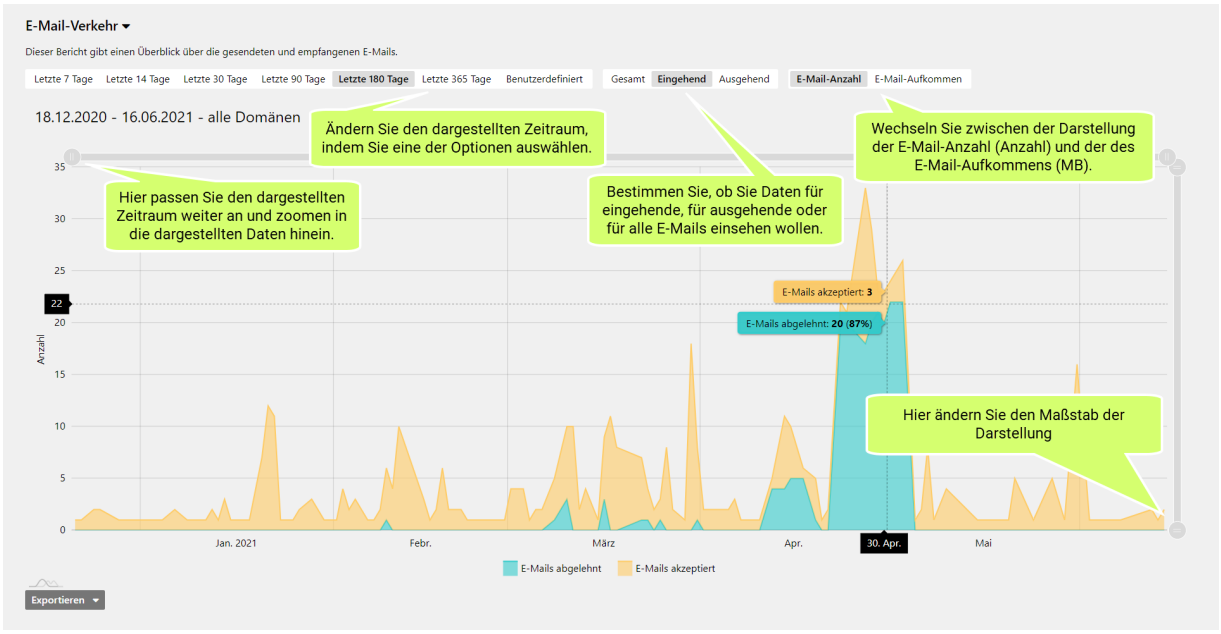
Dashboard



Das Dashboard zeigt Ihnen vier Schnellübersichten zu

- eingehenden E-Mails,
- ausgehenden E-Mails,
- dem Datenvolumen (MB) sowie
- den Top-Spam-Empfängern.

E-Mail-Verkehr



Die Detailansichten zum E-Mail-Verkehr bieten Ihnen detaillierte Übersichten zum gewählten Zeitraum und zur gewählten Richtung des E-Mail-Flusses. Passen Sie die einzelnen Charts an Ihre Bedürfnisse an, indem Sie beispielsweise den dargestellten Zeitraum ändern oder ausschließlich Daten für eingehende E-Mails anzeigen.

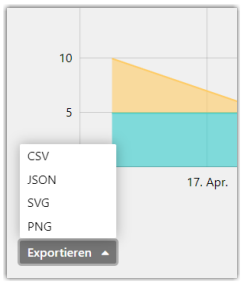
Top-Spam-Empfänger

Diese Ansicht zeigt Ihnen die Empfänger, die im gewählten Zeitraum den meisten Spam erhalten haben.

Charts exportieren

Sie können alle Charts als Dateien in den Formaten CSV, JSON, SVG oder PNG exportieren.

1. Öffnen Sie im gewünschten Chart das Drop-Down-Menü in der linken unteren Ecke.
2. Wählen Sie das Format, in das Sie den Chart exportieren wollen.



De-Mail

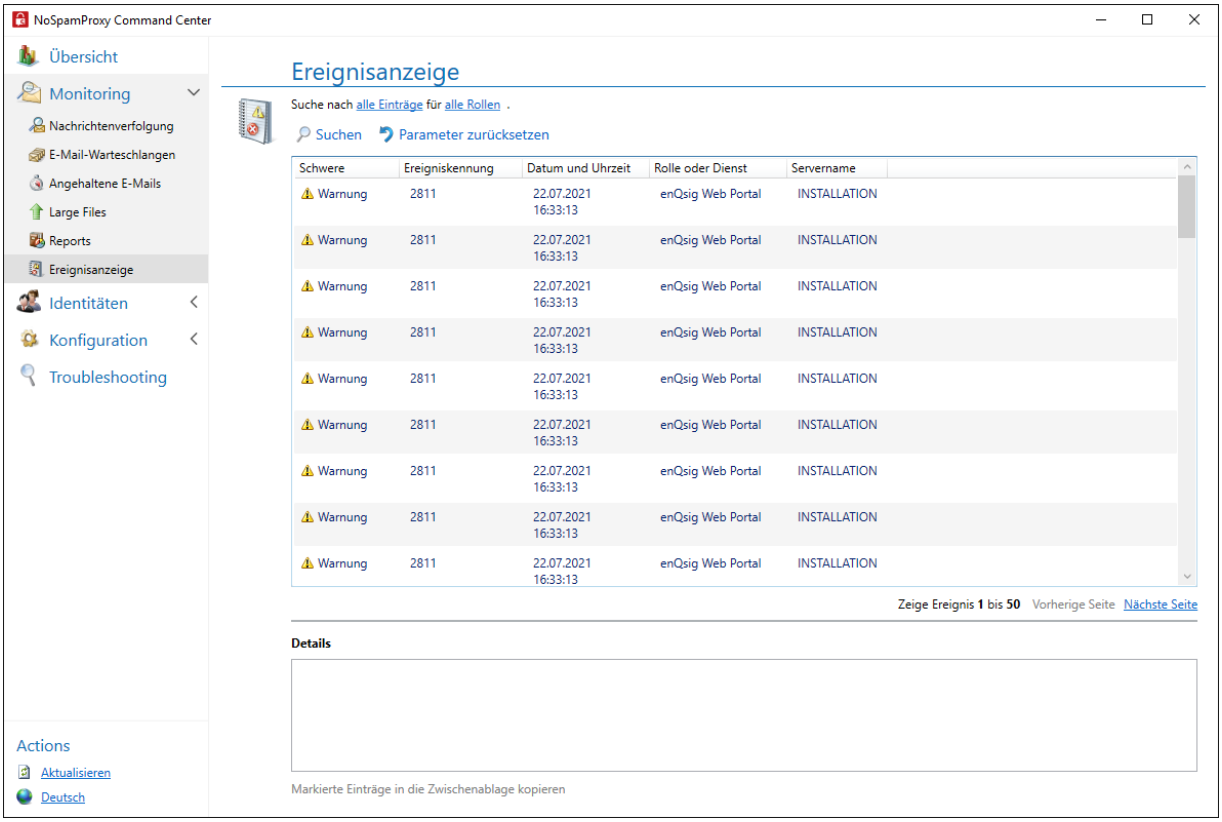
Mit dem De-Mail-Report können Sie eine Einzelverbindungsübersicht für gesendete De-Mails als Excel-Report erzeugen.

Gehen Sie folgendermaßen vor:

1. Wählen Sie aus, ob Sie eine Übersicht für die ganze Organisation oder für eine bestimmte Domäne erstellen möchten.
2. Schränken Sie bei Bedarf den Zeitraum für die Übersicht ein.
3. Klicken Sie auf **Exportiere Einzelverbindungsübersicht als Excel-Datei**.
4. Wählen Sie im folgenden Dialog aus, wo Sie die Excel-Datei speichern möchten.
5. Klicken Sie **Speichern**.

Ereignisanzeige

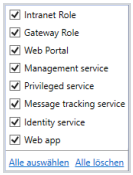
Hier sind die für NoSpamProxy relevanten Serverereignisse verfügbar.



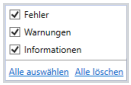
Einträge filtern

Die folgenden Eigenschaften können zur Einschränkung der Ergebnisse verwendet werden:

- Rollen und Dienste



- Art der angezeigten Ereignisse: Fehler, Informationen und Warnungen.



> **TIPP:** Um weiter zurückliegende Einträge anzuschauen, können Sie über **Zurück** und **Weiter** durch das Ergebnis der Suche blättern. Um die Details eines Eintrags anzuzeigen, müssen Sie diesen mit der Maus markieren. Die Details werden im unteren Teil der Seite eingeblendet.

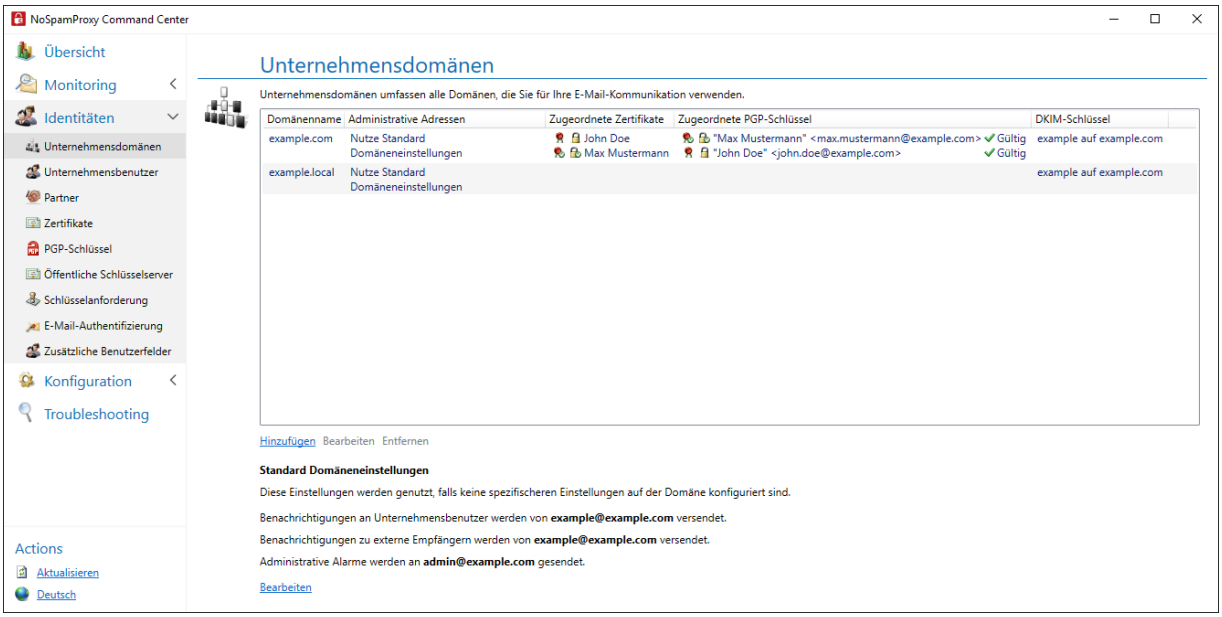
Identitäten

Dieser Bereich bietet Ihnen Zugriff auf alle externen und internen Firmen und Personen, deren E-Mail-Adressen sowie die dazugehörigen kryptographischen Schlüssel und Passworte.

Unternehmensdomänen

Unternehmensdomänen sind die Domänen, für die Sie E-Mails empfangen wollen. Die Liste der Unternehmensdomänen kann auch beim **Regeln erstellen** verwendet werden. Verbindungen zu Domänen, die nicht in der Liste aufgeführt sind, wird NoSpamProxy® als Relay-Missbrauch bewerten

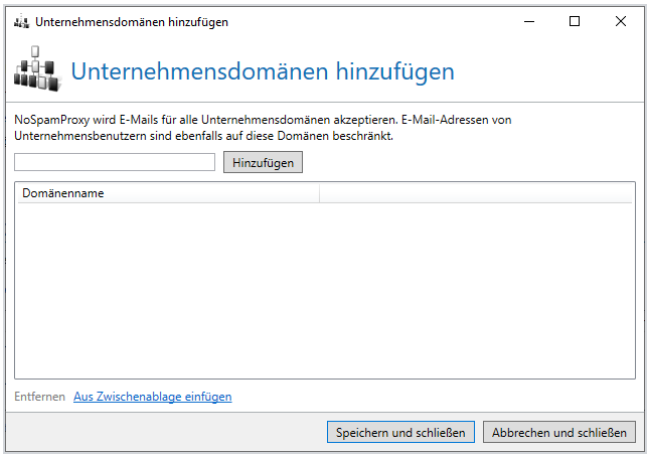
> **HINWEIS:** Sie müssen alle lokalen Domänen in die Liste der Unternehmensdomänen eintragen. Andernfalls werden alle lokalen E-Mails abgewiesen.



Unternehmensdomänen verwalten

Unternehmensdomänen hinzufügen

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie den Namen der Domäne ein, die Sie hinzufügen wollen.
4. Klicken Sie auf **Domäne hinzufügen**.

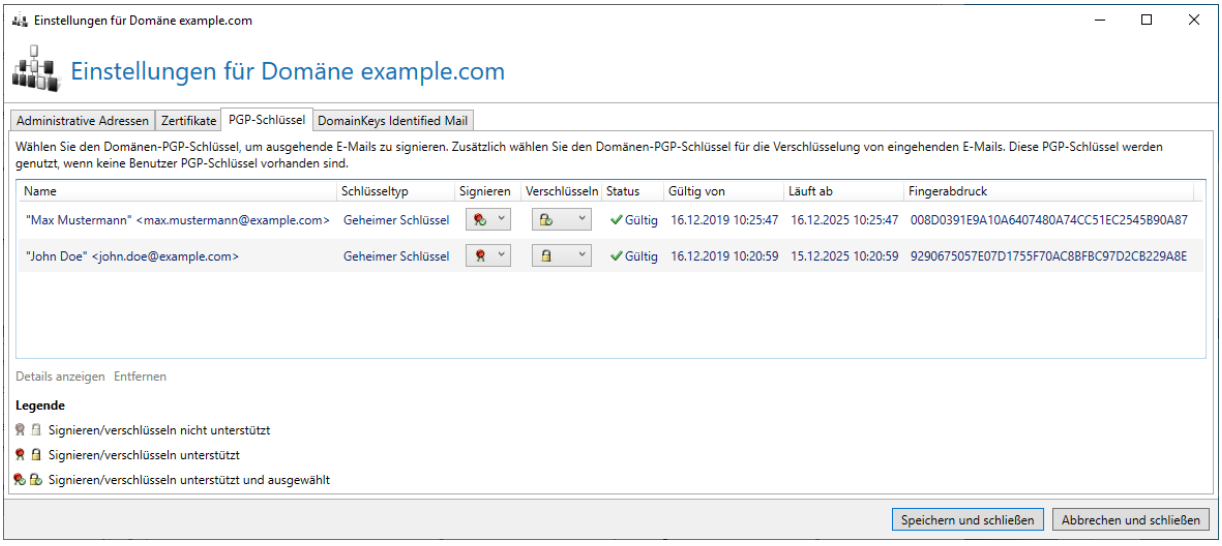
Unternehmensdomänen entfernen

1. Gehen Sie zu **Identitäten > Unternehmensdomänen > Unternehmensdomänen**.
2. Markieren Sie die Domäne, die Sie entfernen wollen.
3. Klicken Sie auf **Entfernen**.

HINWEIS: Beim Löschen von Unternehmensdomänen 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

HINWEIS: Die Verwaltung der Domänenzertifikate und Domänen-PGP-Schlüssel unter den Unternehmensdomänen sowie die Verwaltung der Zertifikate und PGP-Schlüssel unter den E-Mail-Adressen der **Unternehmensbenutzer** läuft nahezu identisch ab. Die folgende Beschreibung der Schlüsselauswahl gilt für beide Einsatzbereiche.



Kryptographische Schlüssel auswählen

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Doppelklicken Sie die Domäne, deren kryptographische Schlüssel Sie bearbeiten wollen **oder** markieren Sie die Domäne und klicken Sie **Bearbeiten**.
3. Wechseln Sie zur Registerkarte **Zertifikate** beziehungsweise **PGP-Schlüssel**.
4. Bestimmen Sie
   - unter **Signieren**, welcher der kryptographischen Schlüssel für die Signierung von E-Mails verwendet werden soll und
   - unter **Verschlüsseln**, welcher der kryptographischen Schlüssel für die Verschlüsselung von E-Mails verwendet werden soll.
5. Klicken Sie **Speichern und schließen**.

HINWEIS: NoSpamProxy bietet Ihnen für den jeweiligen kryptographischen Schlüssel nur die Optionen an, die dieser auch unterstützt. Es kann nur jeweils ein Schlüssel zur Verschlüsselung beziehungsweise Signierung ausgewählt werden kann. Falls Sie zu einem späteren Zeitpunkt einen anderen Schlüssel auswählen, wird der zuerst ausgewählte nicht mehr für die Verschlüsselung benutzt.

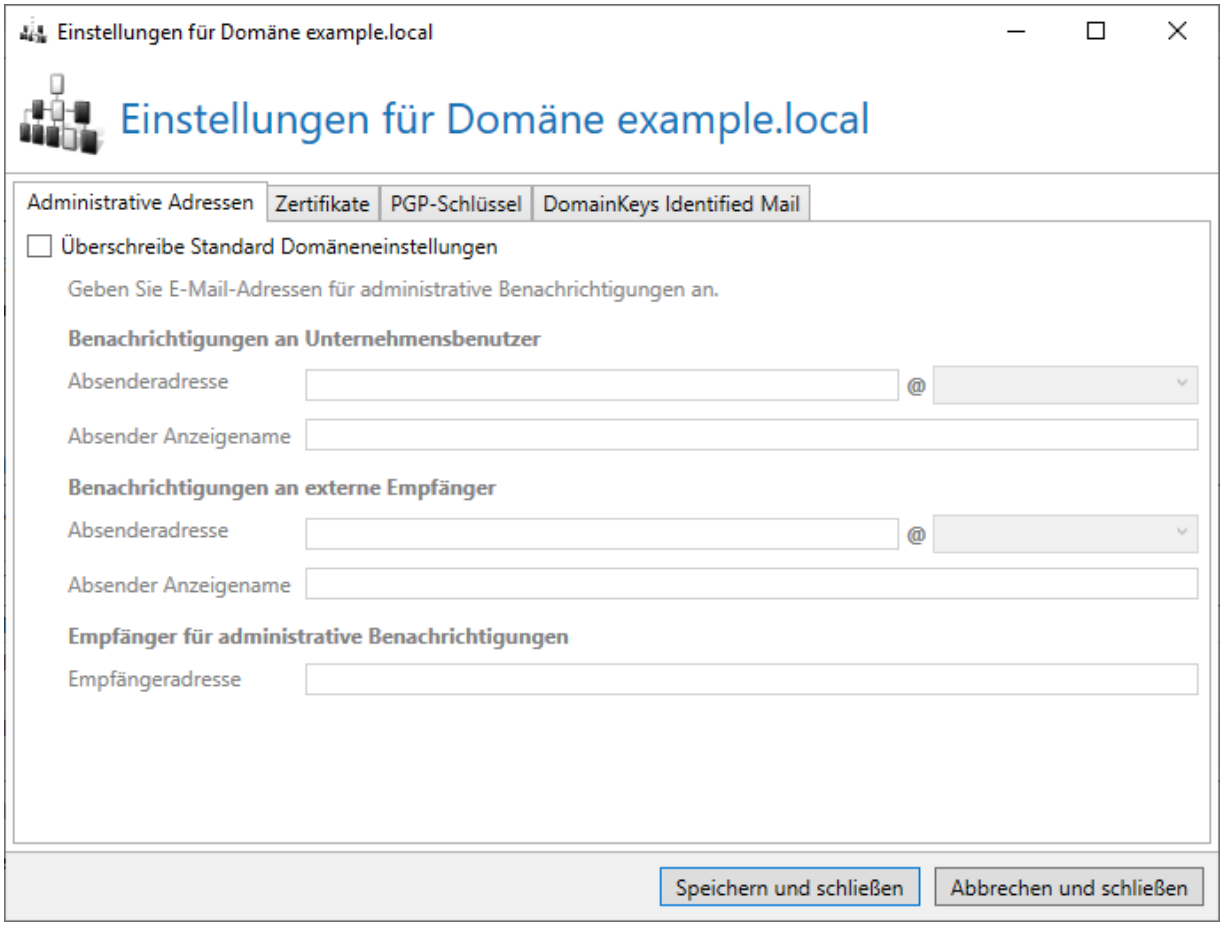
Details anzeigen

- Klicken Sie **Details anzeigen**, um alle Eigenschaften des Schlüssels einzusehen.

- Klicken Sie **Entfernen**, um den jeweiligen kryptographischen Schlüssel zu löschen.

Administrative Adressen einrichten

Domänenspezifische Adressen

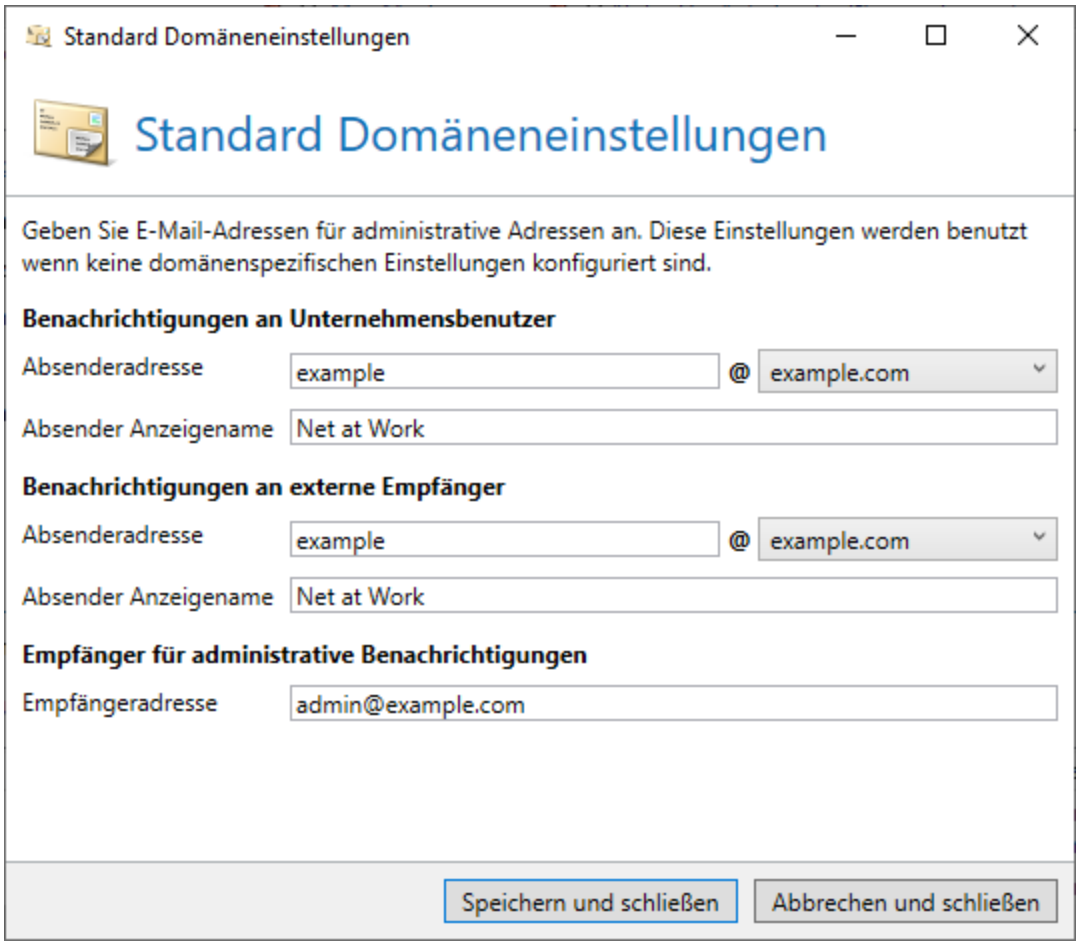


NoSpamProxy benötigt für die von ihm zu sendenden E-Mail-Benachrichtigungen gültige Absenderadressen sowie eine Adresse, an die administrative Alarme gesendet werden. Um domänenspezifische Adressen zu konfigurieren, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Identitäten > Unternehmensdomänen > Unternehmensdomänen**.
2. Doppelklicken Sie die Domäne, die Sie bearbeiten wollen.
3. Wählen Sie **Überschreibe Standard-Domäneneinstellungen**, um die hier gemachten Einstellungen an Stelle der Standard-Domäneneinstellungen zu verwenden.
4. Geben Sie die jeweiligen E-Mail-Adressen ein.
5. Klicken Sie **Speichern und schließen**.

Domänenübergreifende Adressen

Sie können administrative Adressen konfigurieren, die für das Senden von E-Mail-Benachrichtigungen sowie das Empfangen von administrativen Alarmen genutzt werden, falls keine spezifischen Einstellungen für die jeweilige Domäne konfiguriert sind. Gehen Sie folgendermaßen vor:

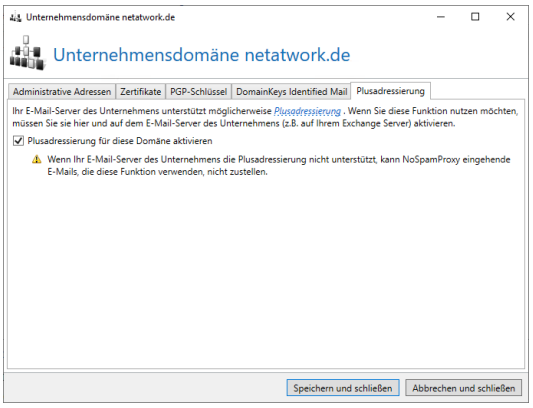


1. Gehen Sie zu **Identitäten > Unternehmensdomänen > Unternehmensdomänen**.
2. Klicken Sie **Standard-Domäneneinstellungen**.
3. Geben Sie die jeweiligen E-Mail-Adressen ein.
4. Klicken Sie **Speichern und schließen**.

> **TIPP:** Falls eine Domäne eine von den Standardadresse abweichende Adresse benötigt, können Sie diese auf der jeweiligen Domäne vornehmen.

Plusadressierung

Plusadressierung (auch bekannt als Unteradressierung) ist eine Methode, um dynamische, verwerfbare E-Mail-Adressen für Postfächer zu unterstützen. Falls aktiviert, ordnet NoSpamProxy beispielsweise der E-Mail-Adresse **max.mustermann+newsletter@example.com** den Unternehmensbenutzer mit der E-Mail-Adresse **max.mustermann@example.com** zu.



WARNUNG: Wenn Ihr E-Mail-Server des Unternehmens die Plusadressierung nicht unterstützt, kann NoSpamProxy eingehende E-Mails, die diese Funktion verwenden, nicht zustellen.

Plusadressen (auch Unteradressen genannt) werden im Rahmen der Lizenzierung **nicht** gezählt, sofern die Plusadressierung für die jeweilige Domäne aktiviert ist. Dies gilt sowohl für die Lizenzierung der Module als auch für die Lizenzierung von Diensten. Es werden nur die zu Grunde liegenden E-Mail-Adressen der Benutzer gezählt, für die Plusadressen vorliegen.

> **HINWEIS:** Wenn Sie diese Funktion nutzen möchten, müssen Sie sie hier **und** auf dem E-Mail-Server des Unternehmens aktivieren (also beispielsweise Ihrem Exchange-Server).

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Doppelklicken Sie die Domäne, die Sie bearbeiten wollen oder markieren Sie sie und klicken Sie **Bearbeiten**.
3. Wechseln Sie zur Registerkarte **Plusadressierung**.
4. Setzen Sie das Häkchen bei **Plusadressierung für diese Domäne aktivieren**.
5. Klicken Sie **Speichern und schließen**.

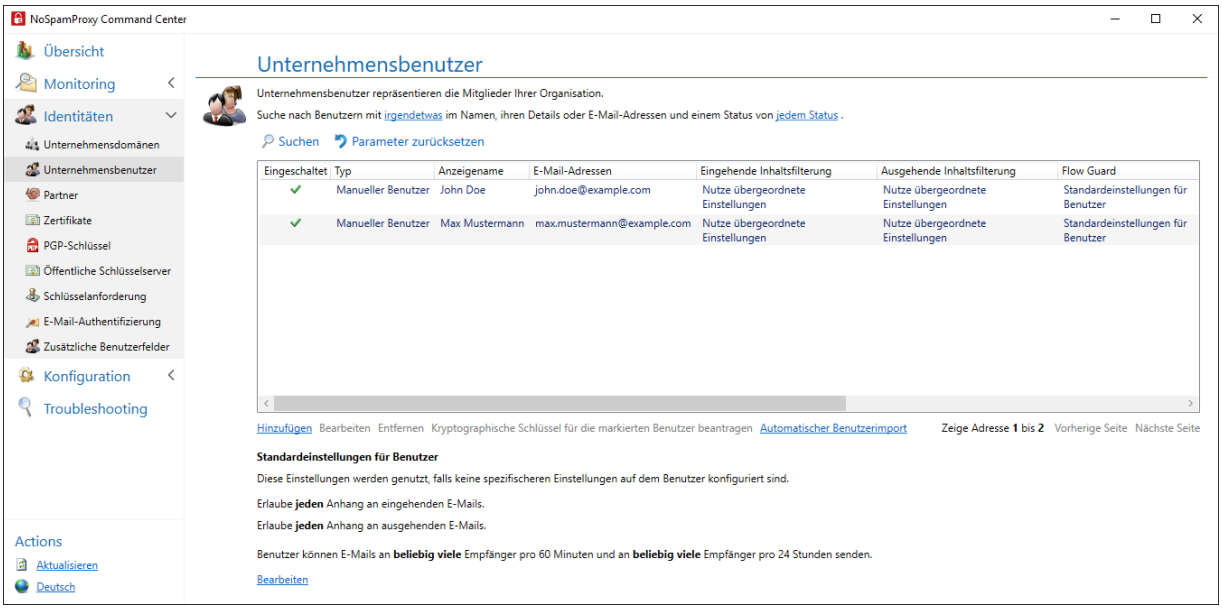
> **TIPP:** Weitere Informationen finden Sie in der **Microsoft-Dokumentation**.

Unternehmensbenutzer

Wie auch bei den **Unternehmensdomänen** kann NoSpamProxy die einzelnen Empfänger prüfen und E-Mails an nicht existierende Empfänger direkt abweisen. Dazu ist es erforderlich, dass NoSpamProxy 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** anstatt auf **Unternehmensdomänen** filtern.

HINWEIS: Damit NoSpamProxy die Liste der Unternehmensbenutzer verwendet, muss in den entsprechenden Regeln für eingehenden E-Mail-Verkehr auf der Registerkarte **Nachrichtenfluss** der Bereich von **an eine Unternehmensdomäne** auf **an eine E-Mail-Adresse des Unternehmens** umgestellt werden. Erst jetzt nutzt NoSpamProxy die Liste der Unternehmensbenutzer für die Ermittlung gültiger E-Mail-Adressen.



Typen von Benutzern

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

- **Manuell eingetragene Benutzer**| Sämtliche Eigenschaften von manuell eingetragenen Benutzern können Sie in NoSpamProxy verwalten. Diese Benutzer können beliebig verändert und gelöscht werden.
- **Replizierte Benutzer**| Replizierte Benutzer werden aus einem Verzeichnisdienst wie dem Active Directory **importiert**. Die Eigenschaften dieser Benutzer müssen in der ursprünglichen Quelle verändert werden, da in bei replizierten Benutzern nur eine Lese-Ansicht der meisten Eigenschaften in NoSpamProxy 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.

Verwandte Schritte

- **Unternehmensbenutzer hinzufügen|** Alle Benutzer, die von NoSpamProxy verwaltet werden sollen, müssen zunächst hinzugefügt werden. Siehe **Unternehmensbenutzer hinzufügen**.
- **Benutzer automatisch importieren|** Über **Automatischer Benutzerimport** haben Sie die Möglichkeit, den Import von Benutzerdaten zu automatisieren. Siehe **Benutzerimport automatisieren**.
- **Adressen umschreiben|** Die Adressumschreibung schreibt die E-Mail-Adresse eines Unternehmensbenutzers auf eine andere E-Mail-Adresse um. Siehe **Adressumschreibung einrichten**.
- **Kryptographische Schlüssel beantragen|** Wenn Sie entsprechende Anbieter konfiguriert haben, können Sie über NoSpamProxy Encryption Zertifikate und PGP-Schlüssel für die E-Mail-Adressen der **Unternehmensbenutzer** erstellen lassen. Siehe **Zertifikatsanbieter konfigurieren** und **Kryptographische Schlüssel beantragen**.
- **Bestimmte Inhaltsfilter als Standard festlegen|** Siehe **Standardeinstellungen für Benutzer konfigurieren**.

Unternehmensbenutzer hinzufügen

Um einen Unternehmensbenutzer hinzuzufügen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer** und klicken Sie **Hinzufügen**.
2. Geben Sie den Namen des neuen Benutzers sowie (optionale) Details an.

3. Geben Sie alle E-Mail-Adressen des Benutzers ein, indem Sie den lokalen Teil der E-Mail-Adresse eingeben und die Domäne aus dem Drop-Down-Menü auswählen.

   > **HINWEIS:** Die erste eingegebene Adresse wird als primäre Adresse markiert. Sie können dieses in der Liste der E-Mail-Adressen über **Als primäre Adresse einstellen** ändern. Die primäre Adresse wird für andere Funktionen wie beispielsweise De-Mail verwendet.

4. Wählen Sie aus der Liste der Zertifikate und PGP-Schlüssel diejenigen aus, die Sie für die jeweilige E-Mail-Adresse verwenden wollen.

   > **HINWEIS:** Weitere Informationen zum Bearbeiten von Zertifikaten einer Benutzer E-Mail-Adresse finden Sie unter **Kryptographische Schlüssel verwenden**.

5. (Optional) Richten Sie Adressumschreibungen für die E-Mail-Adresse ein.
6. Wählen Sie den Inhaltsfilter, der dem Benutzer zugeordnet werden soll oder verwenden Sie die **Standardeinstellungen für Benutzer konfigurieren**.
7. Bestimmen Sie, welche De-Mail-Funktionen für diesen Benutzer verfügbar sein sollen.
8. Bestimmen Sie, ob der Name dieses Benutzers für die **CxO-Betrugserkennung** verwendet werden soll.
9. Klicken Sie **Fertigstellen**.

Benutzerimport automatisieren

Sie können den Import von Benutzerdaten automatisieren, indem Sie in der Intranetrolle mehrere Benutzerimporte einrichten. Dies ermöglicht es Ihnen, die Unternehmensbenutzer in der Gatewayrolle von NoSpamProxy differenziert auf dem aktuellen Stand zu halten.

Als Quelle können Sie entweder

- ein on-premises Active Directory,
- ein Azure Active Directory,
- eine generisches LDAP oder
- eine Textdatei

angeben.

Neuer Benutzerimport per on-premises Active Directory

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Klicken Sie **Automatischer Benutzerimport** und dann **Hinzufügen**.
3. Wählen Sie **On-Premises Active Directory** als Typ des Benutzerimports.
4. Bestimmen Sie unter **Allgemein** einen eindeutigen Namen, den Aktualisierungszyklus sowie den Status des Benutzerimports.

5. Wählen Sie die Art des Servers und den Benutzer, der darauf zugreifen darf.

> **TIPP:** Die Active-Directory-Suche wählt die Benutzer aus, die importiert werden. Sie können hier auf bestimmte Container filtern, beispielsweise `OU=Vertrieb, OU=User, DC=domäne, DC=DE`. 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.

> **HINWEIS:** 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.

6. **(Optional)** Geben Sie einen zusätzlichen LDAP-Filter an.
7. Geben Sie unter **Gruppen** an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.
8. Klicken Sie **Fertigstellen**.

Neuer Benutzerimport per Azure Active Directory

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Klicken Sie **Automatischer Benutzerimport** und dann **Hinzufügen**.
3. Wählen Sie **Azure Active Directory** als Typ des Benutzerimports.
4. Bestimmen Sie unter **Allgemein** einen eindeutigen Namen, den Aktualisierungszyklus sowie den Status des Benutzerimports.
5. Führen Sie einen der folgenden beiden Schritte aus:
    - Geben Sie Ihre globale Azure Client ID an. Um eine globale Azure Client ID nutzen zu können, müssen Sie vorher per PowerShell eine globale Azure-Verbindung herstellen. Nutzen Sie hierfür das folgende Cmdlet: `Set-NspGlobalOffice365AutoImportCredential -ClientId IhreClientID -ClientCertificateThumbprint ThumbprintIhresNoSpamProxyZertifikats`
    - Geben Sie Ihren Mandantennamen und Ihre Client ID an.
6. (Falls kein Zertifikat vorhanden) Wählen Sie ein Zertifikat.
7. Geben Sie unter **Gruppen** an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.
8. (Optional) Weisen Sie unter **Zusätzliche Benutzerfelder** Werte aus dem Verzeichnis den zusätzlichen Benutzerfeldern zu.
9. Klicken Sie **Fertigstellen**.

HINWEIS: Um in NoSpamProxy den automatischen Benutzerimport per Azure Active Directory einzurichten, muss NoSpamProxy als App im Azure-Portal registriert sein. Siehe **Registrieren von NoSpamProxy in Microsoft Azure**.

HINWEIS: NoSpamProxy unterstützt keine öffentlichen Ordner, da diese seitens Azure Active Directory ebenfalls nicht mehr unterstützt werden.

Neuer Benutzerimport über generisches LDAP

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Klicken Sie **Automatischer Benutzerimport** und dann **Hinzufügen**.
3. Wählen Sie **Generisches LDAP** als Typ des Benutzerimports.
4. Bestimmen Sie unter **Allgemein** einen eindeutigen Namen, den Aktualisierungszyklus sowie den Status des Benutzerimports.
5. Geben Sie den Server sowie den Port ein und wählen Sie die Art der Authentifizierung.
6. Geben Sie den Search Root sowie den Klassennamen an, unter dem die Gruppen zu finden sind.

   TIPP: Sie können die Suche durch Anwendung eines Filters auf Benutzer mit bestimmten Eigenschaften einschränken. Außerdem können Sie die LDAP-Suche im Verzeichnis auf bestimmte Container einschränken.

7. Geben Sie unter **LDAP-Adressfelder** zusätzliche LDAP-Felder an, in denen nach E-Mail-Adressen gesucht werden soll. Dies ist notwendig, falls Ihr System die E-Mail-Adressen nicht in den Standardfeldern **mail** oder **otherMailBox** speichert.
8. Geben Sie unter Gruppen an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig der jeweiligen Gruppenmitgliedschaft.
9. Klicken Sie **Fertigstellen**.

> **TIPP:** Die **Zusätzlichen Benutzerfelder** eines Benutzers können durch den Benutzerimport direkt mit Werten gefüllt werden. Unter DISCLAIMER erfahren Sie, wie Sie zusätzliche Benutzerfelder innerhalb eines automatischen Benutzerimports konfigurieren.

Neuer Benutzerimport per Textdatei

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Klicken Sie **Automatischer Benutzerimport** und dann **Hinzufügen**.
3. Wählen Sie **Textdatei** als Typ des Benutzerimports.
4. Bestimmen Sie unter **Allgemein** einen eindeutigen Namen, den Aktualisierungszyklus sowie den Status des Benutzerimports.
5. Geben Sie den Pfad zu der Datei an, die die Benutzeradressen enthält.
6. Wählen Sie unter **Inhaltsfilterung** die Richtlinien für eingehende und ausgehende E-Mails.
7. Klicken Sie **Fertigstellen**.

HINWEIS: Die Textdatei benötigt kein spezielles Format. Alle E-Mail-Adressen werden formatunabhängig gefunden und importiert.

HINWEIS: 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 unter konfiguriert.

Neue Gruppe im Benutzerimport

HINWEIS: Um Funktionen für Benutzergruppen freizugeben, muss eine Active-Directory-Verbindung oder LDAP-Verbindung konfiguriert sein.

HINWEIS: Der Bereich von Active-Directory-Gruppen muss vom Typ **Universell** sein. Weitere Informationen zu Gruppenbereichen finden Sie in der **Microsoft-Dokumentation**.

Gehen Sie folgendermaßen vor:

1. Suchen Sie nach der Gruppe, die Sie berechtigen wollen und wählen Sie diese aus.

> **HINWEIS:** Falls Sie NoSpamProxy Large Files oder NoSpamProxy Protection lizenziert haben, können Sie für jede Gruppe die verwendeten Inhaltsfilter auswählen.

2. Wählen Sie die Inhaltsfilter für eingehende und ausgehende E-Mails aus.
3. Setzen Sie die stündlichen und täglichen Limits für den Flow Guard.
4. Wählen Sie, ob Sie alle Mitglieder der Gruppe für die CxO-Betrugserkennung nutzen wollen.
5. Wählen Sie unter **Automatische Schlüsselanforderung** einen bereits konfigurierten Anbieter für kryptographische Schlüssel. Die Intranetrolle wird mit dem Anbieter einen Schlüssel erstellen, falls nicht bereits ein gültiger Schlüssel vorhanden ist.
6. Legen Sie fest, welche De-Mail Funktionen den Mitgliedern dieser Gruppe zu Verfügung gestellt werden.

   > **HINWEIS:** Alle Benutzer, die De-Mail nutzen wollen, benötigen eine De-Mail-Adresse. Diese können Sie über die Adressverwaltung nach einem Ersetzungsmuster erstellen lassen oder manuell über eine 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, ist dieser Dialog nicht benutzbar.

7. (Falls De-Mail verfügbar ist) Wählen Sie aus, ob die Adressumschreibung automatisch nach dem hinterlegten Muster oder manuell über den

Adressumschreibungsknoten erstellt werden soll.

> **HINWEIS:** 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.

8. (Falls De-Mail verfügbar ist) Nutzen Sie eine der vordefinierten Ersetzungsvorlagen und passen Sie sie an, falls Sie den Ersetzungseintrag nicht vollständig manuell erstellen möchten. Alternativ kann die Gruppen-Mailbox- Funktionalität verwendet werden.
9. Klicken Sie **Beenden**.

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

> **WARNUNG:** Es werden nur E-Mail-Adressen importiert, wenn die Domäne auch in den Unternehmensdomänen von NoSpamProxy hinterlegt ist. Alle anderen werden nicht importiert.

Verfügbare Ersetzungseinträge für die individuellen Einträge bei der automatischen Erstellung von Adressumschreibungen

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.

Adressumschreibung einrichten

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 der 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 – zum Beispiel **info@example.com** – umgeschrieben.

Gehen Sie folgendermaßen vor:

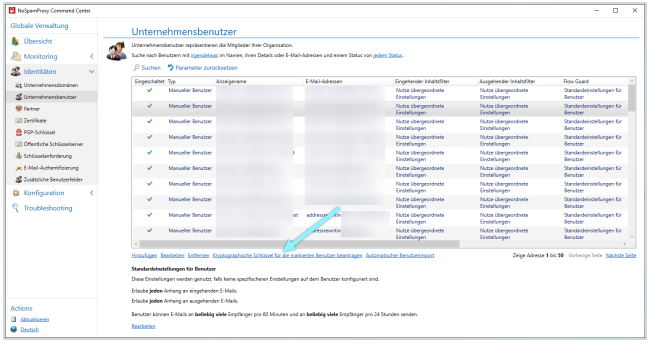
1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Doppelklicken Sie den Benutzer, für den Sie eine Adressumschreibung einrichten wollen oder markieren Sie diesen und klicken Sie **Bearbeiten**.
3. Wechseln Sie zur Registerkarte **E-Mail-Adressen**.
4. Doppelklicken Sie die E-Mail-Adresse, die Sie umschreiben wollen oder markieren Sie diese und klicken Sie **Bearbeiten**.
5. Wechseln Sie zur Registerkarte **Adressumschreibung** und klicken Sie **Hinzufügen**.

6. Geben Sie Folgendes an:
    - eine externe Adresse, die zum Senden verwendet wird.
    - das Verhalten beim Empfang von E-Mails für die externe Adresse.
7. Klicken Sie **Weiter**.
8. Geben Sie den Bereich an, für den die externe Adresse verwendet wird.
9. Klicken Sie **Fertigstellen**.

Kryptographische Schlüssel beantragen

> **HINWEIS:** Stellen Sie sicher, dass Sie Schlüsselanbieter konfiguriert haben. Siehe **Zertifikatsanbieter konfigurieren** beziehungsweise **PGP-Schlüssel verwalten**.

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Wählen Sie die entsprechenden Benutzer in der Liste der Unternehmensbenutzer aus.
3. Klicken Sie **Kryptographische Schlüssel für die markierten Benutzer beantragen**.



4. Wählen Sie einen der konfigurierten Schlüsselanbieter.

5. Klicken Sie **Weiter**.
    - **Schlüsselanforderungsvorfälle**| Hier 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 der Funktion **Entferne ausgewählte Benutzer aus der Schlüsselanforderung** erfolgen.
    - **E-Mail-Adresse/Allgemeiner Name**| Hier 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 eventuell 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.
6. Klicken Sie **Weiter** und dann **Schlüssel anfordern und schließen**.

Die kryptographischen Schlüssel werden beantragt und erscheinen nach Ihrer Fertigstellung unter den jeweiligen Unternehmensbenutzern.

Siehe auch

PGP-Schlüssel verwalten

Kryptographische Schlüssel verwenden

> **HINWEIS:** Die Verwaltung der Domänenzertifikate und Domänen-PGP-Schlüssel unter den Unternehmensdomänen und die Verwaltung der Zertifikate und PGP-Schlüssel unter den E-Mail-Adressen eines Unternehmensbenutzer läuft in allen Bereichen praktisch identisch ab. Der Vorgang der Schlüsselauswahl wird an dieser Stelle zentral beschrieben.

Um einen kryptographischen Schlüssel für Ihre Domänen zu verwenden, müssen Sie mehrere Schritte durchführen.

1. Importieren Sie den Schlüssel für Ihre Unternehmensdomäne. Siehe **Zertifikate verwalten** beziehungsweise **PGP-Schlüssel importieren**.
2. Stellen Sie sicher, dass sich die Domäne des Schlüssels auch in Ihren Unternehmensdomänen befindet.
3. Legen Sie einen Benutzer in dem **Unternehmensbenutzer** an, dem die E-Mail-Adresse des Zertifikats zugeordnet wird.
   Diese E-Mail-Adresse enthält automatisch Ihr importiertes Zertifikat.
4. Gehen Sie über die Funktion **Kryptographische Schlüssel bearbeiten** zu den kryptographischen Schlüsseln der E-Mail-Adresse.
5. Wählen Sie dort den importierten Schlüssel aus und dann die **Zum Domänen-Zertifikaten heraufstufen** oder **Zum Domänen-PGP-Schlüssel heraufstufen**.

Durch das Heraufstufen wird der Schlüssel aus der lokalen E-Mail-Adresse in die Unternehmensdomänen verschoben.

> **HINWEIS:** Kontrollieren Sie nach dem Abspeichern in der betroffenen Unternehmensdomäne die Signatur und Verschlüsselungseinstellungen für Ihr Domänenzertifikat.

Standardeinstellungen für Benutzer konfigurieren

Hier legen Sie fest, welche für einen Benutzer angewendet werden, falls keine Einstellungen auf diesem Benutzer konfiguriert sind.

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Standardeinstellungen für Benutzer**.
2. Klicken Sie **Bearbeiten**.
3. Wählen Sie das gewünschte Verhalten des Inhaltsfilters für eingehende E-Mails (Eingehender Filter) und ausgehende E-Mails (Ausgehender Filter). Siehe **Inhaltsfilter**.

   > Dieser Bereich ist verfügbar, wenn Sie die entsprechende Lizenz erworben haben.

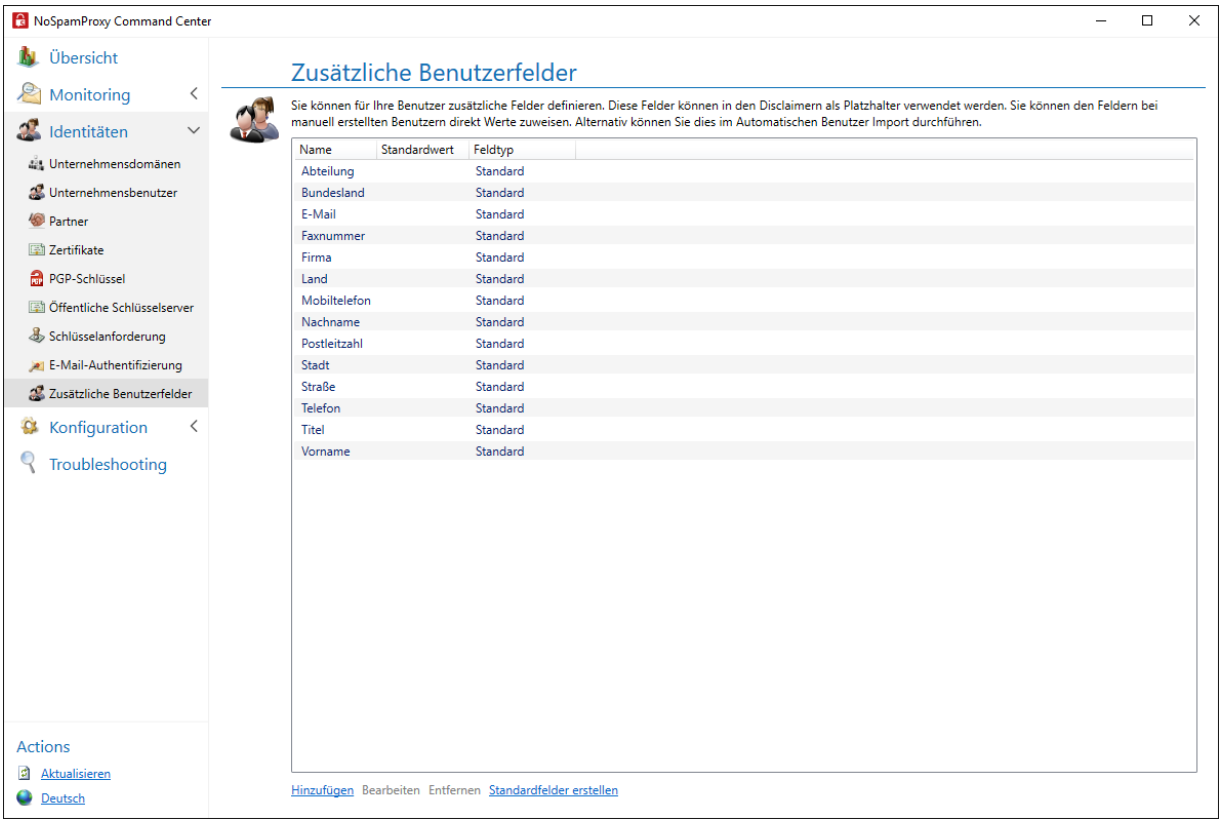
4. Wählen Sie das gewünschte Verhalten des Flow Guard. Siehe **Flow Guard**.
5. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** Inhaltsfilter, die für **Partner** konfiguriert sind, werden ebenfalls angewendet.

Zusätzliche Benutzerfelder hinzufügen

> Dieser Bereich ist verfügbar, wenn Sie die entsprechende Lizenz erworben 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 eingesetzten Werte ersetzt.



1. Gehen Sie zu **Identitäten > Zusätzliche Benutzerfelder > Zusätzliche Benutzerfelder**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie einen Namen für das Feld ein.
4. (Optional) Geben Sie einen Standardwert ein. Dieser Wert wird verwendet, wenn auf dem Benutzer selbst kein Wert gesetzt wird.

TIPP:
Für die meisten Anwendungsfälle ist es empfehlenswert, **Standardfelder erstellen** zu wählen. Dadurch werden häufig genutzte Felder erstellt. Beim Erstellen der Felder wird automatisch die Zuordnung der Benutzerfelder zu Active-Directory-Feldern vorgenommen. Diese Zuordnung können Sie später manuell anpassen.

Standardwerte 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.

Siehe **Benutzerimport automatisieren**.

HINWEIS:

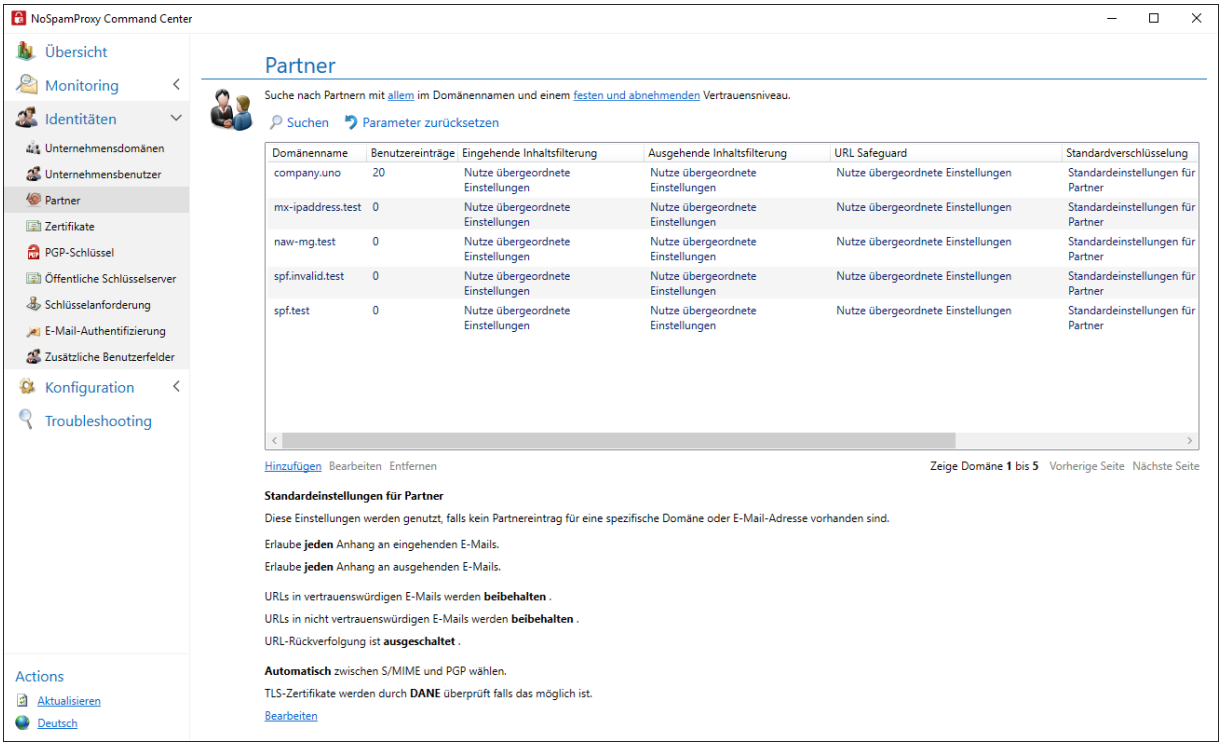
- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden im Vorlagen-Editor mit einem Stern (*) dargestellt, also beispielsweise **[*BenutzerdefiniertesBenutzerfeld]**. Ausgenommen sind Platzhalter in Vorlagen, die mit NoSpamProxy Version 13.2 oder kleiner erstellt wurden.
- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden nicht lokalisiert.

HINWEIS: 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 einen 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. Siehe **Benutzerimport automatisieren**.

Partner

Partner sind externe Kommunikationspartner, mit denen Sie E-Mails austauschen. Einstellungen für Partner können auf den jeweiligen Partnern, der zugehörigen Partnerdomäne oder der jeweiligen E-Mail-Adresse des Partners erfolgen. Die Liste der Partner ist nach den jeweiligen Domänen gruppiert.

> **HINWEIS:** Die Einstellungen auf einer E-Mail-Adresse haben Vorrang vor den Einstellungen auf einer Domäne. Ebenso haben die Einstellungen auf einer Domäne Vorrang vor den Standardeinstellungen für Partner.



Automatisches Entfernen von Partnern

Partner werden automatisch entfernt, wenn der Level-of-Trust-Wert der jeweiligen Domäne auf 0 gesunken ist **und** der Partner keine weiteren Eigenschaften besitzt, die dies verhindern, also beispielsweise hinterlegte Benutzer, Passworte oder Zertifikate.

Verwandte Schritte

Standardverhalten bestimmen| Das grundlegende Verhalten für vertrauenswürdige und nicht vertrauenswürdige E-Mails konfigurieren Sie unter **Standardeinstellungen für Partner**.

Neue Partnerdomäne erstellen| Um eine Domäne für einen Partner zu erstellen, legen Sie diese in NoSpamProxy an. Siehe **Partnerdomänen hinzufügen**.

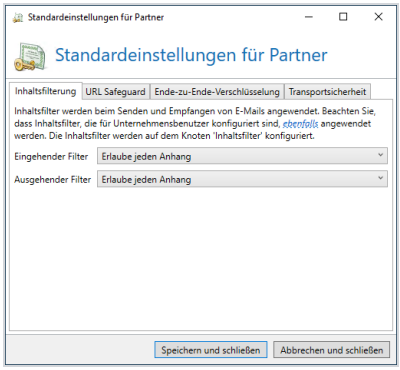
Benutzer hinzufügen| Neue Benutzer einer Domäne fügen Sie der entsprechenden Domäne als Benutzereintrag hinzu. Siehe **Benutzereinträge zu Partnerdomänen hinzufügen**.

Standardeinstellungen für Partner

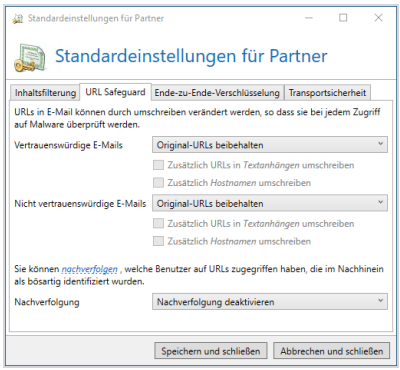
Unter **Identitäten > Partner > Standardeinstellungen für Partner** nehmen Sie Einstellungen vor, die angewendet werden, wenn keine Partnereinträge für eine Domäne oder E-Mail-Adresse vorhanden sind.

- Klicken Sie **Bearbeiten**, um das Dialogfenster **Standardeinstellungen für Partner** zu öffnen.

Inhaltsfilterung| Wählen Sie jeweils eine Richtlinie für E-Mail-Anhänge an eingehenden und ausgehenden E-Mails. Inhaltsfilter werden unter **Inhaltsfilter** konfiguriert.

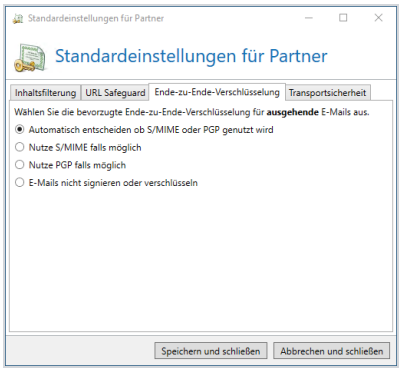


URL Safeguard| Konfigurieren Sie das grundlegende Verhalten des URL Safeguards für vertrauenswürdige und nicht vertrauenswürdige E-Mails. Bestimmen Sie außerdem, ob die Rückverfolgung ein- oder ausgeschaltet sein soll.

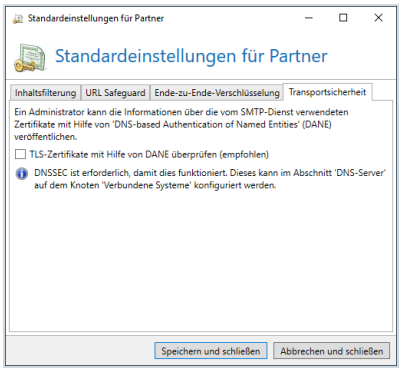


> **TIPP:** Mit Hilfe der Rückverfolgung können Sie nachvollziehen, welche Benutzer auf URLs zugegriffen haben, die sich **danach** als bösartig herausgestellt haben. Details finden Sie dann auf der Registerkarte **URL Safeguard** des jeweiligen Message Tracks. Siehe auch **URL Tracking**.

Ende-zu-Ende-Verschlüsselung| Wählen Sie die gewünschte Ende-zu-Ende-Verschlüsselung.



Transportsicherheit| Konfigurieren Sie die Benutzung eines DNSSEC-fähigen DNS-Servers.



HINWEIS: Durch die Benutzung von **DNS-based Authentication of Named Entities** (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. Um die Absicherung der TLS-Zertifikate über DANE zu erreichen, müssen Sie unter **Verbundene Systeme** einen DNSSEC-fähigen **DNS-Server** konfigurieren.

Partnerdomänen hinzufügen

Jede Partnerdomäne beinhaltet Einstellungen für **Inhaltsfilter**, Ende-zu-Ende-Verschlüsselung, die notwendige Transportsicherheit und das Vertrauen zwischen den Domänen.

1. Gehen Sie zu **Identitäten > Partner > Partner** und klicken Sie **Hinzufügen**.
2. Geben Sie den Namen der Partnerdomäne ein.
3. Wählen Sie die Einstellungen für Inhaltsfilter für eingehende und ausgehende E-Mails.
4. Wählen Sie die Einstellungen für den URL Safeguard.

   > Details zu den Konfigurationsmöglichkeiten finden Sie unter **URL Safeguard einrichten**.

5. Legen Sie die Ende-zu-Ende-Verschlüsselung fest.

   > **HINWEIS:** Sie können hier auch die genutzten S/MIME-Algorithmen auf bestimmte Werte 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. Siehe **Ende-zu-Ende-Verschlüsselung**.

6. Legen Sie ein Domänenpasswort fest. Das Domänenpasswort wird genutzt, um PDF-Anhänge und PDF Mails zu schützen.

7. Wählen Sie die Transportsicherheit für diese Domäne. Die Transportsicherheit legt fest, ob die Kommunikation zu den Server der Partnerdomäne verschlüsselt erfolgen muss und welchen Zertifikaten gegebenenfalls vertraut wird.

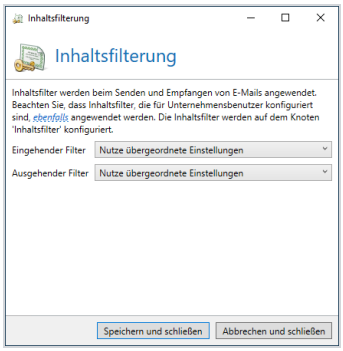
   > **HINWEIS:** Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielserver eingesetzt werden können. Zum Deaktivieren der Transportsicherheit entfernen Sie die Häkchen aus allen Kontrollkästchen.

8. Geben Sie das Vertrauen in diese Domäne an. Das Vertrauen in eine Domäne wird durch an die Domäne gesandte E-Mails stärker und nähert sich ohne weitere E-Mail-Kommunikation mit der Zeit wieder dem Wert 0 an. Sie können das Vertrauen auch auf einen festen Wert einstellen. Siehe **Level of Trust**.
9. Klicken Sie **Fertigstellen**.

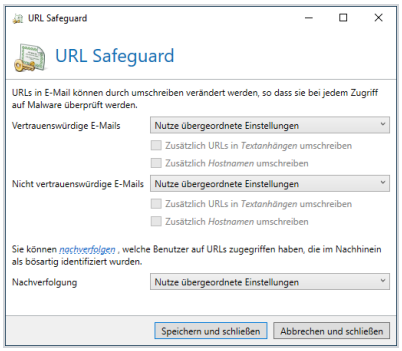
Partnerdomänen bearbeiten

1. Gehen Sie zu **Identitäten > Partner > Partner**.
2. Doppeklicken Sie die Domäne, die Sie bearbeiten wollen und bleiben Sie auf der Registerkarte **Domäneneintrag**.

3. Wählen Sie die Einstellungen für **Inhaltsfilter** für eingehende und ausgehende E-Mails.

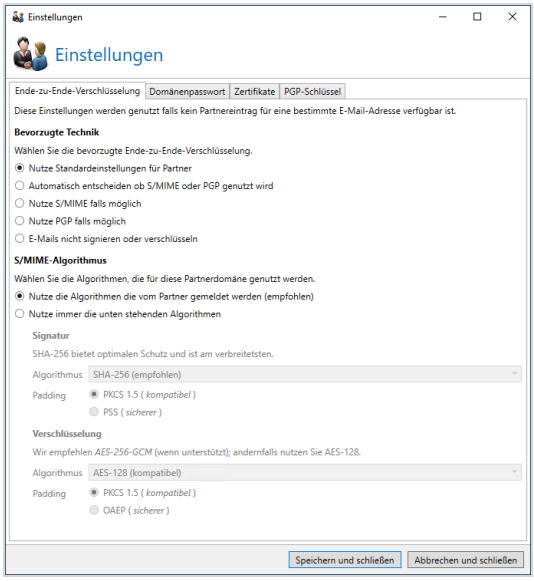


4. Konfigurieren Sie das grundlegende Verhalten des URL Safeguards für vertrauenswürdige und nicht vertrauenswürdige E-Mails. Bestimmen Sie außerdem, ob die Rückverfolgung ein- oder ausgeschaltet sein soll. Von uns empfohlene Einstellungen finden Sie unter **Empfohlene Partner-Einstellungen für den URL Safeguard**.



> **TIPP:** Mit Hilfe der Rückverfolgung können Sie nachvollziehen, welche Benutzer auf URLs zugegriffen haben, die sich **danach** als bösartig herausgestellt haben. Details finden Sie dann auf der Registerkarte **URL Safeguard** des jeweiligen Message Tracks. Siehe auch **URL Tracking**.

5. Machen Sie unter **Ende-zu-Ende-Verschlüsselung** folgende Einstellungen:

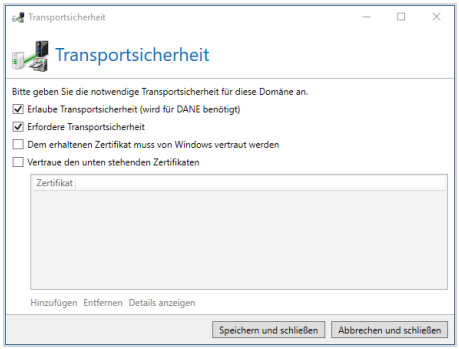


- **Ende-zu-Ende-Verschlüsselung**| Legen Sie die Ende-zu-Ende-Verschlüsselung fest.

> **HINWEIS:** Sie können hier auch die genutzten S/MIME-Algorithmen auf bestimmte Werte 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. Siehe **Ende-zu-Ende-Verschlüsselung**.

- **(Optional) Domänenpasswort**| Legen Sie ein Domänenpasswort fest. Das Domänenpasswort wird genutzt, um PDF-Anhänge und PDF Mails zu schützen.
- **Zertifikate**| Konfigurieren Sie Ihre Zertifikate.
- **PGP-Schlüssel**| Konfigurieren Sie Ihre PGP-Schlüssel.

6. Wählen Sie die Transportsicherheit für diese Domäne. Die Transportsicherheit legt fest, ob die Kommunikation zu den Server der Partnerdomäne verschlüsselt erfolgen muss und welchen Zertifikaten gegebenenfalls vertraut wird. Siehe **Transportsicherheit**.



> **HINWEIS:** Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielserver eingesetzt werden können. Zum Deaktivieren der Transportsicherheit entfernen Sie die Häkchen aus allen Kontrollkästchen.

7. Geben Sie das Vertrauen in diese Domäne an. Das Vertrauen in eine Domäne wird durch an die Domäne gesandte E-Mails stärker und nähert sich ohne weitere E-Mail-Kommunikation mit der Zeit wieder dem Wert 0 an. Sie können das Vertrauen auch auf einen festen Wert einstellen. Siehe **Level of Trust**.

8. Klicken Sie **Dialog schließen**.

> **HINWEIS:** 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.

> **HINWEIS:** Um ein Zertifikat oder einen PGP-Schlüssel zu einem Domänenschlüssel heraufzustufen, gehen Sie zu der Partner-E-Mail-Adresse, die diesen Schlüssel besitzt und klicken **Zum Domänenzertifikat/PGP-Schlüssel heraufstufen**.

Empfohlene Partner-Einstellungen für den URL Safeguard

Wir empfehlen die folgenden Partner-Einstellungen für den URL Safeguard:

Vertrauenswürdige E-Mails| Behalte die originalen URLs bei

Nicht vertrauenswürdige E-Mails| Schreibe die URLs um

Nachverfolgung| URL-Zugriff nachverfolgen

Für **maximale Sicherheit** empfehlen wir die folgenden Einstellungen:

Vertrauenswürdige E-Mails| URLs umschreiben und Zugang sperren, Zusätzlich URLs in Textanhängen umschreiben, Zusätzlich Hostnamen umschreiben

Nicht vertrauenswürdige E-Mails| URLs umschreiben und Zugang sperren, Zusätzlich URLs in Textanhängen umschreiben, Zusätzlich Hostnamen umschreiben

Benutzereinträge zu Partnerdomänen hinzufügen

1. Gehen Sie zu **Identitäten > Partner > Partner** und klicken Sie **Hinzufügen**.
2. Doppelklicken Sie die Domäne, zu der Sie einen Benutzereintrag hinzufügen wollen.
3. Wechseln Sie zur Registerkarte **Benutzereinträge** und klicken Sie **Hinzufügen**.
4. Geben Sie die E-Mail-Adresse für den neuen Benutzer an.
5. Wählen Sie die Einstellungen für Inhaltsfilter für eingehende und ausgehende E-Mails.
6. Wählen Sie die Einstellungen für den URL Safeguard.

   Details zu den Konfigurationsmöglichkeiten finden Sie unter **URL Safeguard einrichten**.

7. Legen Sie die Ende-zu-Ende-Verschlüsselung fest.

   HINWEIS: Sie können hier auch die genutzten S-MIME-Algorithmen auf bestimmte Werte 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.

8. (Optional) Legen Sie ein Benutzerpasswort fest. Das Benutzerpasswort wird genutzt, um PDF-Anhänge und PDF Mails zu schützen.
9. Konfigurieren Sie die Verschlüsselungseinstellungen für vorhandene Zertifikate und PGP-Schlüssel.
10. Klicken Sie **Fertigstellen**.

HINWEIS: Ein Benutzereintrag ist einer E-Mail-Adresse zugeordnet und überstimmt die Einstellungen auf der Domäne, wenn mit dieser E-Mail-Adresse kommuniziert wird.

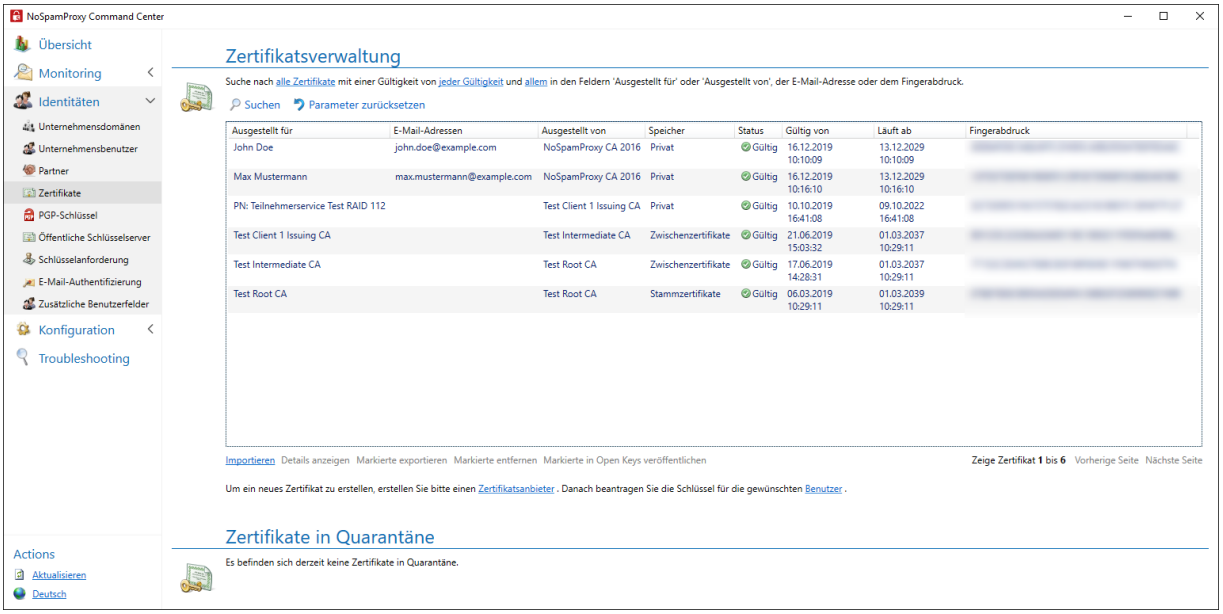
HINWEIS: Sobald ein kryptographischer Schlüssel oder ein Webportal-Passwort für einen bisher unbekannten Partner hinterlegt wird, wird automatisch ein neuer Eintrag für diesen Partner angelegt.

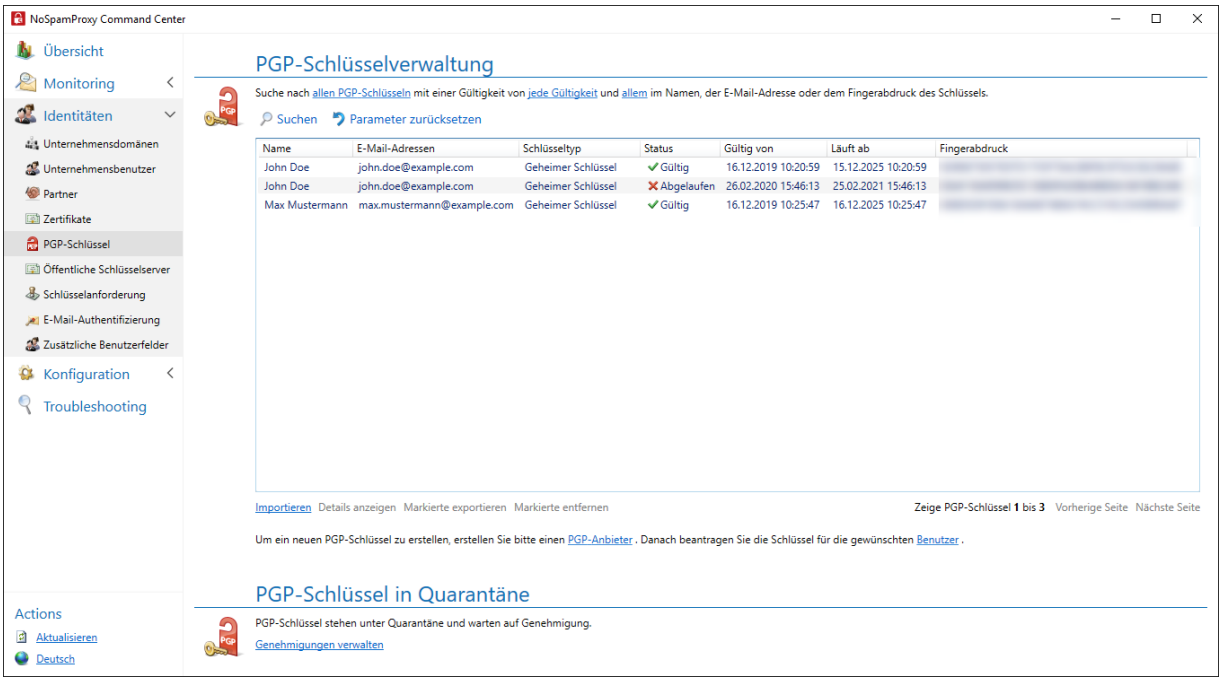
WARNUNG: Das Löschen von kryptographischen Schlüsseln aus einem Partner sowie das Löschen von kryptographischen Schlüsseln aus einer Partnerdomäne oder einer E-Mail-Adresse eines Partners löscht diese Schlüssel endgültig aus NoSpamProxy. Für den Fall, dass Sie sie zu einem späteren Zeitpunkt erneut verwenden wollen, exportieren Sie die Schlüssel vorher. Siehe **PGP-Schlüssel**.

Zertifikate und PGP-Schlüssel

NoSpamProxy Encryption benötigt für den vollständigen Einsatz der Aktionen für E-Mail-Signatur und Verschlüsselung die Zertifikate oder PGP-Schlüssel der Benutzer, die signierte E-Mails an externe E-Mail-Empfänger versenden wollen und verschlüsselte E-Mail-Antworten empfangen wollen.

- Über die Zertifikatsverwaltung haben Sie Zugriff auf alle Zertifikate, die derzeit in NoSpamProxy Encryption gespeichert sind. Dies umfasst sowohl eigene als auch öffentliche Zertifikate sowie Stamm- und Zwischenzertifikate.
- Über die PGP-Schlüsselverwaltung haben Sie Zugriff auf alle PGP-Schlüssel, die derzeit in NoSpamProxy Encryption gespeichert sind.





Unterstützte Zertifikatstypen

NoSpamProxy unterstützt die folgenden Zertifikate:

- Zertifikate, die den Algorithmus Elliptic Curve Digital Signature Algorithm (ECDSA) verwenden. Der Einsatz von ECDSA ermöglicht entsprechend der **RFC 5751** die Verschlüsselung nach dem S/MIME-Standard 4.0.
- Zertifikate, die das Verfahren Rivest–Shamir–Adleman (RSA) verwenden.

Allgemeine Hinweise

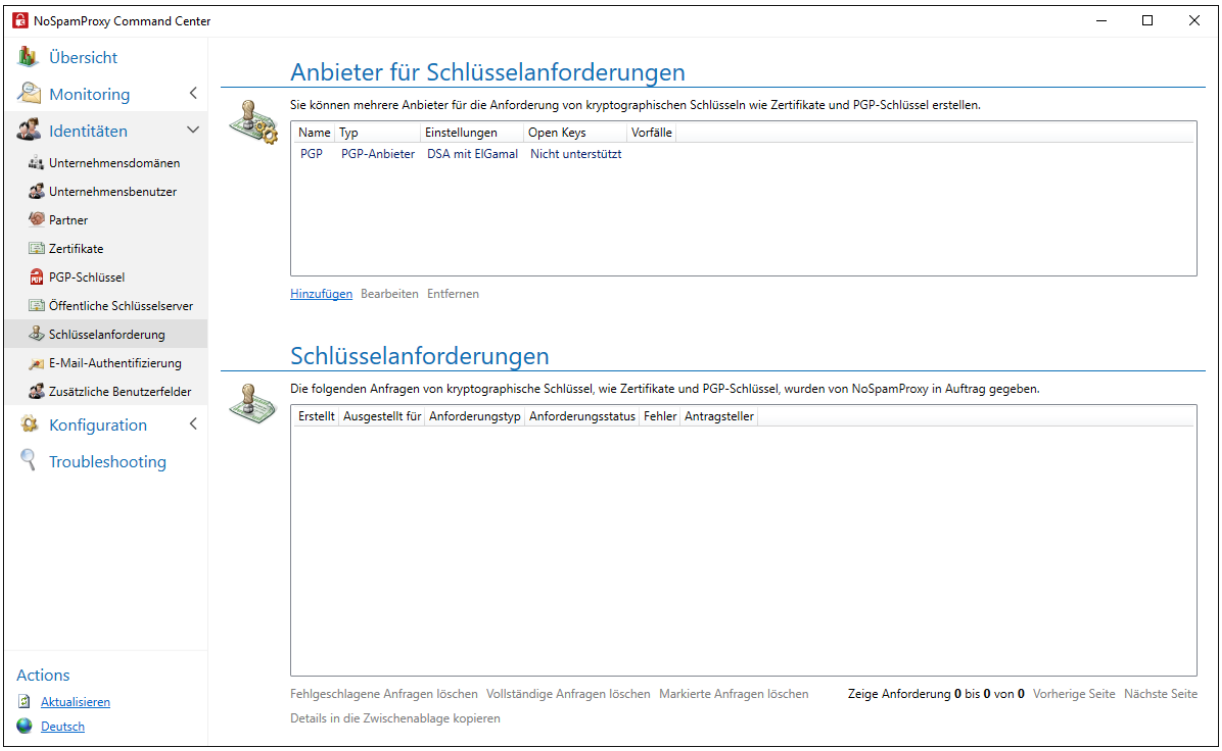
HINWEIS: Die Gatewayrolle sammelt sammelt automatisch öffentliche Zertifikate von E-Mails an lokale Adressen ein.

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

HINWEIS: Sie können weitere Zertifikate aus Dateien in den Dateiformaten **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 beziehungsweise durch diese Aktion gesammelt. Siehe **Signieren und/oder Verschlüsseln von E-Mails**.

Zertifikatsanbieter konfigurieren

Unter **Schlüsselanforderung > Anbieter für Schlüsselanforderungen** können Sie Anbieter konfigurieren, die Zertifikate oder PGP-Schlüssel für die Unternehmensbenutzer von NoSpamProxy Encryption bereitstellen und alle gestellten Zertifikatsanforderungsanfragen einsehen und verwalten.



HINWEIS: Die abgespeicherten Profile stehen bei zukünftigen Schlüsselanforderungen für Unternehmensbenutzer zur Verfügung, ohne die im Profil gespeicherten Einstellungen mehrmals durchführen zu müssen.

Wann werden neue Zertifikate beantragt?

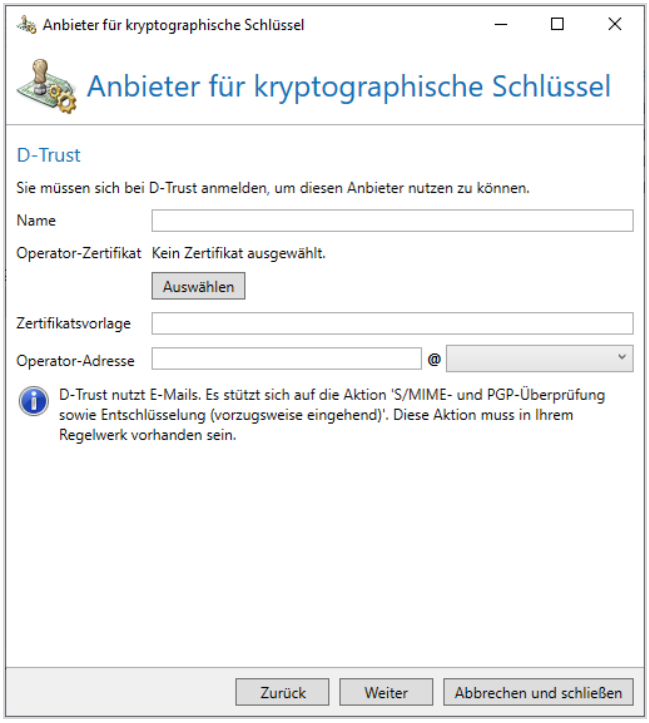
Neue Zertifikate werden automatisch 14 Tage vor Ablauf bei der jeweiligen Managed PKI beantragt.

Siehe auch

PGP-Schlüssel verwalten

D-Trust

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **D-Trust** als Anbieter aus.



4. Tragen Sie den Namen der Zertifikatsvorlage sowie die Operator-Adresse ein. Beide Informationen erhalten Sie von D-Trust.

> **HINWEIS:** Die Operator-Adresse ist die E-Mail-Adresse, die zur Abwicklung von Anfragen verwendet wird. Diese Adresse wird als Absende-Adresse für alle Anfragen verwendet und muss erreichbar sein.

HINWEIS:
Folgende Zertifikatsvorlagen werden unterstützt:

- ADVANCED_PERSONAL_ID_1
- ADVANCED_PERSONAL_ID_2
- ADVANCED_ENTERPRISE_ID_1
- ADVANCED_ENTERPRISE_ID_2
- ADVANCED_TEAM_ID_1
- ADVANCED_TEAM_ID_2

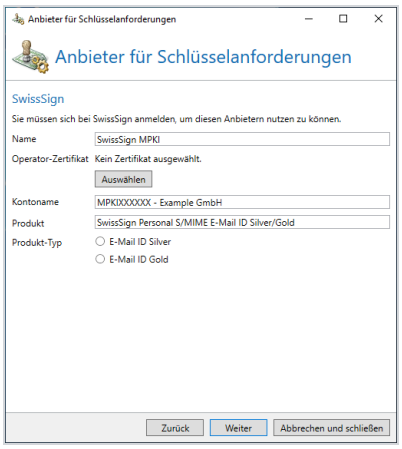
5. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
6. Klicken Sie **Fertigstellen**.

HINWEIS: Um D-Trust als Anbieter nutzen zu können, müssen Sie mit der Deutschen Bundesdruckerei einen gültigen Vertrag abgeschlossen und das Zertifikat von D-Trust in der Zertifikatsverwaltung importiert haben.

SwissSign

HINWEIS: SwissSign bietet ab sofort eine neue MPKI an, welche eine andere URL nutzt. NoSpamProxy nutzt automatisch diese URL, nachdem Sie SwissSign erneut als Anbieter für Schlüsselanforderungen hinzugefügt haben.

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen** und wählen Sie **SwissSign** als Anbieter aus.



3. Wählen Sie das Operator-Zertifikat.
4. Geben Sie den Kontonamen sowie den Produktnamen an und wählen Sie den Produkttyp.

> **HINWEIS:** Für den Kontonamen und für das Produkt nutzen Sie bitte die Daten, die Sie von SwissSign übermittelt bekommen haben. Beachten Sie, dass diese Daten von alten Informationen abweichen können.

5. Klicken Sie **Weiter**.
6. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
7. Klicken Sie **Fertigstellen**.

> **TIPP:** Gemeinsam mit unseren Kollegen von SwissSign ist das folgende Dokument entstanden, das alle Punkte aufführt, die Sie beim Einbinden einer Managed PKI von SwissSign in NoSpamProxy zu beachten müssen: **Hinweise zum Einsatz von NoSpamProxy mit SwissSign-Zertifikaten**

Von NoSpamProxy unterstützte SwissSign Silver-ID-Produkte

NoSpamProxy unterstützt aktuell die folgenden Silver-ID-Produkte:

Silver-Zertifikate ohne State-, Organisations- und Landes-Feld

- Name im Bestellprozess: E-Mail ID Silver, E-Mail-Adresse validiert (Weboberfläche oder Partnerapplikation)
- Ab NoSpamProxy Version: 13.2.21230.1449

> **HINWEIS:** Vor der oben genannten Version wurde die folgende Fehlermeldung angezeigt: **Unconsumed SDN (i.e.: SDN attributes not needed and not utilized; please remove them and resubmit your request): o=[…]**.

Nicht unterstützte Produkte

Das folgende Silver-ID-Produkt wird nicht unterstützt:

Silver-Zertifikate mit State-Feld

- Name im Bestellprozess: E-Mail ID Silver, E-Mail-Adresse validiert, Organisation, Kanton/Bundesland, Land (nur Partnerapplikation)

> **HINWEIS:** Beachten Sie dies im Beschaffungsprozess bei SwissSign und bestellen Sie nur die unterstützten Produkte. Sollten Sie das falsche Produkt bestellt haben, können Sie die **Änderung bei SwissSign mit Hilfe dieses Formulars beantragen**.

Silver-Zertifikate ohne State-Feld

- Name im Bestellprozess: E-Mail ID Silver, E-Mail-Adresse validiert, Organisation, Land (nur Partnerapplikation)
- Ab NoSpamProxy Version: 13.2.21111.1701

> **HINWEIS:** Vor der oben genannten Version wurde die folgende Fehlermeldung angezeigt: **Unconsumed SDN (i.e.: SDN attributes not needed and not utilized; please remove them and resubmit your request): state=[…]**.

Hinweise zu SwissSign-Gold-Produkten

HINWEIS: Wenn Zertifikate für allgemeine oder Systempostfächer angefordert werden sollen, muss vor dem Anzeigenamen (allgemeiner Name/Common Name/CN) ein **Pseudo:** eingefügt werden. Dies kann nicht automatisiert durch NoSpamProxy erfolgen, so dass diese Information aus dem Active Directory oder LDAP kommen. Diese Information zu Beginn stehen und somit idealerweise als Vorname geliefert werden. Um die richtige Reihenfolge im CN zu übermitteln, verwenden Sie die NoSpamProxy Version 13.2.21111.1701 oder höher

GlobalSign Atlas

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **GlobalSign Atlas** als Anbieter aus.

4. Wählen Sie einen Namen für die Schlüsselanforderung.

5. Geben Sie die Zugangsdaten ein.

   > **HINWEIS:** Sie erhalten die Zugangsdaten von GlobalSign.

6. Wählen Sie das mTLS-Zertifikat aus, das Sie nutzen wollen.
7. Wählen Sie, ob und welche der Werte der Felder zur Schlüsselanforderung Sie immer überschreiben wollen. Siehe **Automatisches Überschreiben von Werten**.
8. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
9. Klicken Sie **Fertigstellen**.

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

GlobalSign (legacy)

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.

3. Wählen Sie **GlobalSign (legacy)** als Anbieter aus.

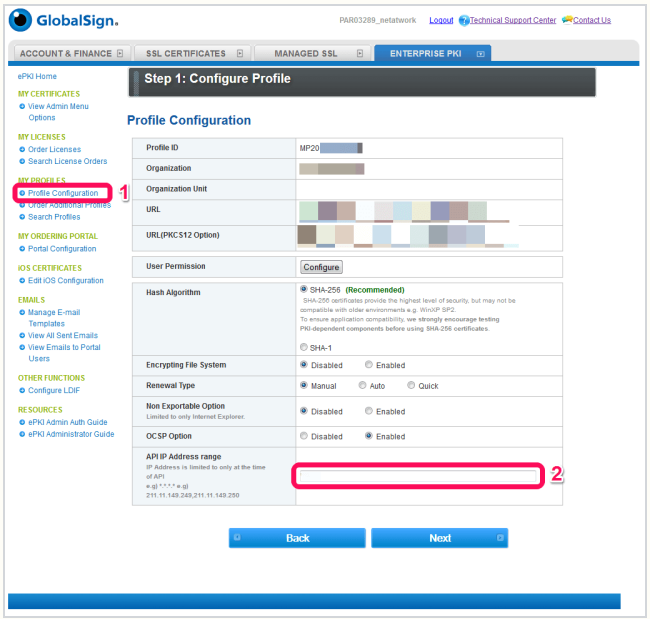
4. Geben Sie die Zugangsdaten ein, die Sie von GlobalSign erhalten haben.

> **HINWEIS:** Nach der Anmeldung bei GlobalSign erhalten Sie die Zugangsdaten für das GlobalSign Management-Portal. Diese Zugangsdaten tragen Sie im GlobalSign-Konfigurationsdialog ein. Im Portal können Sie auch Profile konfigurieren und Zertifikats-Pakete kaufen. Diese Daten tragen Sie hier ebenfalls ein.

5. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
6. Klicken Sie **Fertigstellen**.

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

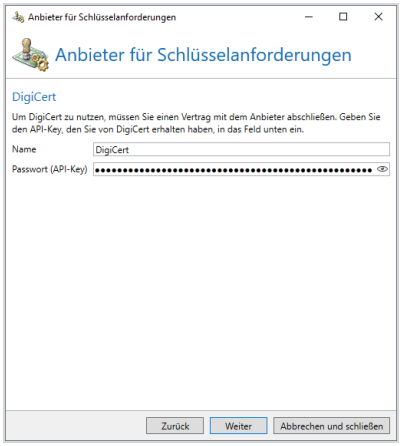
TIPP: Aus Sicherheitsgründen wird die API bei GlobalSign auf bestimmte Anfrage-IP-Adressen limitiert. Damit Sie Ihre Anfragen erfolgreich durchführen können, müssen Sie die öffentlichen IP-Adressen Ihrer Gatewayrollen bei GlobalSign hinterlegen.



DigiCert

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.

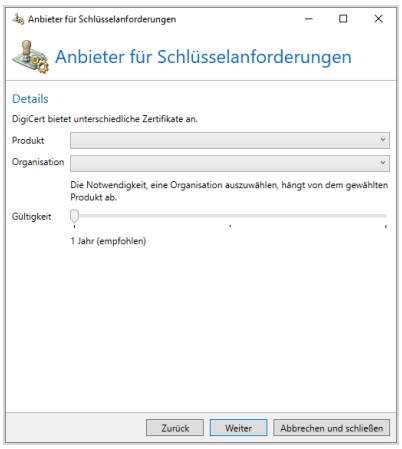
3. Wählen Sie **DigiCert** als Anbieter aus.



4. Geben Sie einen eindeutigen Namen sowie den API-Schlüssel ein, den Sie von DigiCert erhalten haben und klicken Sie **Weiter**.

> **HINWEIS:** Stellen Sie sicher, dass für den API-Schlüssel die Einschränkung **Orders, Domains, Organizations** besteht. Wir raten davon ab, die Einschränkung **keine Einschränkung** zu konfigurieren.

> **HINWEIS:** Der API-Schlüssel muss einem Benutzer zugeordnet sein, der Organisationen anzeigen darf, also entweder **Administrator (uneingeschränkt)** oder **Manager (uneingeschränkt)**.

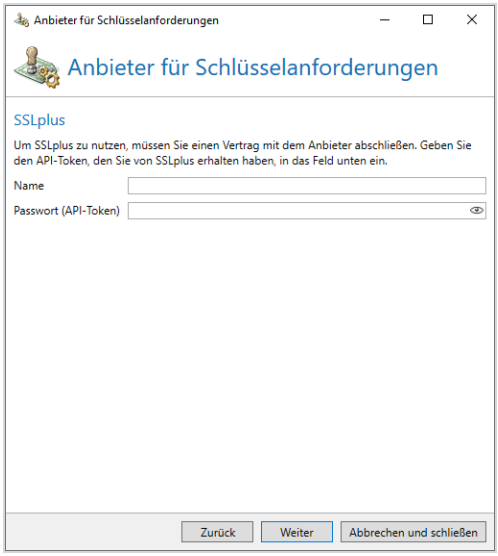


5. Wählen Sie das Produkt, die Organisation sowie die Gültigkeit des Schlüssels und klicken Sie **Weiter**.
6. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
7. Klicken Sie **Fertigstellen**.

SSLplus

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.

3. Wählen Sie **SSLplus** als Anbieter aus.



4. Geben Sie einen eindeutigen Namen sowie den API Token ein, den Sie von SSLplus erhalten haben und klicken Sie **Weiter**.
5. Geben Sie den Namen der CA, den Namen des Produkts sowie die Gültigkeit an und klicken Sie **Weiter**.
6. (Optional) Wählen Sie, ob und welche der Werte der Felder zur Schlüsselanforderung Sie immer überschreiben wollen. Wenn Sie ein Häkchen bei Stadt sowie bei Bundesland oder Bereich setzen, müssen entweder beide Felder ausgefüllt oder beide Felder leer sein.
7. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
8. Klicken Sie **Weiter** und dann **Fertigstellen**.

Deutsches Forschungsnetz (DFN)

Viele Hochschulen und wissenschaftliche Einrichtungen setzen Zertifikate für eine sichere Kommunikation ein. Der DFN-Verein bietet eine Public-Key-Infrastruktur an und übernimmt den technischen Betrieb zentraler Komponenten sowie die

technische und organisatorische Unterstützung für die lokalen Komponenten.

> **HINWEIS:** Weitere Informationen finden Sie auf der Webseite der **DFN-PKI**.

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **Deutsches Forschungsnetz (DFN)** als Anbieter aus.

4. Geben Sie einen eindeutigen Anbieternamen ein und wählen Sie das Zertifikat, das Ihnen durch das DFN zur Verfügung gestellt wurde.
5. Geben Sie den Namen der CA, der Namen der Registrierungsstelle und das Zertifikatsprofil ein. Sie erhalten diese Informationen vom DFN.

6. Kopieren Sie entweder die Sperr-PIN in die Zwischenablage oder erstellen Sie eine neue. Speichern Sie die Sperr-PIN an einem sicheren Ort.
7. Wählen Sie, ob Sie das Zertifikat in das DFN-Verzeichnis aufnehmen wollen und klicken Sie **Weiter**.
8. (Optional) Wählen Sie, ob und welche der Werte der Felder zur Schlüsselanforderung Sie immer überschreiben wollen. Wenn Sie ein Häkchen bei Stadt sowie bei Bundesland oder Bereich setzen, müssen entweder beide Felder ausgefüllt oder beide Felder leer sein.
9. Bestimmen Sie, ob Sie Ihre öffentlichen Schlüssel auf Open Keys veröffentlichen wollen. Siehe **Open Keys**.
10. Klicken Sie **Weiter** und dann **Fertigstellen**.

Windows-Zertifizierungsstelle

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

Voraussetzungen

- Das Betriebssystem des Rechners der Intranetrolle ist Windows 2012 R2 oder neuer.
- Ihre Intranetrolle 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.

1. Gehen Sie zu **Identitäten > Anforderung kryptographischer Schlüssel > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **Windows-Zertifizierungsstelle** aus.
4. Tragen Sie einen eindeutigen Anbieternamen ein.
5. Wählen Sie eine Ihrer Zertifizierungsstellen aus.
   Nach der Auswahl werden alle freigegebenen Zertifikatsvorlagen dieser Stelle angezeigt.
6. Wählen Sie eine Vorlage aus.

   HINWEIS: 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.

7. Tragen Sie die Länderkennung in Form eines ISO 3166-1-konformen Alpha-2-Kürzels an.

> **HINWEIS:** Unter dem Eingabefeld können Sie über die Auswahl der Ländernamen das dazugehörige Alpha-2-Kürzel in das Eingabefeld eintragen lassen.

8. Klicken Sie **Weiter** und dann **Fertigstellen**.

Schlüssel über Open Keys bereitstellen

Sie können Ihre öffentlichen Schlüssel der Anbieter SwissSign, D-Trust und GlobalSign sowie Schlüssel der Active-Directory-Zertifikatsdienste über anderen Personen und Organisationen zur Verfügung stellen.

1. Gehen Sie zu **Identitäten > Öffentliche Schlüsselserver > Open Keys**.
2. Klicken Sie **Bearbeiten**.
3. Setzen Sie das Häkchen neben **Nutze Open Keys (empfohlen)**.

4. Klicken Sie **Speichern und schließen**.

Automatisches Überschreiben von Werten

Für die Anbieter 'D-Trust','GlobalSign Atlas', 'DigiCert', 'SSLPlus', 'DFN' und die Windows-Zertifizierungsstelle 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.

Die folgenden Werte können von den unterschiedlichen Anbietern überschrieben werden:

D-Trust| Organisation, Abteilung, Stadt, Bundesland oder Bereich

GlobalSign Atlas| Organisation, Abteilung, Stadt, Bundesland oder Bereich, Land

GlobalSign (legacy)| Keine

DigiCert| Organisation, Abteilung, Stadt, Bundesland oder Bereich

SSLplus| Organisation, Abteilung, Stadt, Bundesland oder Bereich

Deutsches Forschungsnetz (DFN)| Organisation, Abteilung, Stadt, Bundesland oder Bereich

Windows-Zertifizierungsstelle| Organisation, Abteilung, Stadt, Land

PGP-Schlüssel| Keine

HINWEIS:
Hinweis für Nutzer von GlobalSign Atlas

Wenn Ihr Vertrag für GlobalSign Atlas in der Anfrage keine Werte wie beispielsweise Stadt oder Land zulässt, müssen Sie die Override Values aktivieren und eine leere Zeichenfolge angeben. Der Server filtert leere Zeichenfolgen aus der Anfrage.

Zertifikate verwalten

Zertifikate importieren

1. Gehen Sie zu **Identitäten > Zertifikate > Zertifikatsverwaltung**.
2. Klicken Sie **Importieren**.
3. Klicken Sie **Zertifikate wählen** und wählen Sie die entsprechenden Dateien aus Ihrem Verzeichnis aus.
4. Fügen Sie die Dateien mit **Öffnen** Ihrer Auswahl hinzu. Wiederholen Sie Schritt 3 und 4 beliebig oft.

   > **HINWEIS:** Wenn Sie kryptographische Schlüssel aus mehreren Verzeichnissen importieren möchten, können Sie diesen Vorgang mehrmals wiederholen. Die weiteren ausgewählten Dateien werden ebenfalls der Liste hinzugefügt. Ungewollte Dateien können Sie aus der Liste löschen.

5. Weisen Sie Zertifikatsdateien im PFX- oder P12-Format die entsprechenden Passworte zu.
6. Klicken Sie **Weiter**, um 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.
7. Klicken Sie **Fertigstellen**.

HINWEIS: 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.

HINWEIS: 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 Unternehmensdomänen befinden, die anderen E-Mail-Adressen werden ignoriert. Beim Import eines öffentlichen Schlüssels werden für alle E-Mail-Adressen, deren Domäne nicht zu den Unternehmensdomänen gehört, neue Partner erstellt oder ein bestehender ergänzt. Die übrigen E-Mail-Adressen werden ignoriert.

> **HINWEIS:** 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.

Zertifikate exportieren

1. Gehen Sie zu **Identitäten > Zertifikate > Zertifikatsverwaltung**.
2. Markieren Sie das jeweilige Zertifikat und klicken Sie **Markierte exportieren**.
3. Bestimmen Sie, ob die markierten Zertifikate in einer einzelnen Datei oder in mehreren Dateien gespeichert werden sollen.
4. Bestimmen Sie das Format, in der die Zertifikatsdatei gespeichert werden soll.
5. Geben Sie den Dateinamen beziehungsweise den Zielordner für alle exportierten Zertifikate an.
6. Klicken Sie **Fertigstellen**.

Zertifikate anfordern, sperren oder heraufstufen

In NoSpamProxy können Sie Zertifikate über eine Managed PKI eines externen Zertifikatsanbieters anfordern und sperren. Zusätzlich können Sie Zertifikate zu einem Domänenzertifikat – auch Gatewayzertifikat genannt – für Unternehmensdomänen oder Partnerdomänen heraufstufen. Wenn kein eigenes

Zertifikat für den Empfänger beziehungsweise Absender vorliegt, werden mit einem Domänenzertifikat **alle** E-Mails verschlüsselt, entschlüsselt oder signiert, jeweils abhängig von Zertifikat und Richtung.

HINWEIS:
Die folgenden Voraussetzungen müssen gegeben sein:

- Das NoSpamProxy Encryption ist lizenziert.
- Ein Zertifikatsanbieter ist eingerichtet (für das Anfordern und Sperren).
- Das Zertifikat ist für das gesamte Unternehmen nutzbar (um das Zertifikat heraufzustufen)

TIPP:
Hinweis für Managed Service Provider

Stellen Sie sicher, dass Sie für die von Ihnen administrierten Mandanten ausreichend Verwaltete Zertifikate (Managed Certificates) vergeben, wenn auch eine Managed PKI angebunden werden soll. Ansonsten kommt es zu Unterlizenzierung.

Zertifikate anfordern (manuell über Benutzer)

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Markieren Sie den Kontakt.
3. Klicken Sie **Kryptographische Schlüssel für die markierten Benutzer beantragen** und folgen Sie den Anweisungen im Dialog.

Zertifikate anfordern (automatisch über eine Benutzergruppe)

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Klicken Sie **Automatischer Benutzerimport**.
3. Markieren Sie den betroffenen Active-Directory-Import markieren und klicken Sie **Bearbeiten**.
4. Markieren Sie auf dem Reiter **Gruppen** die Active-Directory-Gruppe und klicken Sie **Hinzufügen**.
5. Wählen Sie im Dialog **Automatische Schlüsselanforderung** den entsprechenden Anbieter aus und bestätigen Sie.

> **HINWEIS:** Bei jedem Active-Directory-Import (nach Zeitplan oder manuell gestartet) wird geprüft, ob für einen Benutzer der Gruppe ein neues Zertifikat benötigt wird.

Zertifikate sperren

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Markieren Sie den Kontakt und klicken Sie **Bearbeiten**.
3. Wählen Sie auf dem Reiter **E-Mail-Adressen** die E-Mail-Adresse mit dem Zertifikat aus und klicken Sie **Bearbeiten**.
4. Markieren Sie auf dem Reiter **Zertifikate** das Zertifikat, das gesperrt werden soll.
5. Klicken Sie **Sperren**.
6. Folgen Sie den Anweisungen im Dialog.

Zertifikat für Partnerdomäne heraufstufen

> **HINWEIS:** Das Heraufstufen eines Zertifikats führt dazu, dass es für ein gesamtes Unternehmen genutzt wird. Die Gegenseite muss dies immer unterstützen und erlauben, dass das Zertifikat dafür genutzt werden darf. Bei Fragen zum Zertifikat wenden Sie sich bitte an die ausstellende Behörde.

1. Gehen Sie zu **Identitäten > Partner**.
2. Markieren Sie die Partnerdomäne und klicken Sie **Bearbeiten**.
3. Markieren Sie auf dem Reiter **Benutzereinträge** den Benutzer mit dem Domänenzertifikat und klicken Sie **Bearbeiten**.
4. Markieren Sie auf dem Reiter **Zertifikate** das Zertifikat, das heraufgestuft werden soll und klicken Sie **Zu Domänenzertifikaten heraufstufen**.
5. Folgen Sie den Anweisungen im Dialog.

Das Zertifikat ist nach dem Heraufstufen nicht mehr im Benutzereintrag zu finden, sondern auf dem Reiter **Domäneneintrag** unter **Ende-zu-Ende-Verschlüsselung > Bearbeiten** auf dem Reiter **Zertifikate**.

Zertifikat für Unternehmensdomäne heraufstufen

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
2. Markieren Sie den Kontakt und klicken Sie **Bearbeiten**.
3. Wählen Sie auf dem Reiter **E-Mail-Adressen** die E-Mail-Adresse mit dem Zertifikat und klicken Sie **Bearbeiten**.
4. Markieren Sie auf dem Reiter **Zertifikate** das Zertifikat, das heraufgestuft werden soll.

5. Klicken Sie Zu **Domänenzertifikat heraufstufen**.
6. Folgen Sie den Anweisungen im Dialog.

Das Zertifikat ist nach dem Heraufstufen nicht mehr im Kontakt zu finden, sondern unter **Unternehmensdomänen** in der betroffenen Domäne auf dem Reiter **Zertifikate**.

Zertifikate auf Gültigkeit prüfen

Sobald Zertifikate und deren Zertifikatsketten für die E-Mail-Signatur oder -Verschlüsselung genutzt werden, müssen diese normalerweise auf Gültigkeit geprüft werden. Beachten Sie, dass bestimmte Grundvoraussetzungen erfüllt sein müssen, damit ein Endzertifikat als gültig betrachtet wird.

- Das Zertifikat inklusive seiner vollständigen Zertifikatskette ist im Zertifikatsspeicher von NoSpamProxy hinterlegt.
- Die Sperrprüfung des Endzertifikats und aller in der Zertifikatskette enthaltenen Zwischenzertifikate war erfolgreich.

Über die Certificate Revocation List

Beachten Sie, dass die Prüfung bevorzugt auf Basis des Online Certificate Status Protocol durchgeführt wird. Bietet das jeweilige Zertifikat diese nicht an, wird auf die Prüfung via Zertifikatsperrliste (Certificate Revocation List, CRL) zurückgegriffen. Beim Abruf der CRL jedes Zertifikats müssen drei Dinge gegeben sein:

- Die CRL ist von allen Gateways aus abrufbar.
- Die CRL selbst ist noch gültig.
- Das betroffene Zertifikat ist nicht auf der Zertifikatsperrliste.

Die Gültigkeit der CRL kann durch einen einfachen Abruf (im Falle einer per HTTP-verlinkten Liste) per Browser und anschließendem Öffnen mit Windows-Bordmitteln geprüft werden. Beachten Sie hierbei eventuell greifende Proxy-Einstellungen. Siehe auch **Konfigurieren eines Webproxy für NoSpamProxy 9.2 und höher**.

Prüfung mit Hilfe eines automatisierten Skripts

Am einfachsten ist die Prüfung mit Hilfe eines automatisierten Skripts durchführbar.

1. Melden Sie sich auf dem System an, auf dem die Intranetrolle installiert ist.
2. Führen Sie dort das **Skript** aus. Nutzen Sie dazu wahlweise die PowerShell-Kommandozeile oder die PowerShell ISE. Nach dem Ausführen des Skripts werden Sie nach dem Fingerabdruck des Zertifikats gefragt, das geprüft werden soll
3. Gehen Sie zum Message Track der betroffenen E-Mail.
4. Öffnen Sie die Registerkarte **Aktivitäten**. Sie finden dort den Namen des Antragstellers als Link.
5. Rechtsklicken Sie den Link, um ihn zu kopieren.
6. Geben Sie den Fingerabdruck ein.

Siehe auch

Der Sperrstatus eines Zertifikats kann nicht abgerufen werden

Zertifikate in Quarantäne

Zertifikate, 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.

Unter **Zertifikate in Quarantäne** sehen Sie die Zertifikate, die derzeit in Quarantäne gestellt sind.

- Klicken Sie **Markierte genehmigen**, um die markierten Schlüssel zu bestätigen und damit für die weitere Nutzung zu aktivieren.
- Klicken Sie **Markierte ablehnen**, um die markierten Schlüssel abzulehnen und zu löschen.

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

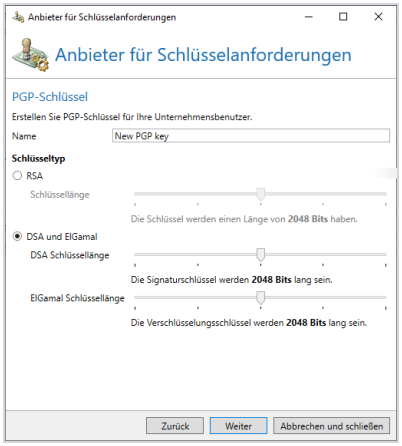
PGP-Schlüssel verwalten

PGP-Schlüssel erstellen

Sie können PGP-Schlüssel mit unterschiedlichen Verschlüsselungsalgorithmen und Schlüssellängen erstellen.

1. Gehen Sie zu **Identitäten > Schlüsselanforderung > Anbieter für Schlüsselanforderungen**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **PGP-Schlüssel** aus und klicken Sie **Weiter**.

4. Geben Sie einen eindeutigen Namen ein.



5. Wählen Sie den PGP-Schlüsseltyp sowie die Schlüssellänge und klicken Sie **Weiter**.

> **HINWEIS:** Es stehen 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 bei diesen, welche Schlüsselalgorithmen und Schlüssellängen von Ihrer Infrastruktur unterstützt wird.

6. Bestimmen Sie die Gültigkeit für den Schlüssel.

> **TIPP:** Dies ist sinnvoll, da aufgrund von steigender Rechenkapazität Schlüssel mit höherer Schlüssellänge notwendig werden können.

7. Signieren Sie die neuen Schlüssel mit einem bestehenden Schlüssel.

> **TIPP:** Dies kann in bestimmten Situationen den Schlüsselaustausch vereinfachen, da dann nur noch der übergeordnete Schlüssel - beispielsweise der Firmenschlüssel ausgetauscht werden muss. Alle mit diesem Schlüssel signierten PGP-Schlüssel gelten dann automatisch als vertrauenswürdig.

8. Klicken Sie **Fertigstellen**.

Siehe auch

Kryptographische Schlüssel beantragen

PGP-Schlüssel importieren

Sie können sowohl öffentliche als auch private oder geheime kryptographische Schlüssel manuell importieren.

1. Gehen Sie zu **Identitäten > PGP-Schlüssel > PGP-Schlüsselverwaltung**.
2. Klicken Sie **Importieren**.
3. Klicken Sie **PGP-Schlüssel für den Import auswählen** und wählen Sie die entsprechenden Dateien aus Ihrem Verzeichnis aus.
4. Fügen Sie die Dateien mit **Öffnen** Ihrer Auswahl hinzu. Wiederholen Sie Schritt 3 und 4 beliebig oft.

> **HINWEIS:** Wenn Sie kryptographische Schlüssel aus mehreren Verzeichnissen importieren möchten, können Sie diesen Vorgang mehrmals wiederholen. Die weiteren ausgewählten Dateien werden ebenfalls der Liste hinzugefügt. Ungewollte Dateien können Sie aus der Liste löschen.

5. Weisen Sie passwortgeschützten PGP-Schlüsseln die entsprechenden Passworte zu.
6. Klicken Sie **Weiter**, um 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.
7. Klicken Sie **Fertigstellen**.

> **HINWEIS:** 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.

HINWEIS: 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 Unternehmensdomänen befinden, als auch in den Partnern. Seine Art ist hier von Bedeutung: Beim Import eines privaten Schlüssels werden die E-Mail-Adressen beachtet, deren Domänen sich in der Liste der Unternehmensdomänen befinden, die anderen E-Mail-Adressen werden ignoriert. Beim Import eines öffentlichen Schlüssels werden für alle E-Mail-Adressen, deren Domäne nicht zu den Unternehmensdomänen gehört, neue Partner erstellt oder ein bestehender ergänzt. Die übrigen E-Mail-Adressen werden ignoriert.

PGP-Schlüssel exportieren

1. Gehen Sie zu **Identitäten > PGP-Schlüssel > PGP-Schlüsselverwaltung**.
2. Markieren Sie den jeweiligen PGP-Schlüssel und klicken Sie **Markierte exportieren**.
3. Bestimmen Sie, ob Sie nur die öffentlichen Schlüssel oder auch vorhandene private oder geheime Schlüssel exportieren möchten.
4. Führen Sie einen der beiden folgenden Schritte durch:
    - **Wenn Sie nur den öffentlichen Schlüssel exportieren|** Geben Sie einen Pfad und einen Dateinamen für die zu exportierenden Dateien an.
    - **Wenn Sie den öffentlichen Schlüssel und verfügbare geheime Schlüssel exportieren|** Geben Sie einen Pfad und einen Dateinamen für die zu exportierenden Dateien an. Wir empfehlen Ihnen, zusätzlich ein Passwortz für alle zu exportierenden Schlüssel anzugeben.

5. Klicken Sie **Fertigstellen**.

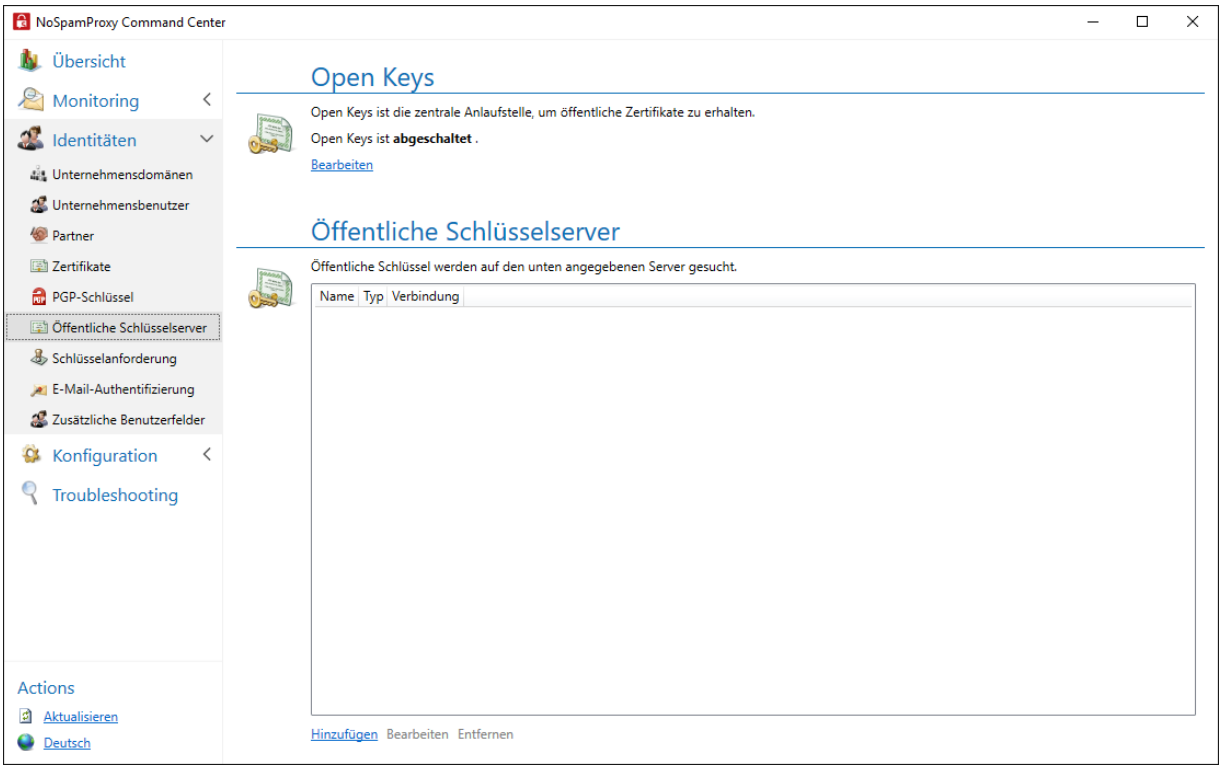
PGP-Schlüssel in Quarantäne

PGP-Schlüssel, 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.

Im Dialog **PGP-Schlüssel-Quarantäne** sehen Sie die PGP-Schlüssel, die derzeit unter Quarantäne gestellt sind.

- Klicken Sie **Markierte genehmigen**, um die markierten Schlüssel zu bestätigen und damit für die weitere Nutzung zu aktivieren.
- Klicken Sie **Markierte ablehnen**, um die markierten Schlüssel abzulehnen und zu löschen.

Öffentliche Schlüsselserver



Open Keys

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

Open Keys wird standardmäßig genutzt, um öffentliche Zertifikate abzufragen. Sollte der Service deaktiviert sein, können Sie ihn manuell aktivieren.

Open Keys aktivieren

1. Gehen Sie zu **Identitäten > Öffentliche Schlüsselserver > Open Keys**.
2. Klicken Sie **Bearbeiten**.

3. Setzen Sie das Häkchen neben **Nutze Open Keys (empfohlen)**.

4. Klicken Sie **Speichern und schließen**.

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.

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Identitäten > Zertifikate > Zertifikatsverwaltung**.
2. Markieren Sie ein oder mehrere Zertifikate.
3. Klicken Sie dann **Markierte in Open Keys veröffentlichen**. Die ausgewählten Zertifikate werden automatisch hochgeladen.
4. Klicken Sie im folgenden Dialog auf **Veröffentlichen**.

Andere öffentliche Schlüsselserver

1. Gehen Sie zu **Identitäten > Öffentliche Schlüsselserver > Öffentliche Schlüsselserver**.
2. Klicken Sie **Hinzufügen**.

3. Wählen Sie den Anbieter für kryptographische Schlüssel aus und konfigurieren Sie diesen entsprechend:

Generisches LDAP

- **Name und Servername|** Der Name ist nur für Sie relevant und wird von der Software nicht weiter verwendet.
- **Port|** Verbindung zum LDAP-Server des Anbieters. Der Standard-Port für LDAP-Abfragen ist 389.
- **Authentifizierungsmethode|** Verlangt der Anbieter eine Authentifizierung, so können Sie die im unteren Abschnitt angeben.
- **Suche|** 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.
- **Filter|** Gibt den Suchfilter an, mit dessen Hilfe Zertifikate gesucht werden. Dies muss ein gültiger LDAP-Suchstring sein.

  > **BEISPIEL:**
  > '(|(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.

- **LDAP-Felder|** Wählen Sie aus, ob Sie X509-Zertifikate, PGP-Schlüssel oder beides von diesem Anbieter abrufen möchten.

> **HINWEIS:** Sie müssen mindestens eine Art von Schlüsseln wählen und festlegen, aus welchem LDAP-Feld der Schlüssel geladen werden soll.

- **Domänen** Konfigurieren Sie, 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.

TeleTrusT European Bridge CA

- **Name**| Geben Sie den Namen an, unter dem Sie diesen Schlüsselanbieter speichern möchten. Alle weiteren Einstellungen werden automatisch von NoSpamProxy vorgenommen.

Secardeo certBox

> **HINWEIS:** 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.

- **Name**| Geben Sie dem Anbieter einen Namen. Dieser ist nur für Sie relevant und wird von der Software nicht weiter verwendet.
- **Anbindung**| Wählen Sie, ob Sie den Secardeo Cloud-Dienst oder eine lokale certBox ansprechen wollen. Für den Cloud-Dienst müssen Sie Ihre Firewall so konfigurieren, dass Sie ausgehende Verbindungen auf Port 389 (LDAP) zulässt.

Weitere LDAP-Verzeichnisse mit Konfigurationseinstellungen

Hier finden Sie einige bekannte Schlüsselserver namhafter Hersteller. Des Weiteren finden Sie in der Liste die entsprechenden Einstellungen für die Einbindung in NoSpamProxy.

> **HINWEIS:** Diese Verzeichnisse werden automatisch über **Open Keys** abgefragt. Open Keys kann ab NoSpamProxy Version 12.1 aktiviert werden.

A-Trust

- Hostname: ldap.a-trust.at:389
- Anmeldung: Anonymous
- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

Arbeitsagentur (Für weitere Infos zu diesem LDAP-Server wenden Sie sich bitte an: IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de)

- Hostname: cert-download.arbeitsagentur.de:389
- Anmeldung: CN=Username,OU=BA,O=Bundesagentur fuer Arbeit,C=de
- LDAP Suche: Im Container OU=BA,O=Bundesagentur fuer Arbeit,C=de auf (mail=%e)
- LDAP Felder: userCertificate;binary

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Hostname: x500.bund.de:389
- Anmeldung: Anonymous
- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

D-TRUST

- Hostname: directory.d-trust.net:389
- Anmeldung: Anonymous
- LDAP Suche: Im Container c=de auf (mail=%e)
- LDAP Felder: userCertificate;binary

Datev

- Hostname: ldap.crl.esecure.datev.de:389
- Anmeldung: Anonymous
- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

HINWEIS: Dieses System wird über Open Keys abgefragt, es werden aber nur Zertifikate von vertrauten Root CAs importiert, da nicht jede CA zum Verschlüsseln geeignete Zertifikate ausstellt.

Deutsches Forschungsnetz (DFN)

- Hostname: ldap.pca.dfn.de:389
- Anmeldung: Anonymous
- LDAP Suche: Im Container mit der Basis-DN: o=DFN-Verein,c=DE nach (mail=%e) suchen
- LDAP Felder: userCertificate;binary

S-Trust

- Hostname: directory.s-trust.de:389
- Anmeldung: Anonymous
- LDAP Suche: Im Container dc=s-trust,dc=de auf (mail=%e)
- LDAP Felder: userCertificate;binary

Siemens PKI

- Hostname: cl.siemens.com:389
- Anmeldung: Anonymous
- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

T-Systems Mailpass

- Hostname: ldap.t-mailpass.de:389
- Anmeldung: Anonymous

- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

DigiCert, Inc. (vormals VerSign Inc.)

- Hostname: ldap://directory.pki.digicert.com:389
- Anmeldung: Anonymous
- LDAP Suche: Unbeschränkte Suche auf (mail=%e)
- LDAP Felder: userCertificate;binary

SwissSign AG

- Hostname: directory.swisssign.net:389
- Anmeldung: Anonymous
- LDAP Suche: Im Container o=SwissSign,c=CH auf (mail=%e)
- LDAP Felder: userCertificate;binary

Ausstehende Anforderungen

Alle ausstehenden Zertifikatsanforderungsanfragen werden unter **Identitäten > Schlüsselanforderung > Schlüsselanforderungen** aufgelistet. Sie können hier fehlgeschlagene Anfragen, vollständige Anfragen oder die markierten Anfragen löschen.

- Einträge für **erfolgreich abgeschlossene Schlüsselanforderungen** werden nach sieben Tagen automatisch aus dieser Liste gelöscht.

- Einträge für **ausstehende Schlüsselanforderungen** werden nach sechs Stunden aus dieser Liste entfernt.
- Einträge für **fehlgeschlagene Schlüsselanforderungen** werden nach sechs Stunden aus dieser Liste entfernt.

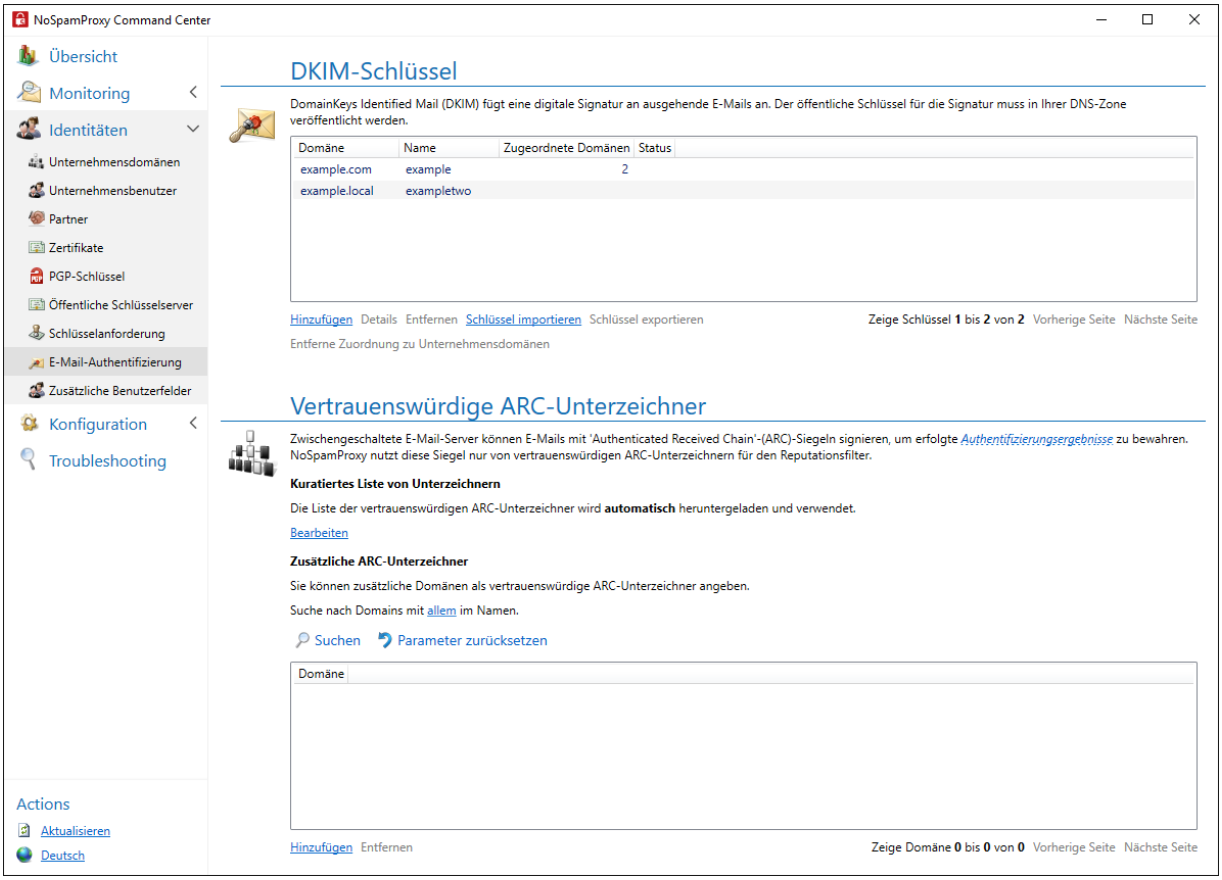
WARNUNG: Wenn Sie Zertifikatsanforderungen löschen, die entweder ausstehen oder sich in einer Warteschlange befinden, werden die angeforderten Zertifikate ungültig und dadurch zerstört. Das Löschen kann nicht rückgängig gemacht werden. Über **Details in die Zwischenablage kopieren** können Sie den Text aller markierten Einträge in die Zwischenablage kopieren. Dies ist bei Problemen mit der Zertifikatsanforderung hilfreich, da Sie dadurch sofort alle Statusmeldungen der betroffenen Anfragen für Supportfälle an Dritte weitergeben können.

HINWEIS: Über **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.

Wann werden neue Zertifikate beantragt?

Neue Zertifikate werden automatisch 14 Tage vor Ablauf bei der jeweiligen Managed PKI beantragt.

E-Mail-Authentifizierung



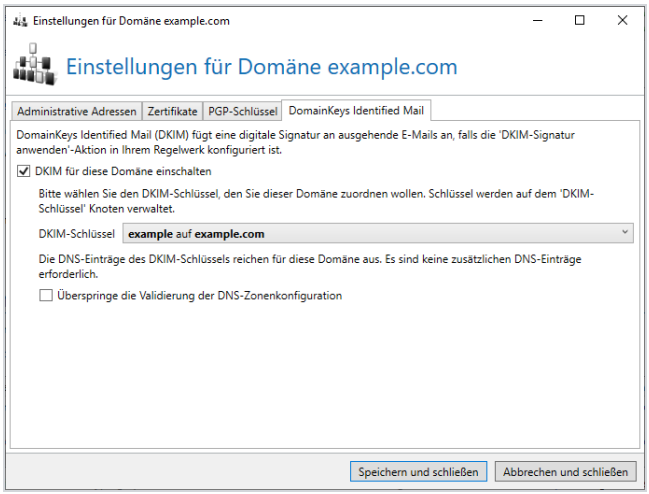
DomainKeys Identified Mail (DKIM)

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 aktivieren

Die für diesen Vorgang notwendigen Schlüssel können Sie unter **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.

1. Gehen Sie zu **Identitäten > Unternehmensdomänen > Unternehmensdomänen**.
2. Doppelklicken Sie die Domäne, die Sie bearbeiten wollen.
3. Wechseln Sie zur Karteikarte **DomainKeys Identified Mail**.
4. Aktivieren Sie **DKIM** für die Domäne.



5. Wählen Sie einen der bereits erstellten Schlüssel aus der Liste der DKIM-Schlüssel aus.

HINWEIS: 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. 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. Wenn alle notwendigen DNS-Einträge veröffentlicht und im Internet bekannt sind, starten Sie die Auswahl des DKIM-Schlüssels bitte erneut.

WARNUNG:
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**. Dies ermöglicht es Ihnen, durch unterschiedlich konfigurierte Regeln für einen Teil Ihrer E-Mails DKIM einzusetzen und für einen anderen Teil DKIM zu unterdrücken.

HINWEIS: Falls für die Intranetrolle ein interner DNS-Server konfiguriert ist, der nicht ins Internet auflöst, müssen die DKIM-Einträge auf diesem DNS-Server ebenfalls erstellt werden.

DKIM-Schlüssel

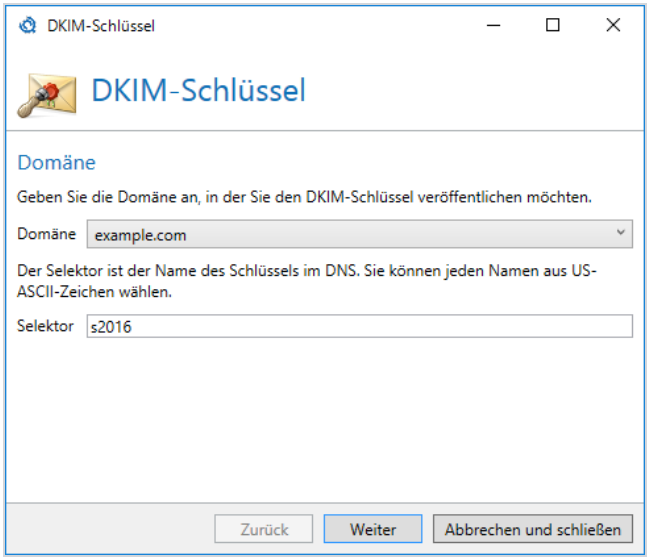
DomainKeys Identified Mail (DKIM) sichert ausgehende E-Mails mit einer elektronischen Signatur. Durch die Auswertung dieser Signatur kann der Empfänger erkennen, ob die E-Mail von der richtigen Domäne versandt wurde (Sicherstellen der Authentizität) und ob sie während des Transports verändert wurde (Sicherstellen 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.

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.

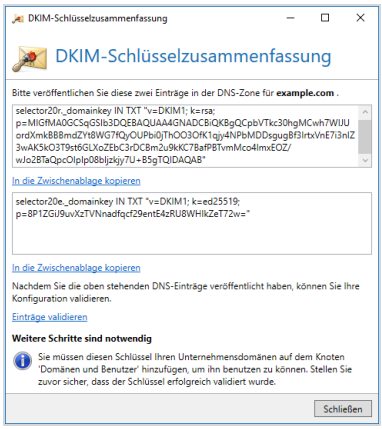
DKIM-Schlüssel hinzufügen

1. Gehen Sie zu **Identitäten > E-Mail-Authentifizierung > DKIM-Schlüssel**.
2. Klicken Sie **Hinzufügen**.



3. Geben Sie die Domäne an, in der Sie den DKIM-Schlüssel veröffentlichen wollen.
4. Geben Sie einen Selektor an.
5. Klicken Sie **Weiter**.

6. Veröffentlichen Sie die beiden gezeigten Einträge in der DNS-Zone der jeweiligen Domäne.



7. Klicken Sie **Fertigstellen**.

> **HINWEIS:** Um den DKIM-Schlüssel nutzen zu können, müssen Sie diesen unter **Unternehmensdomänen** aktivieren. Stellen Sie vorher sicher, dass die Überprüfung des Schlüssels erfolgreich ist.

> **TIPP:** Alternativ können Sie beispielsweise mit OpenSSL einen eigenen RSA-Schlüssel erzeugen und ihn über die entsprechende Schaltfläche importieren.

DKIM für Unternehmensdomänen aktivieren

Die erstellten DKIM-Schlüssel müssen Sie für Ihre Unternehmensdomänen aktivieren. Siehe **E-Mail-Authentifizierung**.

DKIM-Schlüssel importieren

1. Gehen Sie zu **Identitäten > DKIM-Schlüssel > DKIM-Schlüssel**.
2. Klicken Sie **Schlüssel importieren**.
3. Wählen den Schlüssel auf Ihrer Festplatte aus und klicken Sie **Öffnen**.
4. Wählen Sie auf der folgenden Seite die Unternehmensdomäne aus, in der Sie den Schlüssel veröffentlichen wollen.
5. Vergeben Sie einen Namen für den Selektor und klicken Sie **Weiter**.
6. Folgen Sie den Anweisungen auf der nächsten Seite.
7. Klicken Sie **Fertigstellen**.

DKIM-Schlüssel exportieren

> **TIPP:** Wir empfehlen Ihnen, den DKIM-Schlüssel zu exportieren, damit Sie ihn im Falle eines Datenverlustes wiederherstellen können. Über die Schaltfläche **Schlüssel exportieren** können Sie dies tun. Der Schlüssel wird im PKCS#8-Format abgespeichert.

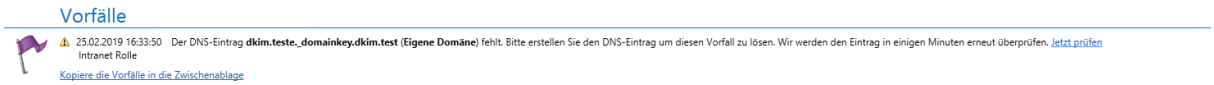
Verwenden von DKIM ab Version 13

Ab Version 13 erzeugt NoSpamProxy zwei DKIM-Schlüssel, einen im RSA-Format und einen EdDSA-Format (Edwards-Curve Digital Signature Algorithm). Die RFC hierzu finden Sie unter **https://tools.ietf.org/html/rfc8463**.

Im Beispiel der “key2018r” ist im RSA-Format wie bisher auch. Der “key2018e” ist mit Version 13 neu und muss zusätzlich im DNS veröffentlicht werden.

Upgrade auf NoSpamProxy Version 13

Nach einem Upgrade auf Version 13 wird der EdDSA-Key automatisch zusätzlich zu den existierenden Schlüsseln erzeugt. Ebenfalls wird folgender Vorfall auf der Startseite der Konsole dargestellt “Der DNS-Eintrag dkim.teste._ domainkey.dkim.test (Unternehmensdomäne) fehlt. Bitte erstellen Sie den DNS-Eintrag um diesen Vorfall zu lösen. Wir werden den Eintrag in einigen Minuten erneut überprüfen.”



E-Mails gelten als gültig, solange eine der aufgetragenen DKIM-Schlüssel erfolgreich validiert werden konnte. Es stellt also kein Problem dar, wenn der neue DKIM-Schüssel im EdDSA-Format benutzt wird aber noch nicht veröffentlich ist. Dies sollte aber trotzdem zeitnah umgesetzt werden.

Falls für die Intranetrolle ein interner DNS-Server konfiguriert ist, der nicht ins Internet auflöst, müssen die DKIM-Einträge auf diesem DNS-Server ebenfalls erstellt werden.

Erstellung eines neuen Schlüsselpaares

Ab Version 13 wird eine größere Verschlüsselungssicherheit (2048bit) für den RSA-Schlüssel verwendet, wodurch der Schlüssel größer als die im DNS erlaubten 255 Zeichen wird. Hierfür muss der erzeugte Schlüssel beim Einbinden in das DNS korrekt umgebrochen werden. Hierfür verwenden Sie das doppelte Anführungszeichen (“) und brechen entsprechend dort um, so dass im ersten Teil weniger als 255 Zeichen enthalten sind.

Erzeugter Schlüssel in NoSpamProxy (ohne Umbruch):

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAzvf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstlIgGY
XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw
P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy
J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH6kQ+SEc
a0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6FpneHXCfAY6m
OI6vykmkVfb/MAr9CZFKrWY+17dPHDhKJDEwsQymCGUu
GwzLwlPcjLVbMSQGXrtdWy8cJbeOa+iO2Gwp4yS2urmT
/k8aK4256GhSQbBH3HOCxRgNL3Yb4G1mo92QIDAQAB"
```

Zu verwendender Schlüssel im DNS (mit Umbruch)

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAzvf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstlIgGY
XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw
P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy
J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH"
"6kQ+SEca0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6Fpne
HXCfAY6mOI6vykmkVfb/MAr9CZFKrWY+17dPHDhKJDEw
```

```
sQymCGUuGwzLwlPcjLVbMSQGXrtdWy8cJbeOa+iO2Gwp

4yS2urmT/k8aK4256GhSQbBH3HOCxRgNL3Yb4G1mo92Q

IDAQAB"
```

Sicherung der DKIM-Schlüssel

Vor jedem Update des NoSpamProxy-Systems auf eine neue Version, oder bei normalen Sicherungen, sollte der aktuelle DKIM-Schlüssel exportiert und gesichert werden. Den Schlüssel kann man unter “Identitäten > DKIM-Schlüssel” exportieren und im Falle einer Wiederherstellung des Systems auch wieder importieren.

HINWEIS: Manche DKIM Validierungstools geben bei DKIM Schlüssel im neuen EdDSA-Format noch einen Fehler aus, da diese nur RSA-Formate erwarten. Funktionierende Tools sind z.B. MXToolBox https://mxtoolbox.com/dkim.aspx

Siehe auch

- **DKIM-Schlüssel**

Vetrauenswürdige ARC-Unterzeichner

Wozu dient Authenticated Received Chain (ARC)?

SPF, DKIM und DMARC sind wichtige Mechanismen im Kampf gegen Spam und Phishing:

- SPF definiert die IP-Adressen und Namen der erlaubten Versender für seine SMTP-Domäne.
- DKIM signiert E-Mails und schützt sie damit vor Veränderung und Fälschung.
- DMARC bestimmt, wie streng der Empfänger die durch SPF und DKIM gemachten Einstellungen umsetzen soll.

Probleme können immer dann auftreten, wenn E-Mails um- oder weitergeleitet werden. Dies kommt beispielsweise häufig bei Mailinglisten oder beim Aufbringen automatischen Signaturen oder E-Mail-Disclaimern vor.

ARC bewahrt die Ergebnisse der durch SPF, DKIM und DMARC vorgenommenen E-Mail-Authentifizierung aller beteiligten Server auf. (Gewollte) Modifizierungen der E-Mail führen so nicht mehr zu Fehlern. Jede Zwischenstation, die eine E-Mail hinsichtlich SPF, DKIM und DMARC verifiziert und den Header der E-Mail entsprechend anpasst, signiert zusätzlich auch die eigenen Ergebnisse mit einem ARC-Eintrag. Wird die E-Mail per Um- oder Weiterleitung an den nächsten Server gesendet, muss dieser laut RFC zusätzlich auch alle ARC-Information der Zwischenstationen verifizieren. So entsteht die sogenannte *Chain of Custody*, die Kontrollkette.

Wann wird ARC angewendet?

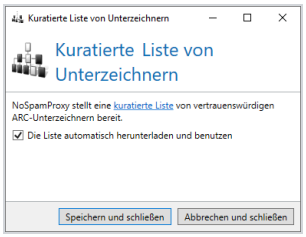
NoSpamProxy wendet ARC standardmäßig als Teil der Reputationsprüfung an.

HINWEIS: Sollte ein oder mehrere Tests vom Typ DMARC - also SPF, DKIM oder DMARC - fehlschlagen, wird dieses Ergebnis durch eine intakte ARC-Kontrollkette überschrieben. In einem solchen Fall werden keine Strafpunkte vergeben, die das **Spam Confidence Level (SCL)** erhöhen würden.

Vertrauenswürdige ARC-Unterzeichner konfigurieren

Eine von NoSpamProxy kuratierte Liste von Unterzeichnern verwenden

1. Gehen Sie zu **Identitäten > E-Mail-Authentifizierung > Vertrauenswürdige ARC-Unterzeichner > Kuratierte Liste von Unterzeichnern**.
2. Klicken Sie **Bearbeiten**.
3. Setzen Sie das Häkchen bei **Die Liste automatisch herunterladen und benutzen**.

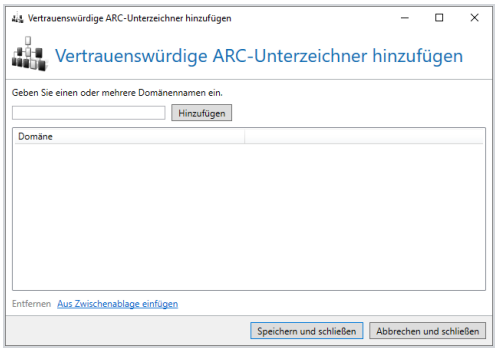


4. Klicken Sie **Speichern und schließen**.

Zusätzliche ARC-Unterzeichner verwenden

1. Gehen Sie zu **Identitäten > E-Mail-Authentifizierung > Vertrauenswürdige ARC-Unterzeichner > Zusätzliche ARC-Unterzeichner**.
2. Klicken Sie **Hinzufügen**.

3. Geben Sie einen oder mehrere Domänennamen ein und klicken Sie **Hinzufügen**.

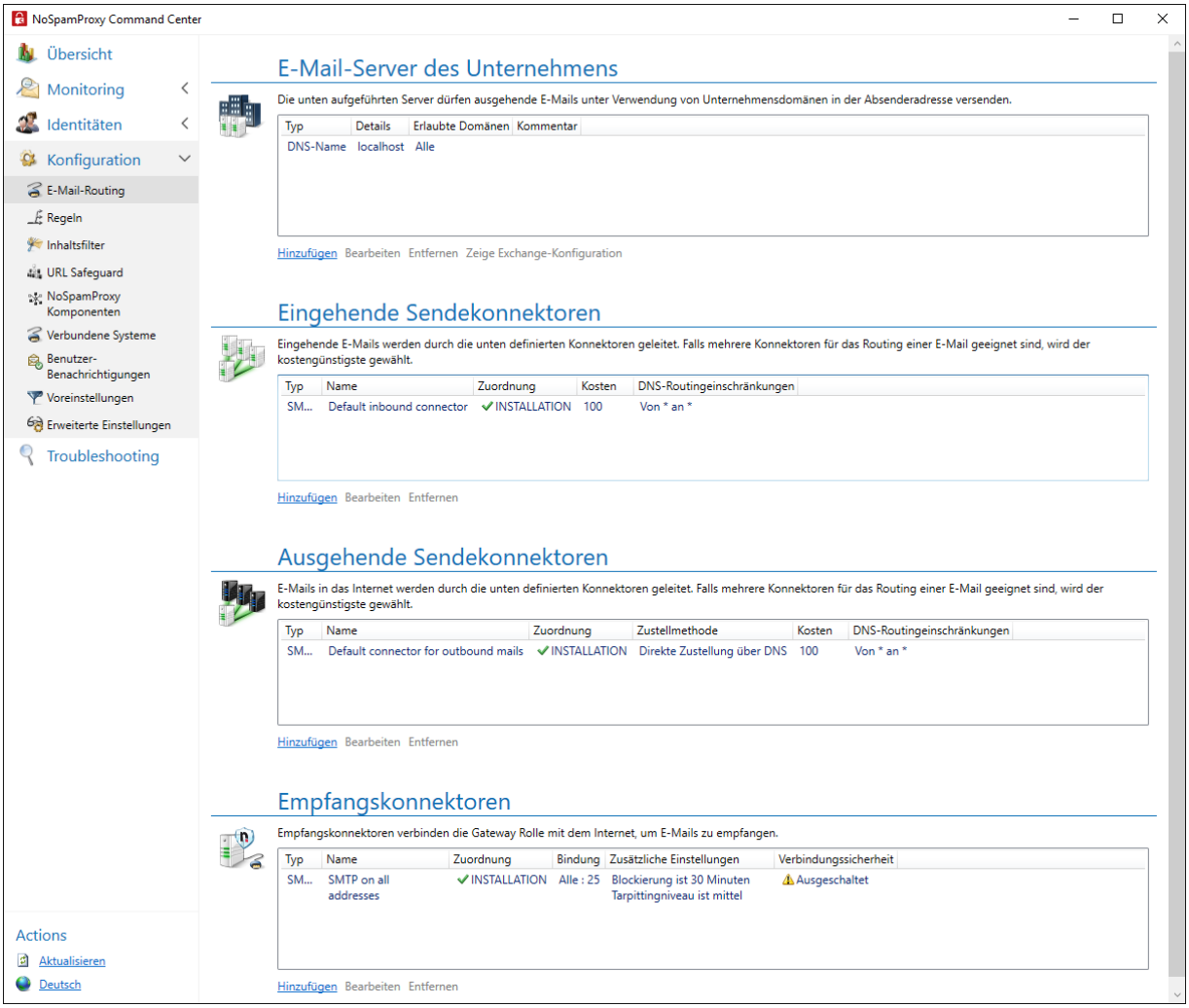


4. Klicken Sie **Speichern und schließen**.

Konfiguration

Dieser Bereich bietet Ihnen Zugriff auf Einstellungen für die Verbindung zur Gatewayrolle, Verbindungsoptionen und Einstellungen des Web Portals, Einstellungen der Datenbank, Benachrichtigungsadressen sowie Optionen zum Schutz sensibler Daten.

E-Mail-Routing einrichten



E-Mail-Server des Unternehmens hinzufügen

Alle E-Mail-Server, die eine Unternehmensdomäne in der Absenderadresse von E-Mails verwenden sollen, müssen zwingend als E-Mail-Server des Unternehmens in NoSpamProxy hinterlegt sein.

Hinzufügen per IP-Adresse, Subnetz oder Hostnamen

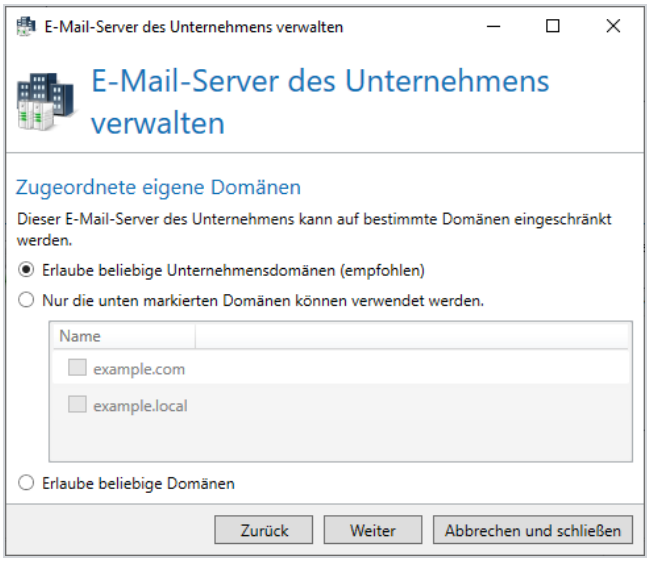
Ein Server gilt hier als E-Mail-Server des Unternehmens, sofern er

- von der angegebenen IP-Adresse sendet,
- von einer Adresse im angegebenen Subnetz sendet oder
- der hier konfigurierte DNS-Hostname auf die Adresse des Servers verweist.

HINWEIS: Ein Subnetz wird in der CIDR-Schreibweise angegeben, z.B. 192.168.100/24.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie den **Mit einer IP-Adresse, einem Subnetz oder einem DNS-Hostnamen** aus und klicken Sie **Weiter**.
4. Geben Sie die Adresse des Servers ein, indem Sie einen voll qualifizierten DNS-Hostnamen, eine IP-Adresse oder Subnetz angeben und klicken Sie **Weiter**.

5. Bestimmen Sie, welche Unternehmensdomänen dem Server zugeordnet sind und klicken Sie **Weiter**.



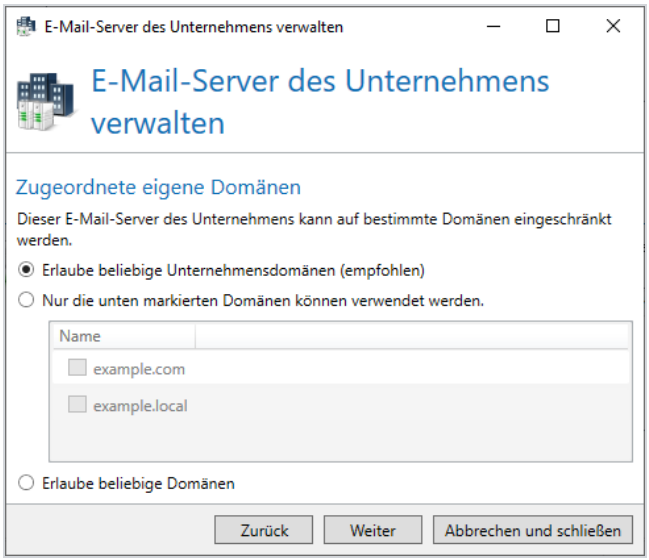
6. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie **Fertigstellen**.

Hinzufügen per TLS-Client-Zertifikat

Ein Server gilt hier als E-Mail-Server des Unternehmens, 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, das das konfigurierte Zertifikat in seiner Zertifikatskette enthält. Wird ein End-Zertifikat eingetragen, so muss sich der Server mit exakt diesem Zertifikat melden.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie aus **Mit einem TLS-Client-Zertifikat** aus und klicken Sie **Weiter**.

4. Klicken Sie **Zertifikat auswählen** und markieren Sie das Zertifikat, das Sie für die Authentifizierung nutzen möchten.
5. Klicken Sie **Auswählen und schließen** und im nächsten Dialogfenster **Weiter**.
6. Bestimmen Sie, welche Unternehmensdomänen dem Server zugeordnet sind und klicken Sie **Weiter**.



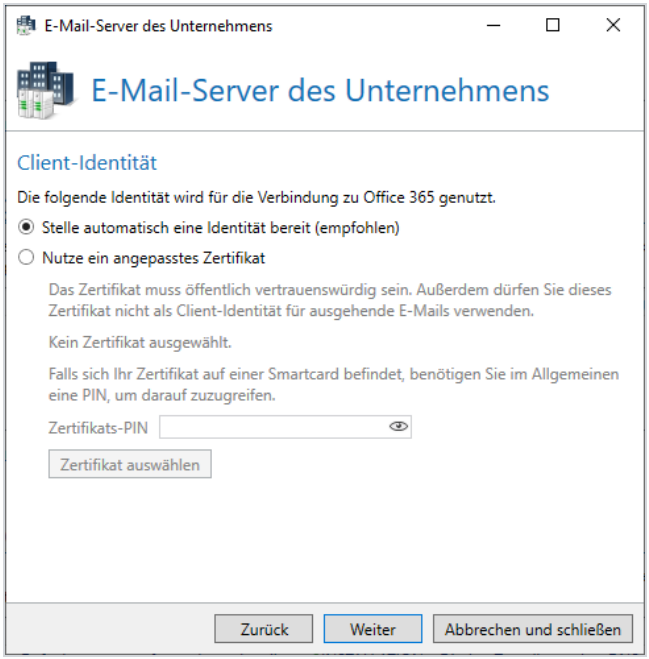
7. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie **Fertigstellen**.

Hinzufügen als Office-365-Mandant

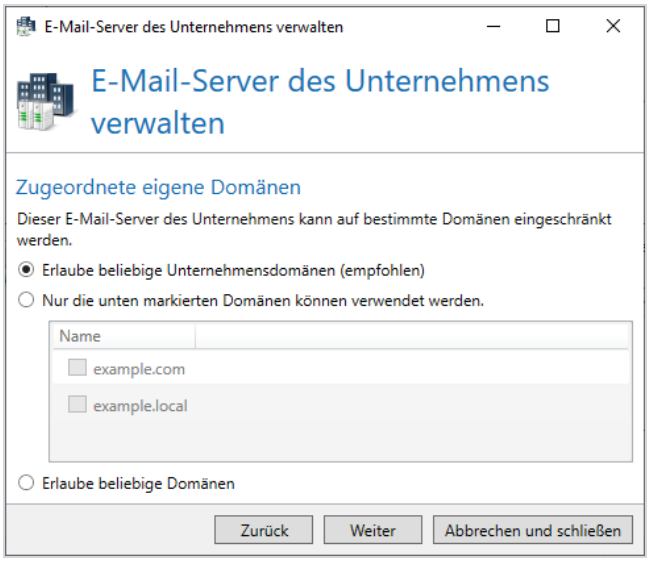
Ein Server gilt hier als E-Mail-Server des Unternehmens, wenn es sich um einen offiziellen Office-365-Server handelt.

> **HINWEIS:** Wenn Sie Office 365 als E-Mail-Server des Unternehmens konfigurieren, wird ein Sendekonnektor für Office 365 konfiguriert.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie den **Als Office-365-Mandant** aus und klicken Sie **Weiter**.
4. Geben Sie Ihren Mandanten-Namen ein und klicken Sie **Weiter**.
5. Konfigurieren Sie die genutzte Client-Identität und klicken Sie **Weiter**.



6. Bestimmen Sie, welche Unternehmensdomänen dem Server zugeordnet sind und klicken Sie **Weiter**



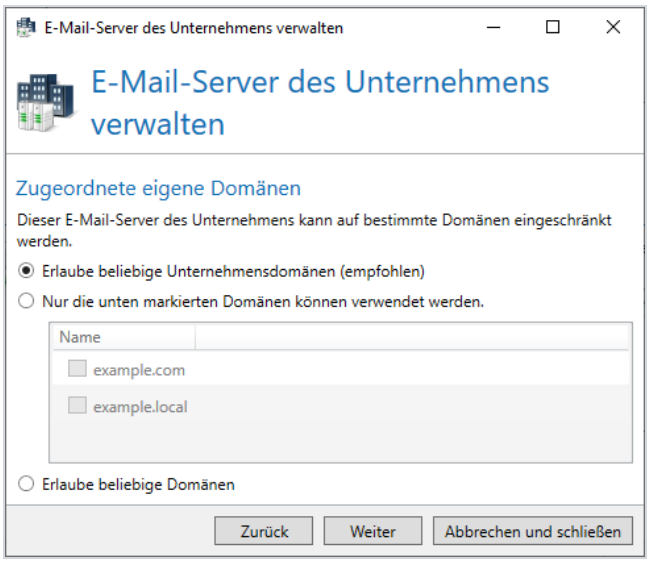
7. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie **Fertigstellen**.

> **HINWEIS:** Durch das Hinzufügen Ihres Office-365-Mandanten wird das erforderliche E-Mail-Routing in NoSpamProxy Server bereits angelegt. Sie müssen nun den Nachrichtenfluss in Microsoft Exchange Online einrichten, indem Sie das bereitgestellte PowerShell-Skript ausführen oder die Einrichtung manuell vornehmen. Markieren Sie den Eintrag für den Office-365-Server und klicken Sie **Zeige Exchange-Konfiguration**, um das PowerShell-Skript sowie weitere Informationen anzuzeigen.

Hinzufügen über einen authentisierten Host

Ein Server gilt hier als E-Mail-Server des Unternehmens, wenn er für die Authentisierung eine Kombination aus Benutzernamen und Passwort verwendet.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie den **Ein durch ein Passwort authentifizierter Host** aus und klicken Sie **Weiter**.
4. Geben Sie einen Benutzernamen an, klicken Sie **In die Zwischenablage kopieren** und klicken Sie **Weiter**.
5. Bestimmen Sie, welche Unternehmensdomänen dem Server zugeordnet sind und klicken Sie **Weiter**.



6. (Optional) Geben Sie einen Kommentar ein.
7. Klicken Sie **Fertigstellen**.

Hinzufügen über eine bestimmte Absenderadresse

Jeder Server, der eine 'MAIL FROM'-Adresse nutzt, gilt hier als E-Mail-Server des Unternehmens.

WARNUNG: Die 'MAIL FROM'-Adresse kann sehr einfach gefälscht werden. Nutzen Sie diese Option nur, falls Sie keine andere Möglichkeit haben, den Server zu identifizieren.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **Mit einer bestimmten Absenderadresse** aus und klicken Sie **Weiter**.
4. Klicken Sie **Hinzufügen**.
5. Geben Sie das Adressmuster an, das Sie für die Absenderadresse verwenden wollen, klicken Sie **Speichern und schließen** und dann **Weiter**.
6. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie **Fertigstellen**.

Eingehende Sendekonnektoren anlegen

Eingehende E-Mails werden über eingehende Sendekonnektoren geleitet. Falls mehrere Konnektoren für das Routing einer E-Mail geeignet sind, wird der kostengünstigste gewählt.

HINWEIS: Die Option zur direkten Zustellung zum lokalen E-Mail-Server ist veraltet und seit Version 13 nicht mehr in NoSpamProxy verfügbar. Es wird immer die Zustellung über Warteschlangen angewendet.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Eingehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
4. Klicken Sie **Fertigstellen**.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

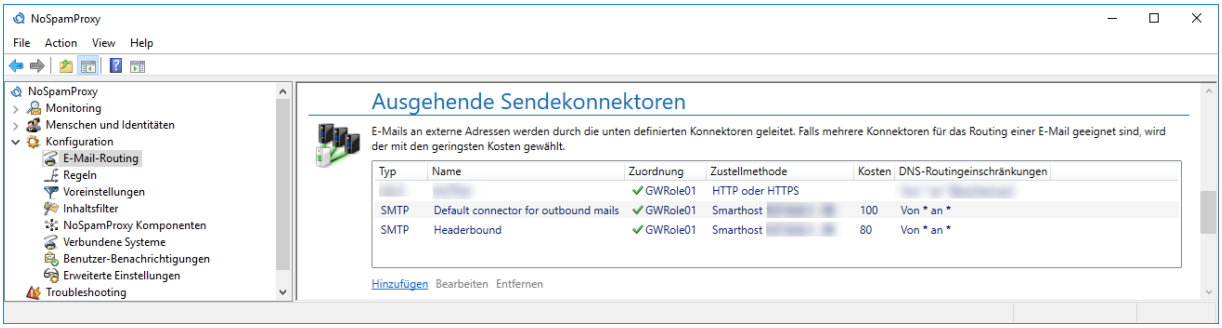
Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Ausgehende Sendekonnektoren anlegen

Ausgehende Sendekonnektoren werden für den Versand von E-Mails an externe Server eingesetzt.



Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Einen Konnektor des Typs SMTP anlegen

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Ausgehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie als Typ **SMTP** aus.

4. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
5. Klicken Sie **Fertigstellen**.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Einen Konnektor des Typs De-Mail über Telekom anlegen

> **HINWEIS:** Für die Anbindung an Telekom De-Mail müssen Sie unter **Verbundene Systeme** zuerst einen **De-Mail-Anbieter** für eine Telekom-De-Mail-Verbindung einrichten.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Ausgehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie als Typ **De-Mail über Telekom** aus.
4. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
5. Klicken Sie **Fertigstellen**.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Einen Konnektor des Typs De-Mail über Mentana-Claimsoft GmbH anlegen

HINWEIS: Für die Anbindung an Mentana-Claimsoft De-Mail müssen Sie unter **Verbundene Systeme** einen **De-Mail-Anbieter** für eine Verbindung zu Mentana-Claimsoft einrichten.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Ausgehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie als Typ **De-Mail über Mentana-Claimsoft GmbH** aus.
4. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
5. Klicken Sie **Fertigstellen**.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Einen Konnektor des Typs Deutschland-Online - Infrastruktur (DOI) anlegen

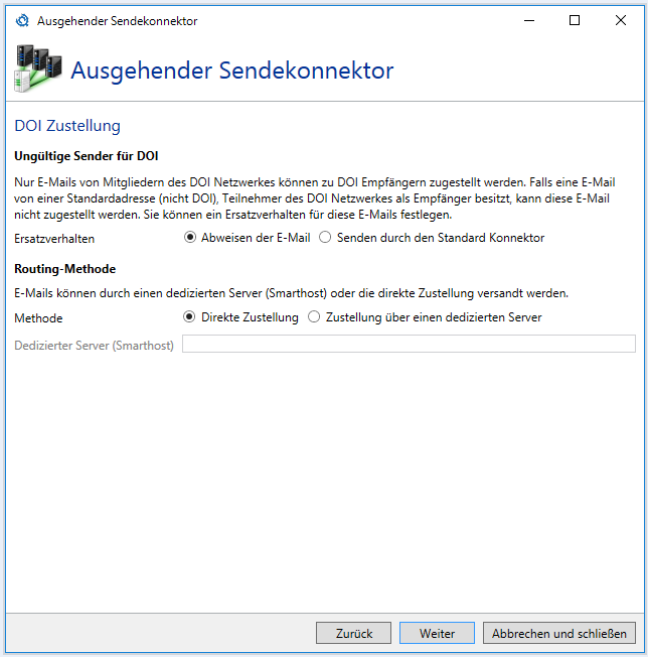
Das Deutschland-Online - Infrastruktur (DOI) Projekt wird unter anderem von Kommunen zur sicheren Übertragung von Nachrichten verwendet.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Ausgehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.

3. Wählen Sie als Typ **Deutschland Online - Infrastruktur (DOI)** aus.
4. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
5. Tragen Sie die FTP- oder Web-Adresse ein, von der Sie die Mailer-Tabelle beziehen und klicken Sie **Weiter**.

6. Konfigurieren Sie das Verhalten für ungültige Absender.

> **HINWEIS:** 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 wählen, ob diese E-Mails an den Absender zurückgehen oder ob sie über einen anderen Konnektor mit höheren **Mehrfach verwendete Einstellungen bei Konnektoren** 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.



7. Klicken Sie **Fertigstellen**.

HINWEIS: 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.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

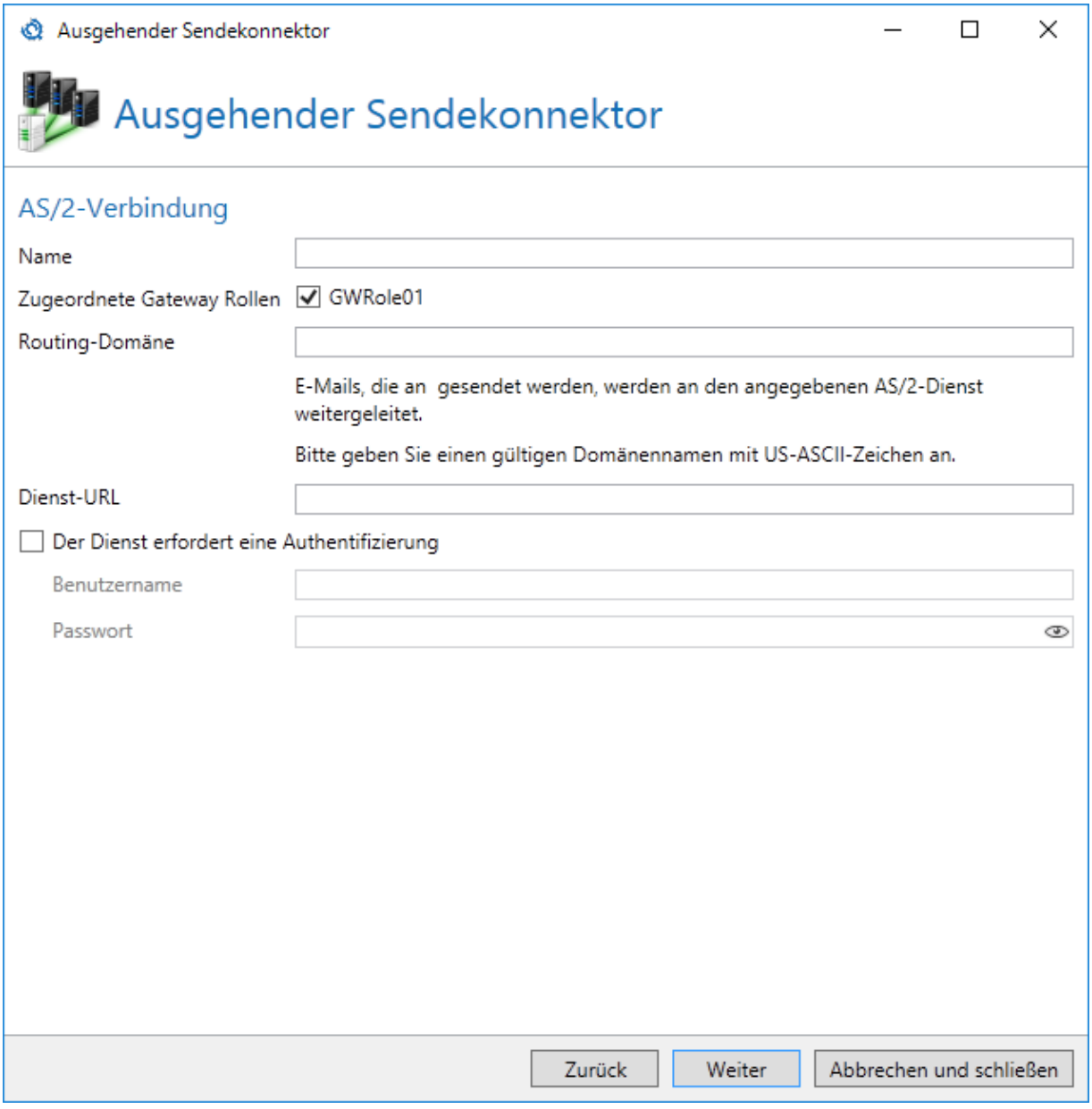
- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Einen Konnektor vom Typ AS2 Business to Business anlegen

Einen Konnektor vom **Typ AS2 Business to Business** anlegen

Der AS2-Konnektor erlaubt es Ihnen, EDI-Dateien an ein AS2-konformes System weiterzuleiten.



1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Ausgehende Sendekonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie als Typ **AS2 Business-to-Business** aus.
4. Folgen Sie den Anweisungen im Dialogfenster.
   Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.

   > **HINWEIS:** 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.

5. Klicken Sie **Weiter**.
6. Geben Sie die AS2-Parameter ein, die Sie von Ihrem Handelspartner erhalten haben.
7. Klicken Sie **Fertigstellen**.

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

HINWEIS: Der Konnektor wird alle E-Mails verarbeiten, die genau einen EDI-Anhang haben. Nach dem Versand der Datei wird die Zustellquittung des AS2-Dienstes an den Absender der ursprünglichen E-Mail weitergeleitet.

HINWEIS: Die Dienst-URL sowie, falls notwendig, Authentifizierungsdaten erhalten Sie von Ihrem Handelspartner.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Empfangskonnektoren anlegen

Sie können mehrere Empfangskonnektoren konfigurieren, 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.

Einen Empfangskonnektor des Typs SMTP anlegen

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 von E-Mails angewendet werden soll.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Empfangskonnektoren** und klicken Sie **Hinzufügen**.
2. Wählen Sie als Typ **SMTP** aus.
3. Legen Sie die Gatewayrollen des Empfangskonnektors, die IP-Adresse und den Port des Konnektors fest. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.
4. Geben Sie bei **Bindung auf IP-Adresse** an, unter welcher Adresse die Verbindungen angenommen werden sollen.

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

5. Geben Sie bei **Port** an, über welchen Port NoSpamProxy E-Mails empfangen soll und klicken Sie **Weiter**.
6. Nehmen Sie die Einstellungen für ungültige Anfragen vor. Beachten Sie dabei die Hinweise unter **Ungültige Anfragen bei SMTP-Empfangskonnektoren**.
7. Nehmen Sie die Einstellungen für die Verbindungssicherheit vor. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei**

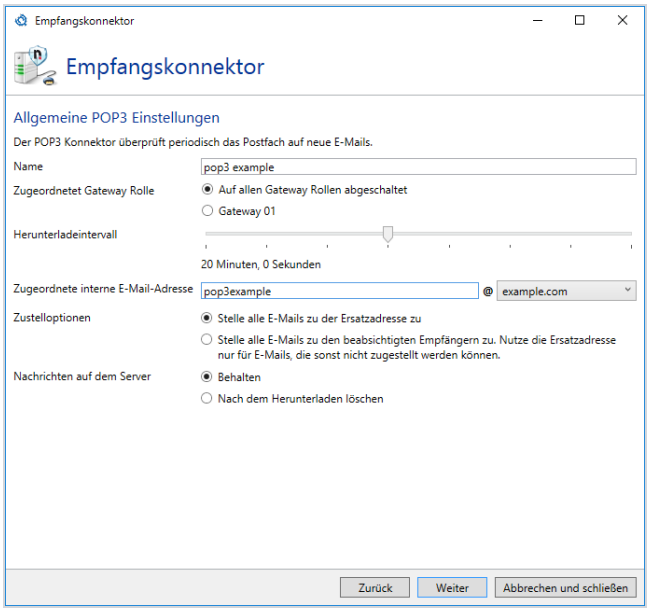
Konnektoren.

8. Klicken Sie **Fertigstellen**.

Einen Empfangskonnektor des Typs POP3 konfigurieren

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 an die konfigurierte interne Adresse zugestellt.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Empfangskonnektoren** und klicken Sie **Hinzufügen**.
2. Wählen Sie als Typ **POP3** aus.
3. Legen Sie einen Namen sowie die Gatewayrollen des Empfangskonnektors fest. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**.

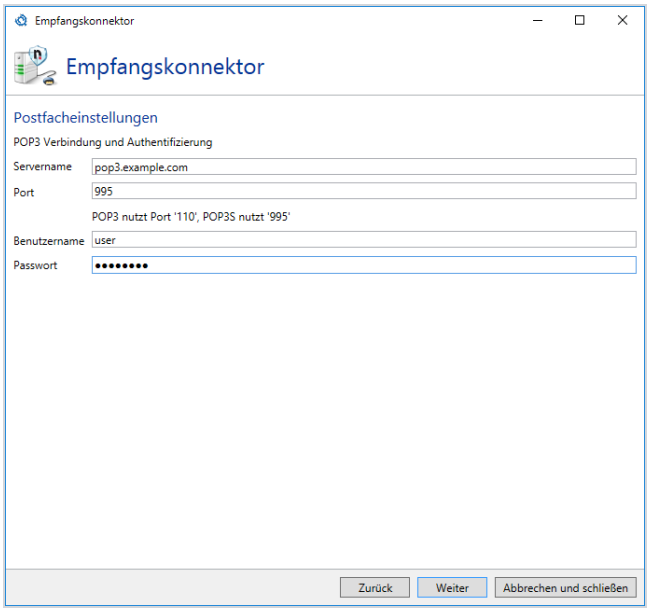


4. Bestimmen Sie unter **Herunterladeintervall**, in welchen Abständen der Konnektor neue E-Mails von der Gegenstelle herunterladen soll.

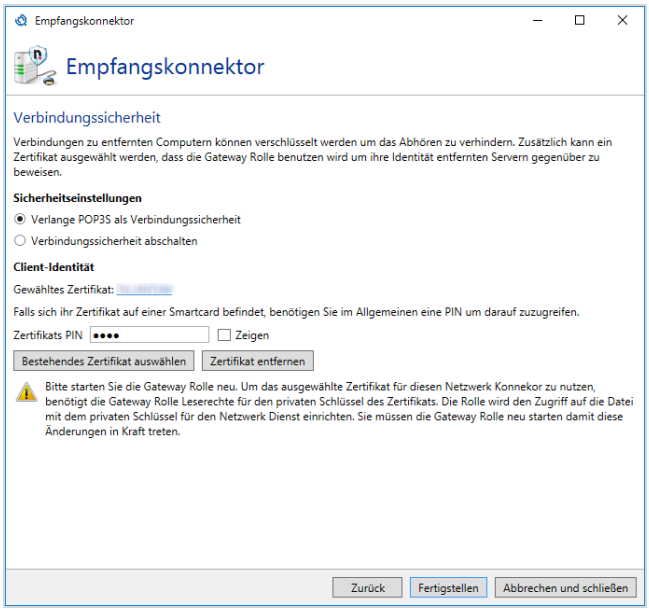
5. Bestimmen Sie unter Zustelloptionen das Zustellverhalten.
    - **Stelle alle E-Mails an die Ersatzadresse zu|** Sämtliche Empfängerdaten in den abgeholten E-Mails werden ignoriert und die E-Mails werden an die angegebene Adresse gesendet.
    - **Stelle alle E-Mails an die beabsichtigten Empfänger zu. Nutze die Ersatzadresse nur für E-Mails, die sonst nicht zugestellt werden können|** Die Empfängerdaten werden 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.
6. Bestimmen Sie, ob die E-Mails nach dem Herunterladen vom Server entfernt werden.

> **HINWEIS:** Falls Sie die E-Mails auf dem Server lassen, werden diese trotzdem nur einmalig heruntergeladen.

7. Legen Sie unter Postfacheinstellungen den Namen, den Netzwerk-Port des Servers sowie die Benutzerinformationen für den Zugriff auf den Server fest.



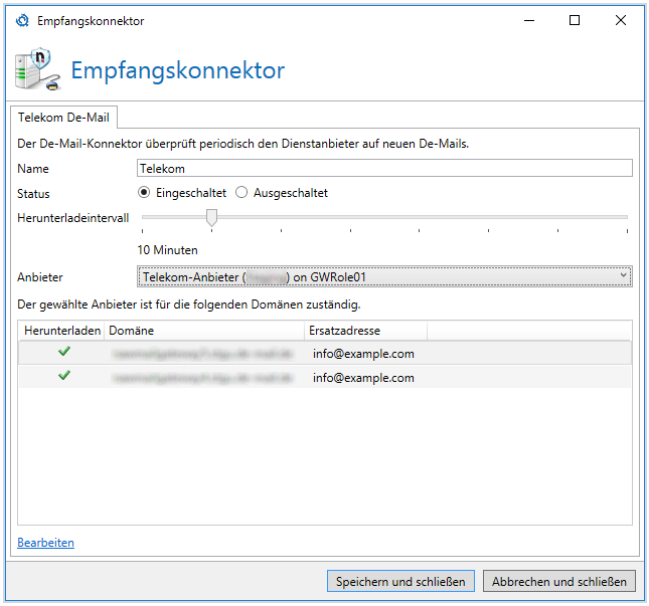
8. Nehmen Sie die Einstellungen für die Verbindungssicherheit fest. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**



9. Klicken Sie **Fertigstellen**.

Einen Empfangskonnektor des Typs De-Mail über Telekom anlegen

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Empfangskonnektoren** und klicken Sie **Hinzufügen**.



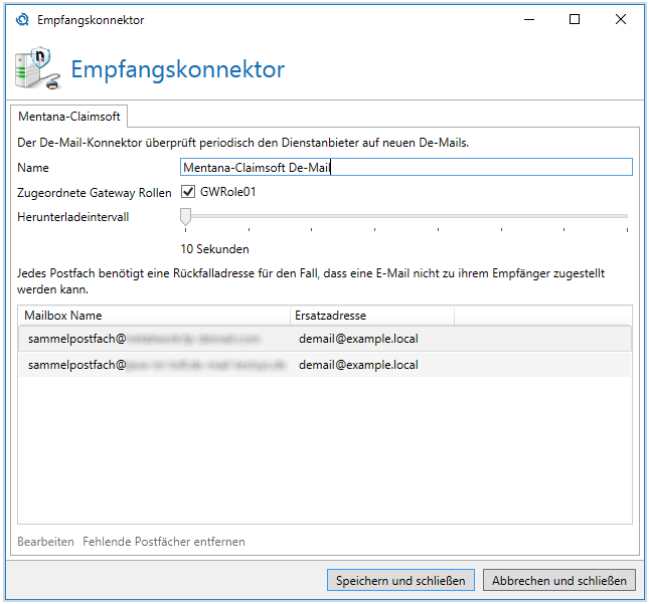
2. Wählen Sie als Typ **De-Mail über Telekom** aus.
3. Legen Sie einen Namen fest und bestimmen Sie, ob der Konnektor eingeschaltet oder abgeschaltet sein soll. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**. Die Zuordnung zu einer Gatewayrolle wird durch den konfigurierten De-Mail-Anbieter festgelegt. Der Konnektor läuft immer auf der Gatewayrolle, auf der das im De-Mail-Anbieter konfigurierte Zertifikat liegt.
4. Bestimmen Sie unter **Herunterladeintervall**, wie oft NoSpamProxy Encryption das De-Mail-Postfach auf neue Nachrichten überprüfen soll.

5. Geben Sie in der Liste der De-Mail-Domänen für jeden Eintrag an, ob De-Mails dieser Domäne heruntergeladen werden sollen.
6. Legen Sie eine Ersatzadresse fest, die benutzt werden kann, falls der ursprüngliche Empfänger der De-Mail in Ihrem Unternehmen nicht mehr verfügbar ist.
7. Klicken Sie **Speichern und schließen**.

Einen Empfangskonnektor des Typs De-Mail über Mentana-Claimsoft GmbH anlegen

> **HINWEIS:** Für die Anbindung an Mentana-Claimsoft De-Mail müssen Sie unter **Verbundene Systeme** zuerst einen De-Mail-Anbieter für eine Verbindung zu Mentana-Claimsoft einrichten.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Empfangskonnektoren** und klicken Sie **Hinzufügen**.
2. Wählen Sie als Typ **De-Mail über Mentana Claimsoft GmbH** aus.



3. Legen Sie einen Namen sowie die Gatewayrollen fest, auf denen der Konnektor arbeiten soll. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**
4. Bestimmen Sie unter **Herunterladeintervall**, in welchen Abständen der Konnektor neue De-Mails von der Gegenstelle herunterladen soll.
5. Geben Sie in der Liste der Postfächer für jedes Postfach eine Ersatzadresse an, die benutzt werden kann, falls der ursprüngliche Empfänger der De-Mail in Ihrem Unternehmen nicht mehr verfügbar ist.

   > **HINWEIS:** Mindestens eine De-Mail-Domäne muss in der Liste zum Herunterladen markiert und mit einer Ersatzadresse konfiguriert sein.

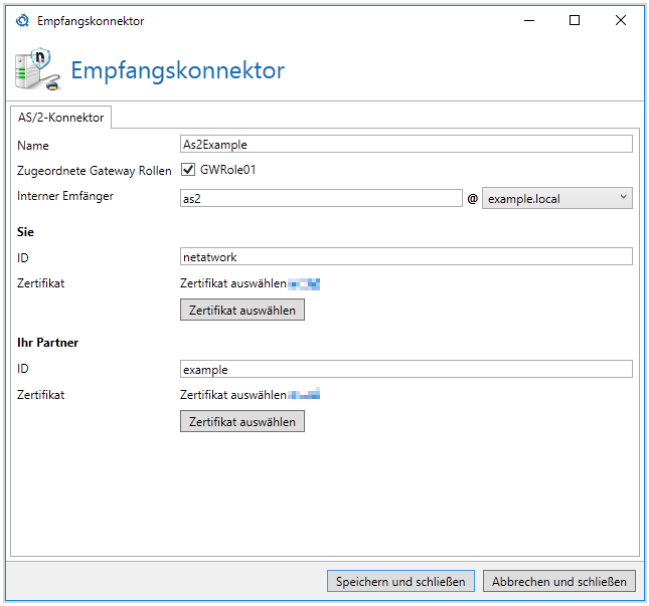
6. Klicken Sie **Speichern und schließen**.

Einen Empfangskonnektor des Typs AS2 Business-to-Business anlegen

Der AS2-Konnektor erlaubt es Ihnen, EDI-Dateien von einem Handelspartner zu empfangen. Die empfangenden Daten werden dann an einen E-Mail-Empfänger weitergeleitet.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Empfangskonnektoren** und klicken Sie **Hinzufügen**.

2. Wählen Sie als Typ **AS2 Business-to-Business** aus.



3. Legen Sie einen Namen sowie die zugeordneten Gatewayrollen fest. Beachten Sie dabei die Hinweise unter **Mehrfach verwendete Einstellungen bei Konnektoren**
4. Geben Sie unter **Interner Empfänger** an, an wen empfangene Daten weitergeleitet werden.
5. Geben Sie sowohl Ihr Zertifikat und Ihre ID als auch das Zertifikat und die ID Ihres Handelspartners an.

> **HINWEIS:** Der Konnektor setzt sowohl eine Signatur als auch eine Verschlüsselung voraus.

HINWEIS: 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 über Ihre Firewall im Internet veröffentlichen.

WARNUNG: 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.

Informationen zum Minimieren von sogenannten Denial-of-Service-Attacken und anderen Schwachstellen finden Sie im Anhang unter **Ungültige Anfragen bei SMTP-Empfangskonnektoren**.

Mehrfach verwendete Einstellungen bei Konnektoren

Einige der folgenden Einstellungen werden in mehreren Konnektoren verwendet:

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.

Zugeordnete Gatewayrollen

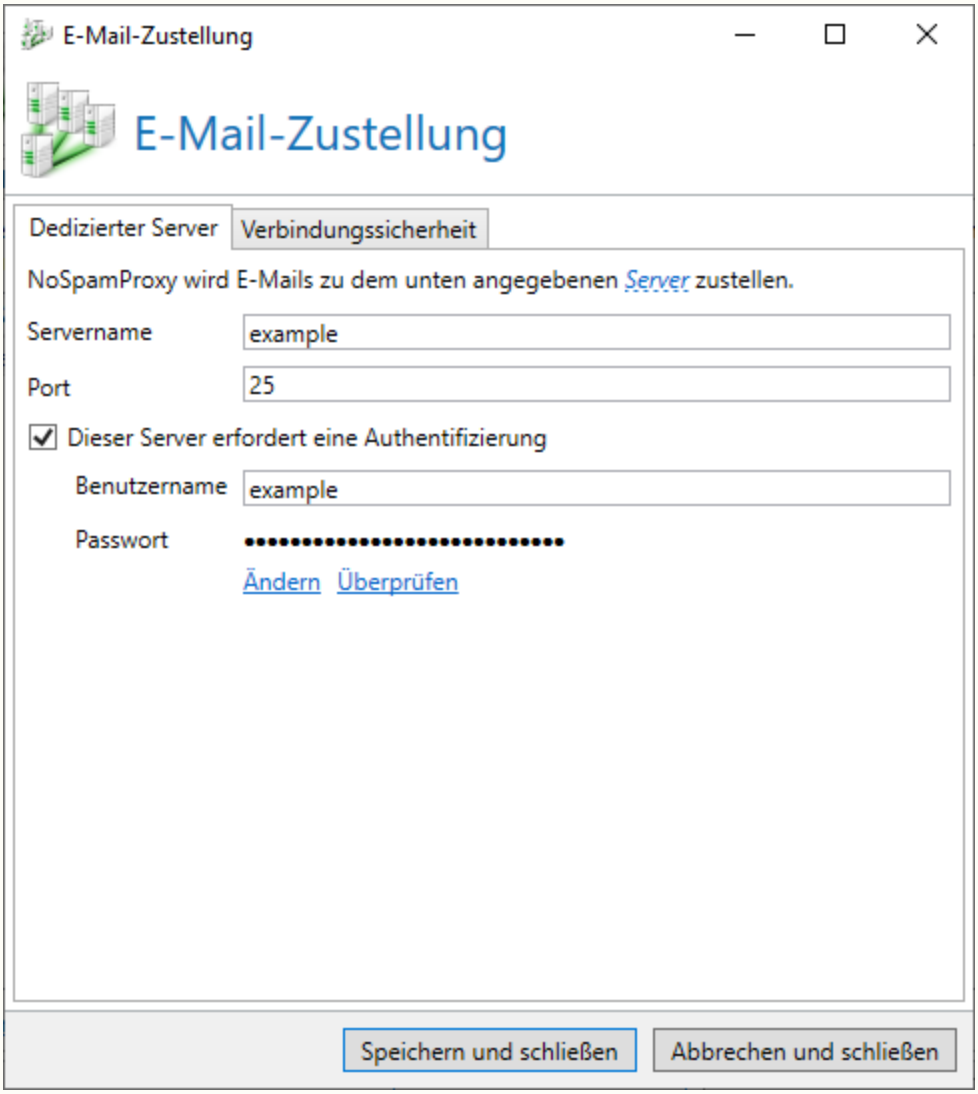
Je nach Typ des Konnektors kann er entweder auf mehreren Gatewayrollen parallel oder nur auf einer einzelnen Rolle verwendet werden. Wählen Sie hier die Gatewayrollen aus, auf denen Sie den Konnektor betreiben möchten.

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.

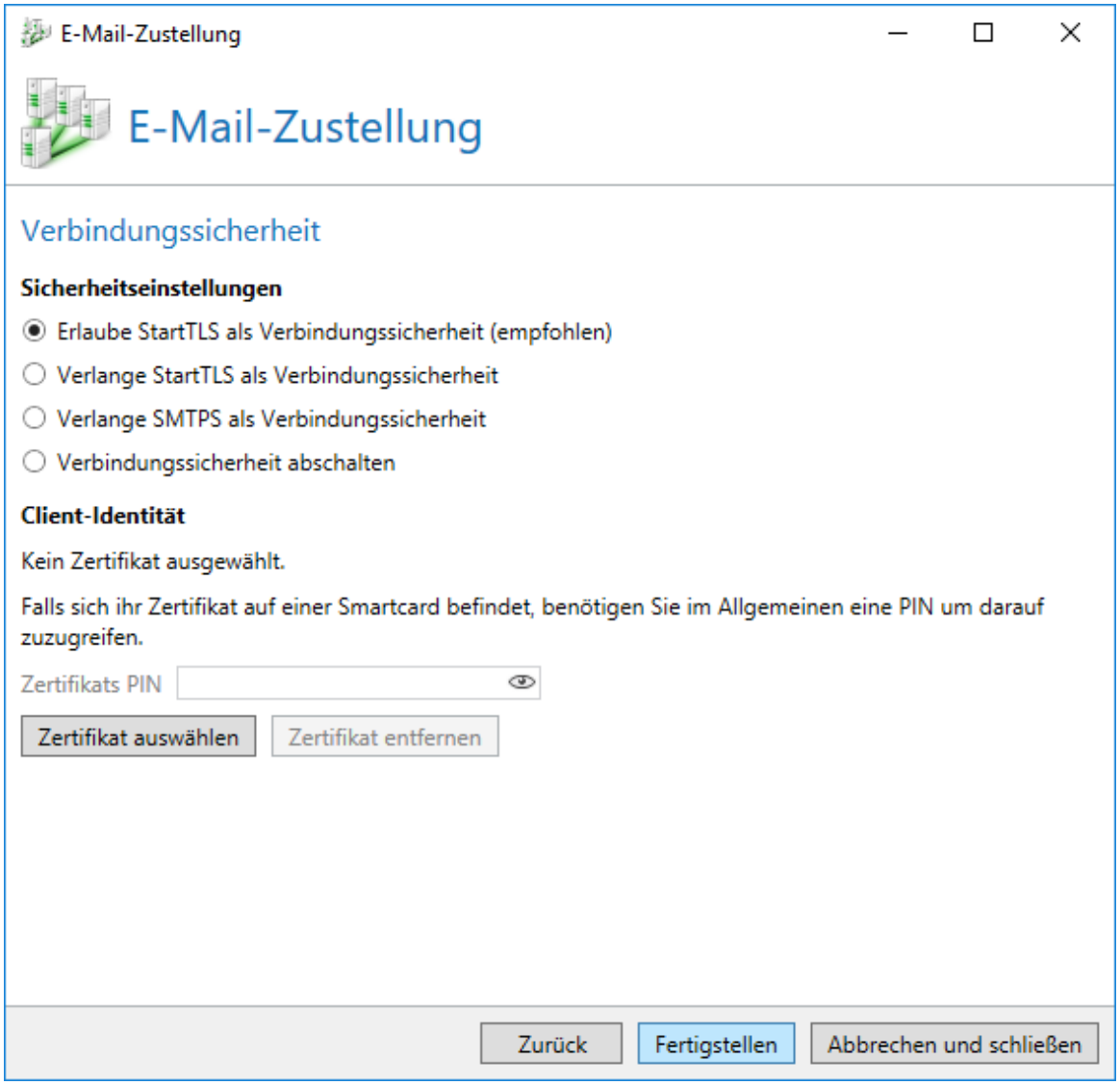
- Geben Sie auf der Seite **Dedizierter Server** den Servernamen (empfohlen) oder die IP-Adresse und den Port des dedizierten Servers ein.
- Falls der Server eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Passwort ein.

TIPP: Um nach Beendigung der Konfiguration zu überpüfen, ob das Ihnen vorliegende Passwort mit dem konfigurierten Passwort übereinstimmt, klicken Sie **Überprüfen**.



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 unter **Verbindungssicherheit** beschrieben, konfigurieren. SMTP-Sendekonnektoren für E-Mails an externe Adressen nutzen die zertifikatsbasierte Identität als **Client-Identität**.


E-Mail-Zustellung
E-Mail-Zustellung
Verbindungssicherheit
Sicherheitseinstellungen
Erlaube StartTLS als Verbindungssicherheit (empfohlen)
Verlange StartTLS als Verbindungssicherheit
Verlange SMTPS als Verbindungssicherheit
Verbindungssicherheit abschalten
Client-Identität
Kein Zertifikat ausgewählt.
Falls sich ihr Zertifikat auf einer Smartcard befindet, benötigen Sie im Allgemeinen eine PIN um darauf zuzugreifen.
Zertifikats PIN
Zertifikat auswählen
Zertifikat entfernen
Zurück
Fertigstellen
Abbrechen und schließen

> **HINWEIS:** 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.

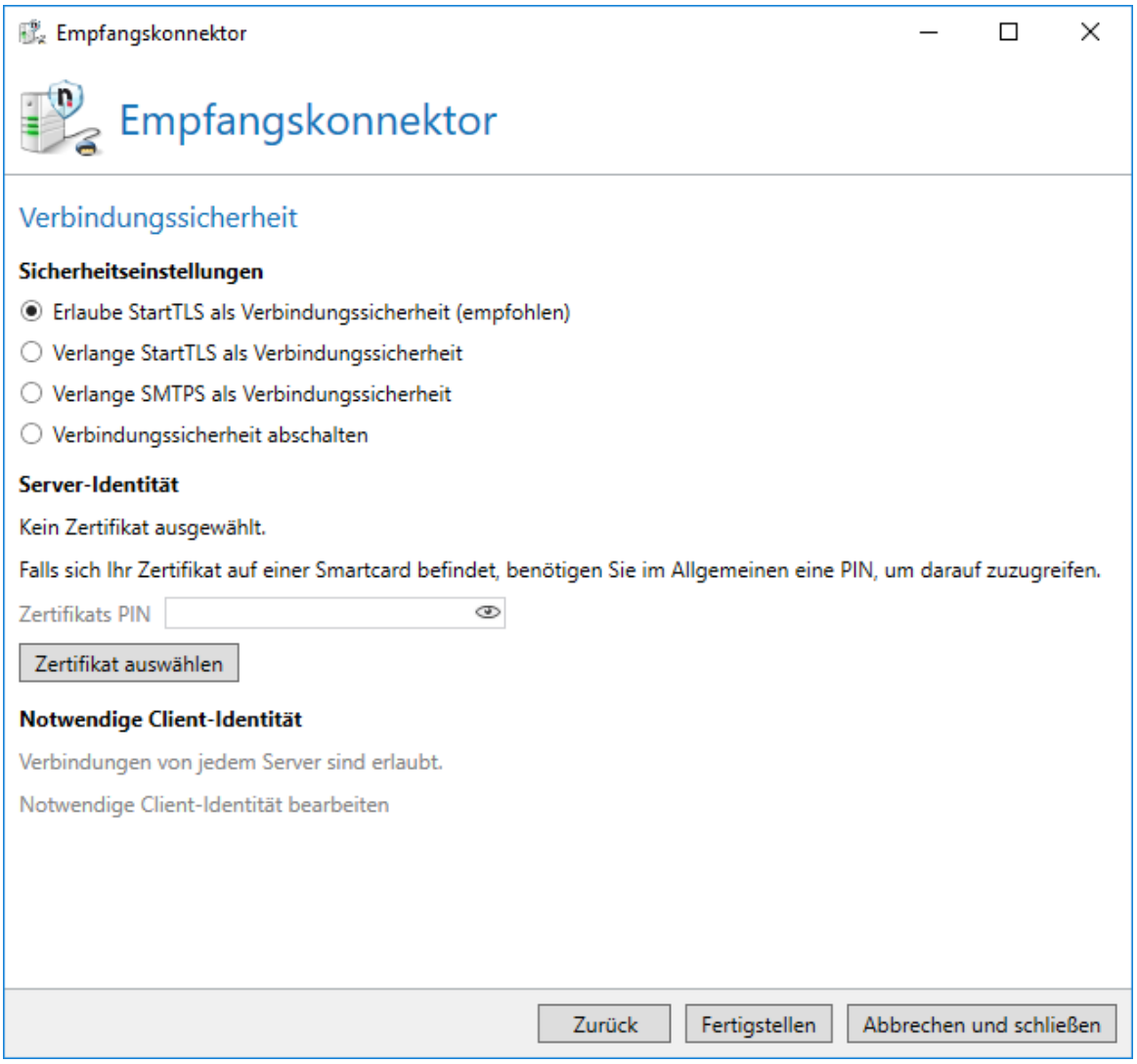
Direkte Zustellung (DNS)

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 NoSpamProxy zu anderen Servern authentifizieren kann.

Verbindungssicherheit

> **HINWEIS:** Informationen zum Austauschen der TLS-Zertifikate für Konnektoren finden Sie unter **Austauschen der TLS-Zertifikate für Konnektoren**.

Die Verbindungssicherheit 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. Es handelt sich hierbei um die Verschlüsselung auf dem Transportweg. Eine Ende-zu- Ende-Verschlüsselung ist nicht gemeint.



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.

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

HINWEIS: 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.

WARNUNG: Beim Hinzufügen eines Zertifikats für die Transportverschlüsselung durch StartTLS benötigt die Gatewayrolle Leserechte auf den privaten Schlüssel. Diese Rechte für die Rolle werden automatisch erteilt. Sie müssen allerdings einmal die Gatewayrolle stoppen und wieder starten, damit diese Änderung wirksam wird und die Gatewayrolle 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.

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

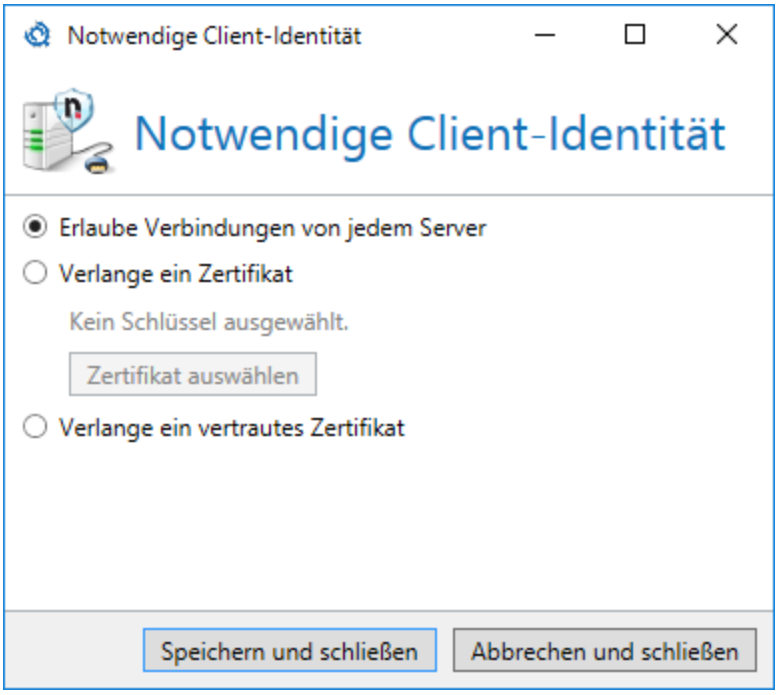
Wenn Sie StartTLS oder SMTPS als Verbindungssicherheit verlangen

Wird für Verbindungen StartTLS oder SMTPS 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.

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.



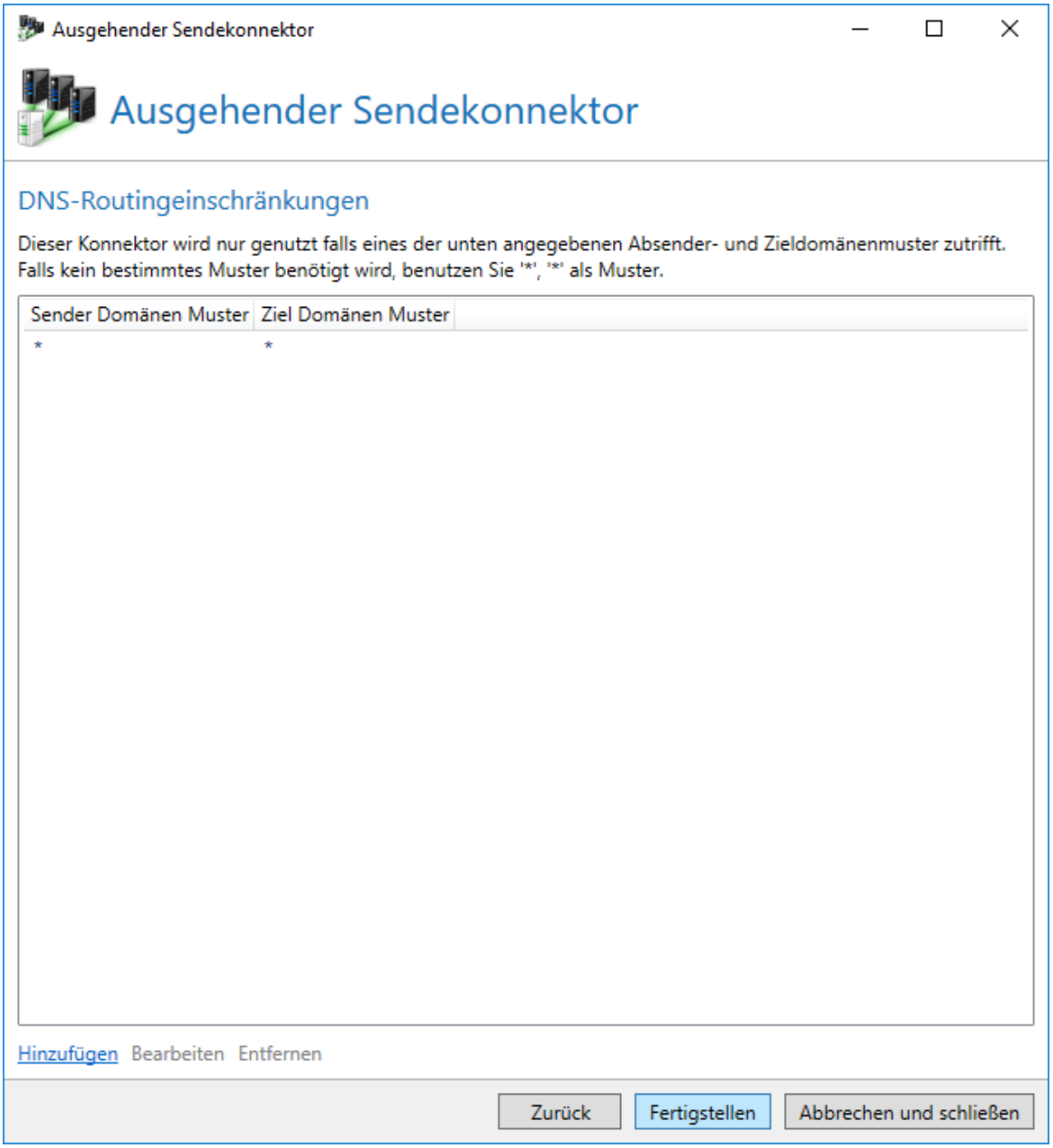
Kosten

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.

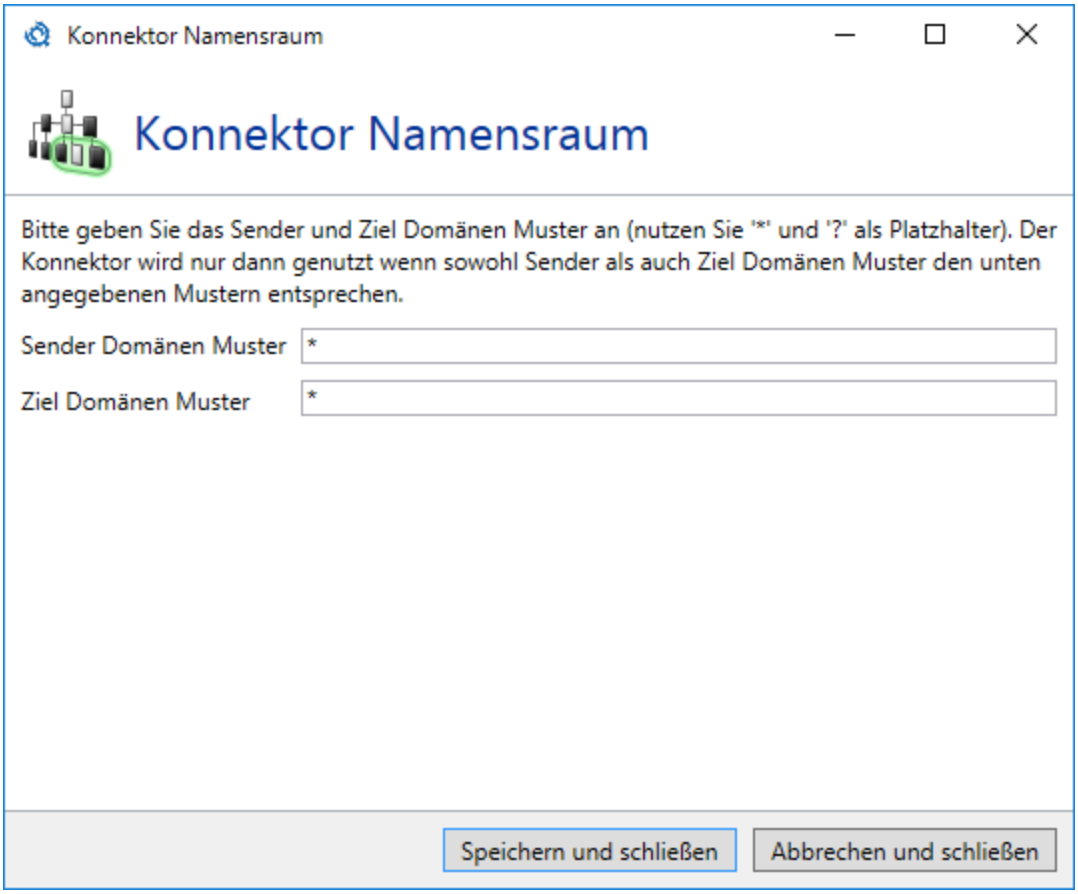
DNS-Routing-Einschränkungen durch Konnektor-Namensräume

Ein Sendekonnektor kann 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.



Ein Konnektor-Namensraum besteht aus einem Muster für sowohl die **Senderdomäne** als auch **Zieldomäne**. Dieses Muster darf auch Platzhalter (***** und **?**) enthalten.



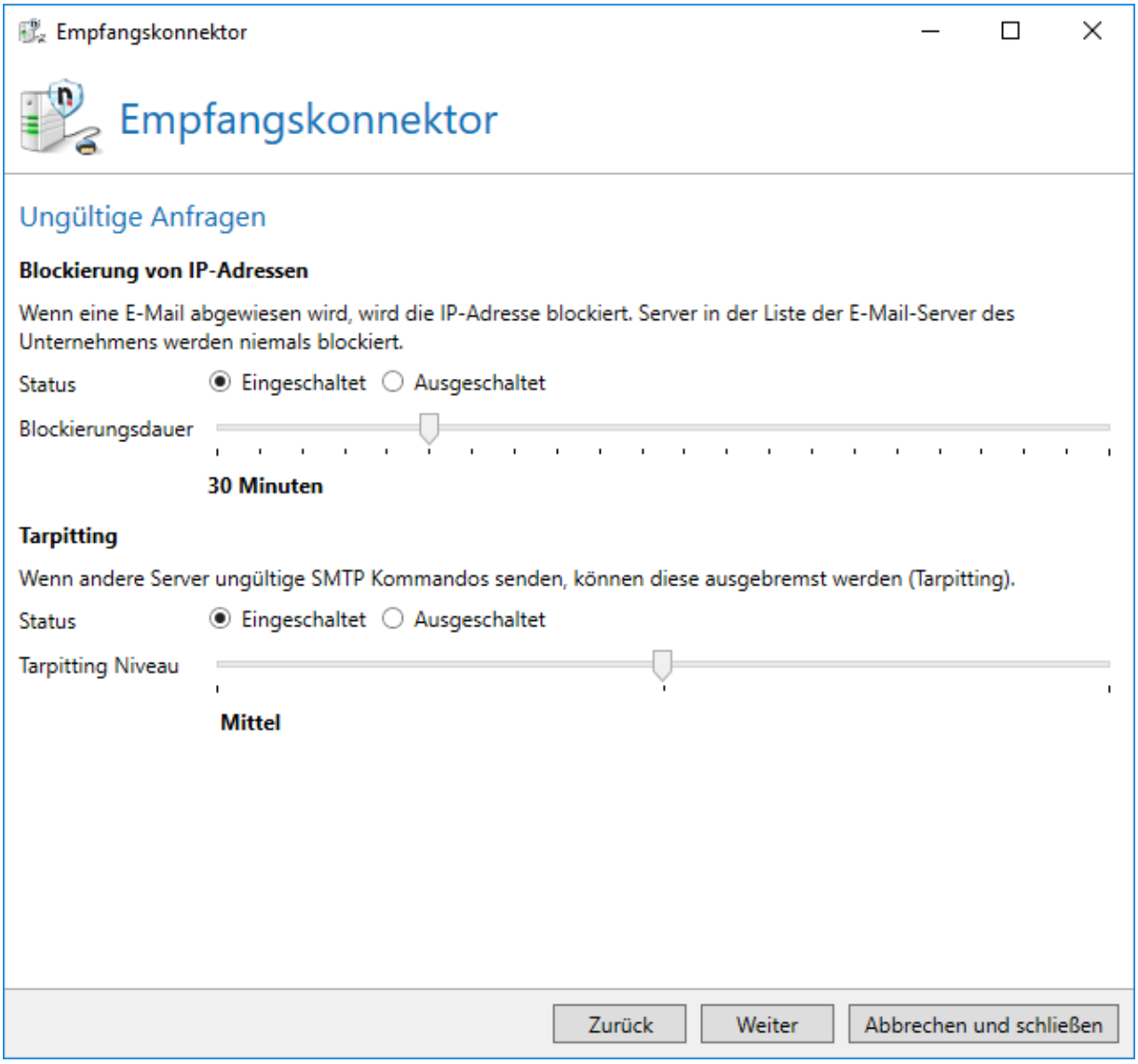
> **BEISPIEL:** Um einen Sendekonnektor für externe Adressen zu bauen, der nur E-Mails von der Domäne "example.com" an die Domäne "netatwork.de" versendet, müssen folgende Einstellungen getätigt werden.

Muster Senderdomäne	Muster Zieldomäne
example.com	netatwork.de

Ungültige Anfragen bei SMTP-Empfangskonnektoren

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 Server einzubrechen. Um diese Angriffe zu minimieren, können Sie solche Anfragen gezielt ausbremsen, beispielsweise durch das sogenannte **Tarpitting**.

Einstellungen für ungültige Anfragen bei der Konfigurierung von SMTP-Empfangskonnektoren



Blockierung von IP-Adressen| Die Blockierung dient dazu, bereits als Spam-Versender erkannte Server gezielt auszubremsen. Wenn ein Server eine E-Mail zu Ihrem NoSpamProxy sendet und diese als Spam eingestuft wird, werden nachfolgende E-Mails vom gleichen sendenden Server für den angegebenen Zeitraum blockiert.

Ein normaler E-Mail-Versender wird nach diesem Zeitraum einen neuen Versuch unternehmen die E-Mail zuzustellen.

Ein Spam-Versender wird wahrscheinlich die Zustellung abbrechen und sich auf ungeschützte E-Mail-Empfänger konzentrieren. Stellen Sie über den Radiobutton Blockierung für verdächtige IP-Adressen die Option zur Blockierung ein oder aus. Mit dem Schieberegler für den Blockierungszeitraum können Sie die Dauer der Blockierung von 5 Minuten bis zu einem Tag (1440 Minuten) festlegen.

Tarpitting| 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 oder an der falschen Stelle übermittelt wird, wartet NoSpamProxy bei jedem weiteren Befehl fünf 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.

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.

Zustellung über Warteschlangen

> **HINWEIS:** Die Option zur direkten Zustellung zum lokalen E-Mail-Server ist veraltet und seit Version 13 nicht mehr in NoSpamProxy verfügbar. Es wird immer die Zustellung über Warteschlangen angewendet.

NoSpamProxy legt die E-Mail nach dem Empfang zunächst in eine Warteschlange und leitet die E-Mail erst dann an den oder die konfigurierten Smarthosts weiter. Für den erfolgreichen Empfang der E-Mail ist es nicht relevant, ob der nächste Smarthost erreichbar ist oder nicht.

> **HINWEIS:** 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.

> **HINWEIS:** Wenn Sie unter **E-Mail-Server des Unternehmens hinzufügen** Office 365 zu den lokalen Servern hinzugefügt haben, 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 Gatewayrollen können Sie diesen Konnektor nicht modifizieren oder löschen.

Einstellungen

Allgemeine Einstellungen| Geben Sie einen Namen ein und wählen Sie eine oder mehrere Gatewayrollen 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 des Smarthost| 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.

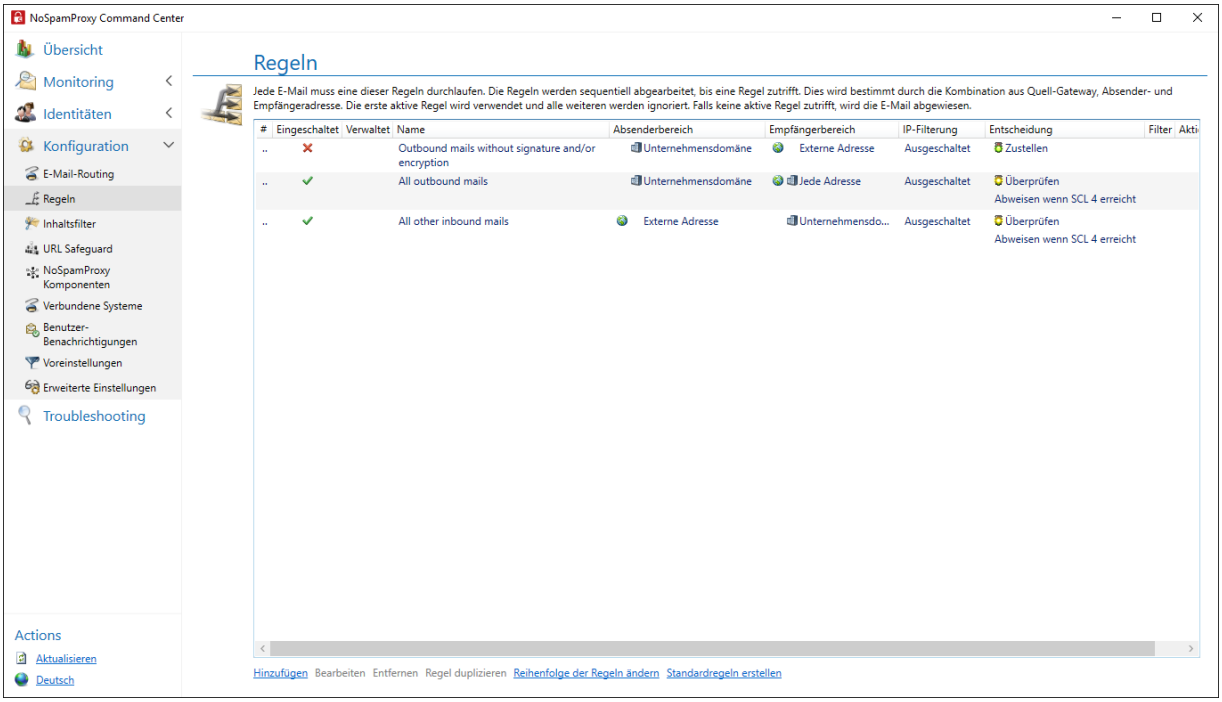
DNS-Routing-Einschränkungen| Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter DNS Routing Einschränkungen. Die Konfiguration der Einschränkungen für die lokale Zustellung läuft ab, wie unter **Mehrfach verwendete Einstellungen bei Konnektoren** beschrieben.

Headerbasiertes Routing einrichten

Sie können in NoSpamProxy ein headerbasiertes Routing einrichten. Bei diesem basiert das Routing nicht auf IP-Adressen oder Domänen, sondern auf Einträgen im Header von E-Mails.

Um headerbasiertes Routing einzurichten, kontaktieren Sie bitte unseren **Support.**

Regeln erstellen



Allgemeine Informationen

Allgemeines über Regeln

NoSpamProxy wendet bei der Bearbeitung von E-Mails Regeln an, die Sie individuell konfigurieren können. Diese Regeln 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 konfigurieren.

Sie können auch festlegen, dass Regeln nur für bestimmte IP-Adressen oder Empfänger gelten, zum Beispiel nur für Absender mit einer bestimmten TLD (Top Level Domain) oder für IP-Adressen aus einem bestimmten Subnetz.

> **TIPP:** Nach der Neuinstallation von NoSpamProxy kann nach dem Einspielen der Lizenz ein Satz von **Verwandte Themen** erstellt werden. Diese ermöglichen es, NoSpamProxy möglichst schnell und mit minimalem Administrationsaufwand die Funktion aufnehmen kann. Trotzdem sollten Sie diese Regeln überprüfen und gegebenenfalls an Ihre Bedürfnisse anpassen.

Regeln und ihre Reihenfolge

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.

Regeln, Filter und Aktionen

- Um eine E-Mail zu bearbeiten, wendet NoSpamProxy Regeln an, die Sie individuell konfigurieren können. Für jede E-Mail werden die einzelnen Filter der zutreffenden Regel ausgeführt.
- Filter bewerten, wie stark die E-Mail ein bestimmtes Filterkriterium erfüllt und vergeben entsprechende Malus- und Bonus-Punkte. Die vergebenen Punkte werden mit dem Multiplikator der Filter gewichtet und dann zu einem Gesamtwert addiert. Überschreitet dieser Wert das konfigurierte **Spam Confidence Level (SCL)** der Regel, wird die E-Mail abgewiesen. Das erlaubte SCL können Sie individuell für jede Regel einstellen. Siehe **Schritt 4: Filter konfigurieren** und **Filter in NoSpamProxy**.

- **Aktionen in NoSpamProxy** werden aufgerufen, nachdem anhand der Filter bestimmt wurde, ob die E-Mail abgewiesen wird oder sie passieren darf. Aktionen können unter anderem die E-Mails verändern, um zum Beispiel eine Fußzeile zu ergänzen oder unerwünschte Anlagen zu entfernen. Aktionen können aber auch E-Mails, die nach der Bewertung durch die Filter eigentlich passieren würden, trotzdem abweisen. Damit kann beispielsweise ein Virenscanner die E-Mail noch abweisen, obwohl sie nicht als Spam erkannt wurde. Aktionen sind also übergeordnete Einstellungen, mit denen Filter gegebenenfalls überstimmt werden können. Welche Aktionen zur Verfügung stehen und wie sie genau funktionieren, erfahren Sie unter **In NoSpamProxy verfügbare Aktionen**.

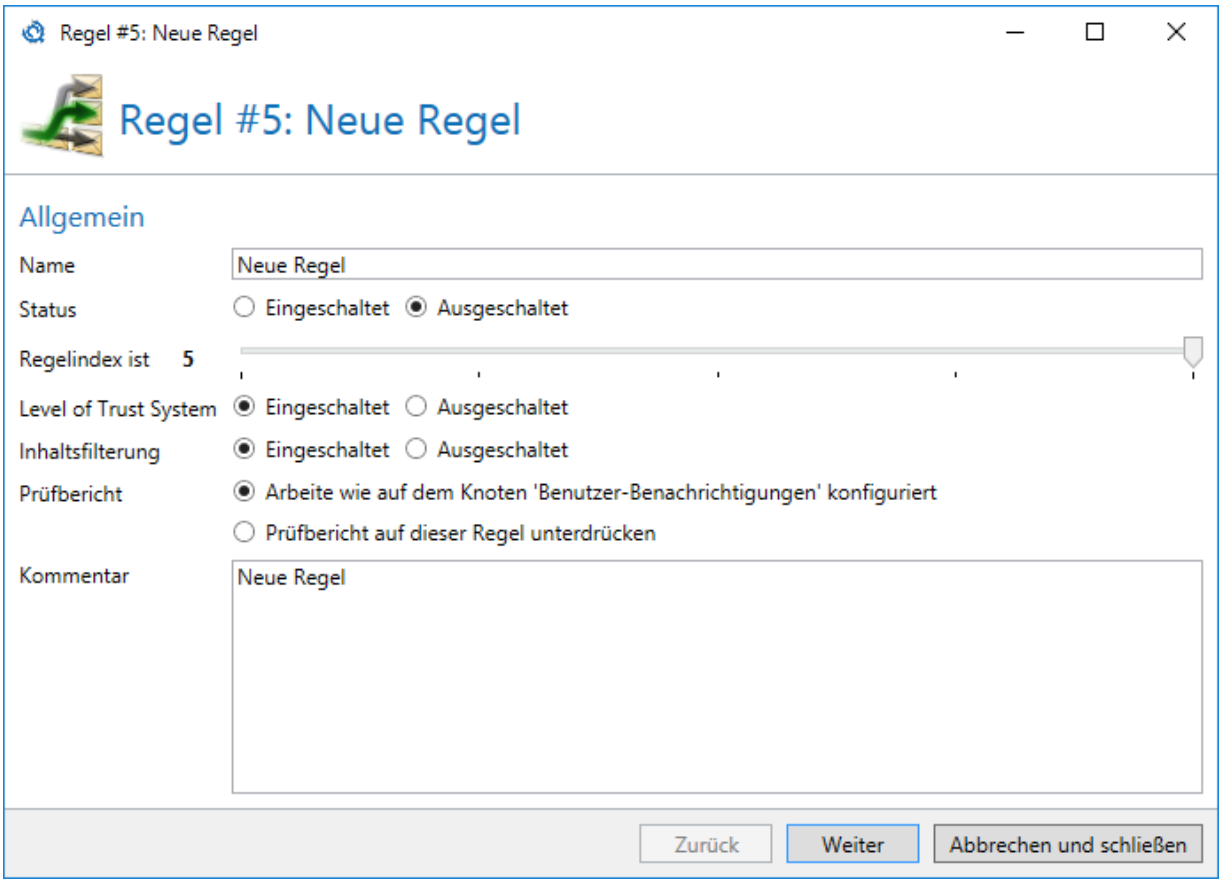
Wann gelten E-Mails als Spam?

In den Regeln konfigurieren Sie verschiedene Filter und Aktionen. Filter bewerten E-Mails und beeinflussen dadurch das **Spam Confidence Level (SCL)** der E-Mails. Das SCL bestimmt, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis ein bestimmtes SCL übersteigt.

Schritte beim Erstellen

Schritt 1: Allgemeine Einstellungen für Regeln konfigurieren

Um eine neue Regel zu erstellen, gehen Sie zu **Konfiguration > Regeln > Regeln** und klicken Sie **Hinzufügen**. Legen Sie zuerst die grundlegenden Eigenschaften für die jeweilige Regel fest.



Name| Vergeben Sie einen eindeutigen Namen für die Regel.

Status| Schalten Sie die Regel ein oder aus.

Regelindex| Legen Sie fest, an welcher Position innerhalb der Rangliste sich die Regel befinden soll.

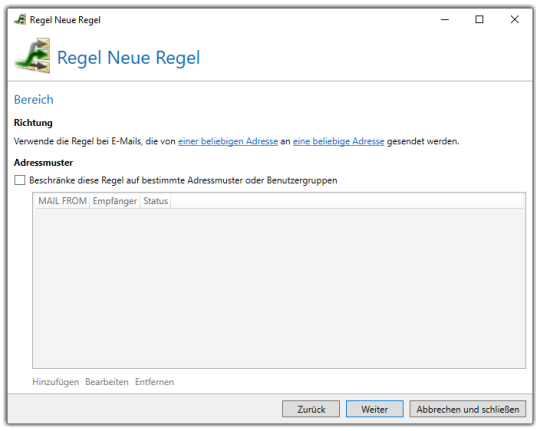
Level of Trust| Schalten Sie Level of Trust an oder aus. Siehe **Level of Trust**.

Inhaltsfilterung| Schalten Sie den Inhaltsfilter an oder aus. Siehe **Inhaltsfilter**.

Prüfbericht| Unterdrücken Sie bei Bedarf die Erstellung eines Prüfberichts für die jeweilige Regel. Siehe **Prüfbericht**.

Kommentar| Geben Sie bei Bedarf einen Kommentar ein.

Schritt 2: Den Bereich von Regeln konfigurieren



Richtung| Wählen Sie aus, für welche Absender und Empfänger die Regel gelten soll.

Adressmuster| Schränken Sie die Regel auf bestimmte Adressmuster oder Benutzergruppen ein.

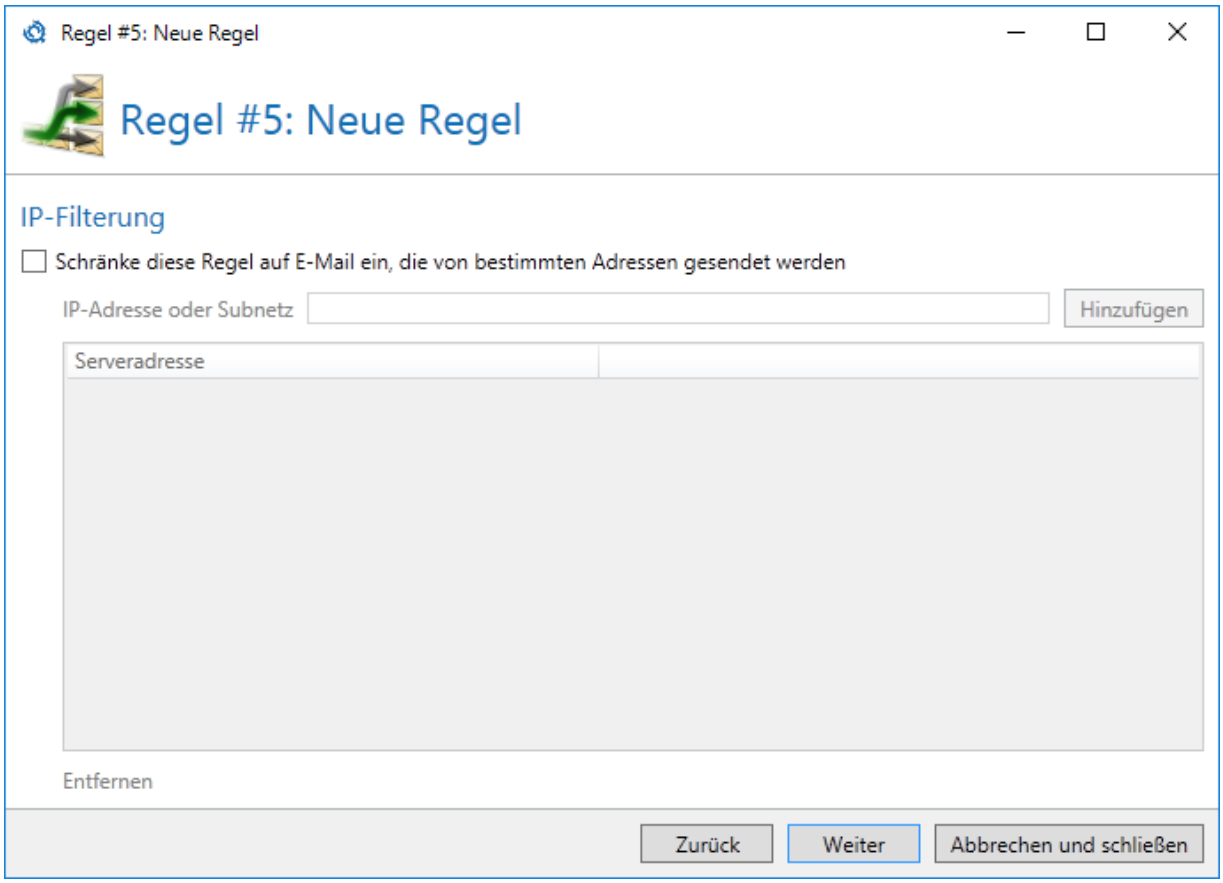
> **HINWEIS:** Verwenden Sie hierbei die MAIL-FROM-Domäne oder Teile von ihr.

> **HINWEIS:** Die maximale Anzahl an konfigurierbaren Adressmustern ist 256.

> **HINWEIS:** Um Gruppen aus einem Benutzerverzeichnis zu erhalten, müssen Sie einen automatischen Benutzerimport von LDAP- oder Active-Directory-Benutzern konfigurieren. Gruppen sind verfügbar, nachdem die erste Synchronisation durchgeführt wurde. Siehe **Benutzerimport automatisieren**.

Schritt 3: IP-Filterung bei Regeln konfigurieren

Hier können Sie die Regel auf bestimmte einliefernde Server einschränken.



1. Setzen Sie das Häkchen bei **Schränke diese Regel auf E-Mails ein, die von bestimmten Adressen gesendet werden**.
2. Geben Sie eine IP-Adresse oder ein Subnetz an
3. Klicken Sie **Hinzufügen**.

> **HINWEIS:** Die maximale Anzahl an konfigurierbaren Adressmustern ist 256.

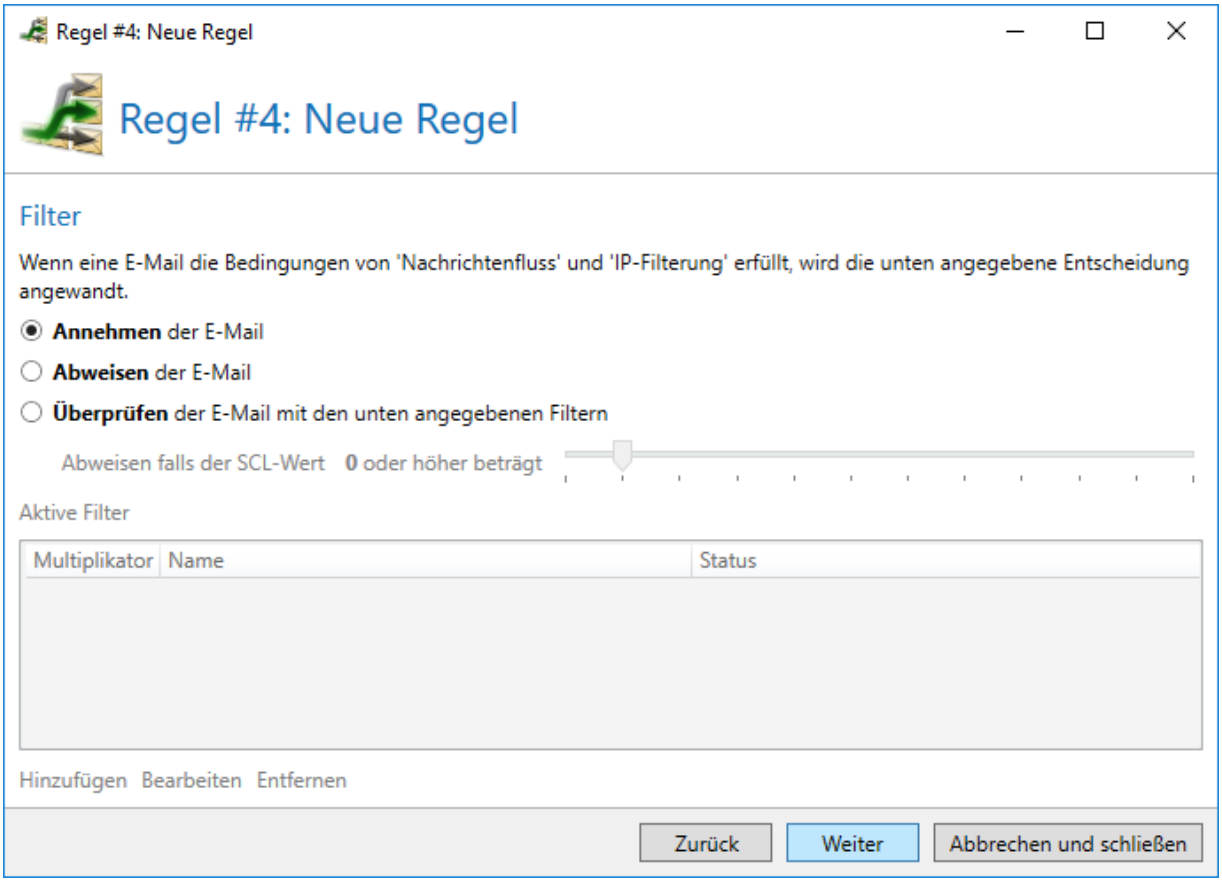
Nächste Schritte

Wenn Sie gerade dabei sind, eine neue Regel zu erstellen, wählen Sie jetzt die Filter aus. Siehe **Schritt 4: Filter konfigurieren**.

Schritt 4: Filter konfigurieren

Filter bewerten E-Mails und beeinflussen dadurch das **Spam Confidence Level (SCL)** der E-Mails. Das SCL bestimmt, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis ein bestimmtes SCL übersteigt.

Hier aktivieren Sie die gewünschten Filter für eine Regel. Sie können die Filter mit Multiplikatoren gewichten und so ihre Wirkung erhöhen oder verringern.



1. Legen Sie das grundlegende Verhalten der Filter fest.
    - **Annehmen**| Alle E-Mails, die von dieser Regel verarbeitet werden, werden angenommen.
    - **Abweisen**| Alle E-Mails, die von dieser Regel verarbeitet werden, werden abgewiesen.
    - **Überprüfen**| Alle E-Mails, die von dieser Regel verarbeitet werden, werden durch die aktiven Filter verarbeitet.

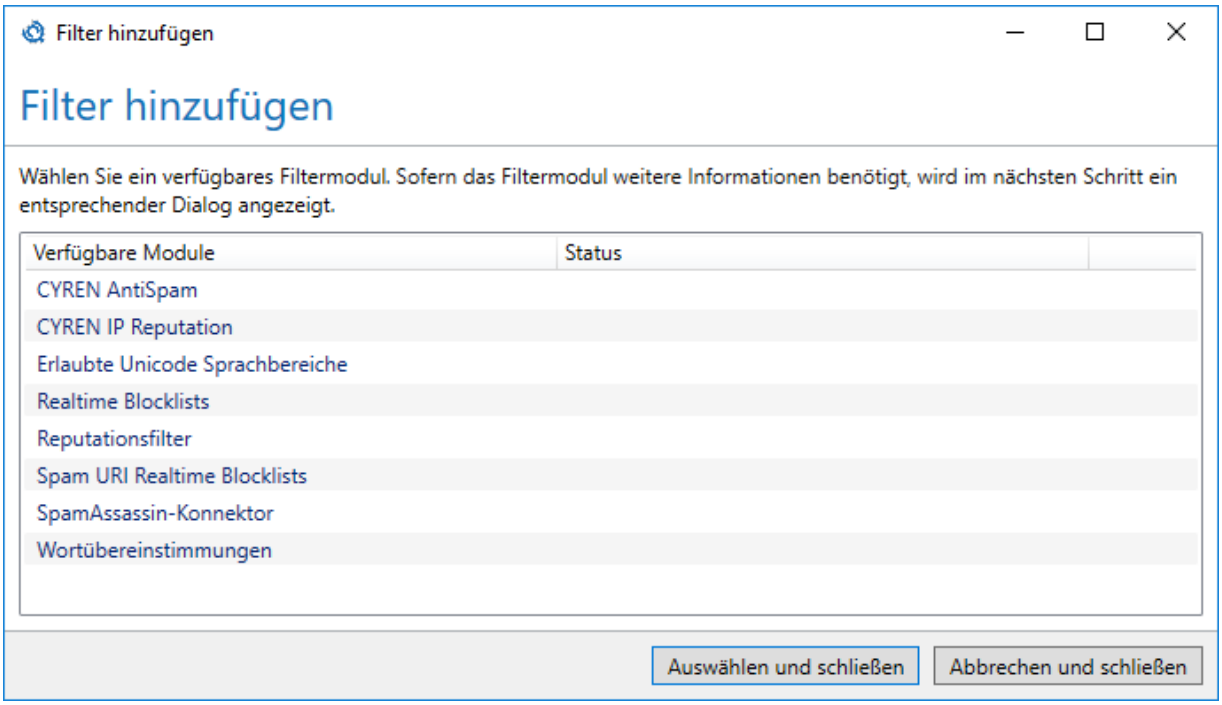
      > **HINWEIS:** Wenn Sie **Überprüfen** wählen, wird das **Spam Confidence Level (SCL)** jeder E-Mail überprüft. Wird der eingestellte Wert erreicht, wird die E-Mail als Spam abgewiesen.

2. (Optional) Klicken Sie auf **Hinzufügen**.
3. Fügen Sie einen oder mehrere Filter hinzu, indem Sie
    - diese doppelklicken oder
    - markieren und dann **Auswählen und schließen** klicken.
4. (Optional) Stellen Sie für die aktiven Filter mit Hilfe des Reglers **Multiplikatoren** ein.

    > **HINWEIS:** Der Multiplikator 5 bedeutet beispielsweise, dass der Filter fünfmal stärker gewichtet wird als ein Filter mit dem Multiplikator 1.

5. Klicken Sie **Weiter**.

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



Schritt 5: Aktionen konfigurieren

Hier wählen Sie die Aktionen aus, die abhängig vom Filterergebnis ausgelöst werden.

Konfigurieren der Aktionen

1. Klicken Sie **Hinzufügen**.
2. Fügen Sie die gewünschte Aktion der Regel hinzu, indem Sie
   - die jeweilige Aktion doppelklicken oder
   - markieren und **Auswählen und schließen** klicken.

   > **HINWEIS:** Je nach gewählter Aktion müssen Sie diese noch konfigurieren. Für Details zu den Konfigurationsoptionen der einzelnen Aktionen beachten Sie die entsprechenden Informationen. Siehe **In NoSpamProxy verfügbare Aktionen**.

3. Klicken Sie **Weiter**.

> **HINWEIS:** 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. Eine Regel mit ungültigen Aktionen wird nicht abgespeichert.

> **HINWEIS:** 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.

Schritt 6: Abweiseverhalten konfigurieren

Hier konfigurieren Sie, wie E-Mails behandelt werden, die aus anderen Gründen als einem Spam- oder Malwareverdacht abgelehnt werden.

Die folgenden grundlegenden Optionen stehen zur Verfügung:

Ablehnen und eine Unzustellbarkeitsnachricht (NDR) für eingehende E-Mails senden. Verwerfen und NDR für ausgehende E-Mails senden.| Der empfangende Server verweigert die Annahme (SMTP-Meldung 5xx). Dadurch muss der einliefernde Server eine Unzustellbarkeitsnachricht (NDR) generieren.

Verwerfen und NDR für alle E-Mails senden.| NoSpamProxy empfängt die E-Mail und sendet eine positive Quittierung an den einliefernden Server (SMTP-Meldung 200). Die E-Mail wird direkt nach der Annahme gelöscht; NoSpamProxy generiert eine Unzustellbarkeitsnachricht und sendet diese an den einliefernden Server.

Abweisen und NDR für alle E-Mails senden.| NoSpamProxy weist die E-Mail ab, generiert eine Unzustellbarkeitsnachricht und sendet diese an den einliefernden Server.

Alle E-Mails abweisen ohne NDR zu senden.| NoSpamProxy lehnt den Empfang der E-Mail ab. Der einliefernde Server muss eine Unzustellbarkeitsnachricht (NDR) generieren.

Regelindex ändern

1. Öffnen Sie die Regel.
2. Stellen Sie unter **Regelindex** die neue Position der Regel ein.
3. Klicken Sie **Speichern und schließen**.

Verwandte Themen

Standardregeln

Standardregeln ermöglichen es, NoSpamProxy möglichst schnell und mit minimalem Administrationsaufwand in Betrieb zu nehmen. Die Konfiguration der Standardregeln basiert auf dem langjährigen Betrieb zahlreicher NoSpamProxy-Installationen und stellt eine grundlegende Best-Practice-Konfiguration dar.

> **HINWEIS:** Falls Sie Standardregeln nutzen wollen, sollten Sie diese Regeln dennoch sorgfältig überprüfen und gegebenenfalls an Ihre Bedürfnisse anpassen.

Standardregeln erstellen

Sie haben zwei Möglichkeiten, Standardregeln zu erstellen:

- über den Konfigurationsassistenten oder
- unter **Konfiguration > Regeln > Regeln**.

Wie NoSpamProxy Protection eine E-Mail als Spam klassifiziert

In den Regeln konfigurieren Sie verschiedene Filter und Aktionen. Filter bewerten E-Mails und beeinflussen dadurch das **Spam Confidence Level (SCL)** der E-Mails. Das SCL bestimmt, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis ein bestimmtes SCL übersteigt. Siehe **Regeln**, **Filter in NoSpamProxy** und **Aktionen in NoSpamProxy**.

- Je höher das SCL, desto höher ist die Spamwahrscheinlichkeit.
- Je geringer das SCL, desto geringer ist die Spamwahrscheinlichkeit.
- Ein SCL von 0 besagt, dass die E-Mail als neutral eingestuft wurde.
- Der Wertebereich für das SCL reicht von -10 und +10 Punkten.

Die Filter können Sie innerhalb der Regeln mit dem Multiplikator unterschiedlich gewichten. Die Bewertung des Filters wird mit dem Multiplikator verrechnet. So können Sie den Einfluss der einzelnen Filter innerhalb einer Regel beeinflussen. Erreicht diese Gesamtgewichtung den Schwellenwert der Regel, wird die E-Mail als Spam behandelt und abgewiesen.

TIPP: Der modulare Aufbau der Regeln bietet zahlreiche Möglichkeiten zur individuellen Anpassung. Außerdem ist die Filtergewichtung mit Multiplikatoren entscheidend. Die Berechnung des SCL-Wertes wird unter **Spam Confidence Level (SCL)** beschrieben.

BEISPIEL:
Sie haben eine Regel mit einem aktiven Filter erstellt: dem Wortfilter. Außerdem ist **Level of Trust** für diese Regel aktiviert. Der Wortfilter überprüft eine E-Mail auf unerwünschte Ausdrücke. Nehmen wir an, eine E-Mail enthält eine Vielzahl von unerwünschten Ausdrücken. Der Wortfilter wird daher bei dieser E-Mail Alarm schlagen und einen hohen Malus-Wert liefern, zum Beispiel 6. Wäre der Wortfilter der einzige Filter in dieser Regel, würde die E-Mail nun einen Gesamtwert von 6 haben. Wenn Sie in der Regel beispielsweise den Schwellenwert mit der Zahl 4 eingestellt haben, würde die E-Mail jetzt geblockt und abgewiesen werden. Der Absender würde eine Unzustellbarkeitsnachricht erhalten.

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

Das Level-of-Trust-System hat immer einen Multiplikator; dieser Multiplikator setzt sich zusammen aus

- der Summe der Multiplikatoren aller auf der Regel aktivierten Filter sowie
- dem Wert 1, der zu dieser Summe hinzuaddiert wird.

Dies ergibt einen Faktor von 2 in unserem Beispiel. Der SCL Wert ergibt sich also aus 6+2*-4. Damit ergibt sich ein SCL von -2. Die E-Mail würde NoSpamProxy Protection passieren.

Inhaltsfilter erstellen

Inhaltsfilter anlegen

> Dieser Bereich ist verfügbar, wenn Sie die entsprechende Lizenz erworben haben.

Jeder **Inhaltsfilter** besteht aus allgemeinen Konfigurationen, Bedingungen und den auszuführenden Inhaltsfilteraktionen. Siehe **Inhaltsfilteraktionen anlegen**.

> **HINWEIS:** Sie müssen die Inhaltsfilteraktionen vorab konfigurieren und können diese dann in mehreren Inhaltsfiltereinträgen verwenden.

Schritt 1: Behandlung von Anhängen und den Umgang mit Archiven konfigurieren

1. Gehen Sie zu **Konfiguration > Inhaltsfilter > Inhaltsfilter** und klicken Sie **Hinzufügen**.
2. Vergeben Sie einen eindeutigen und sprechenden Namen für den Inhaltsfilter.
3. (Optional) Legen Sie die maximale Größe für E-Mails fest, indem Sie das Häkchen im Kontrollkästchen setzen und den Schieberegler betätigen.

   > **HINWEIS:** E-Mails, deren Größe die maximal erlaubte überschreitet, werden abgewiesen.

4. (Optional) Bestimmen Sie, ab welcher E-Mail-Größe die Anhänge in das Webportal verschoben werden.
5. Bestimmen Sie, ab welcher Verschachtelungstiefe E-Mails abgewiesen werden.
6. Klicken Sie **Weiter**.

HINWEIS:
NoSpamProxy unterstützt Content Disarm and Reconstruction (CDR) für folgende Archivformate:

- ZIP
- RAR
- TAR
- 7ZIP
- BZIP, auch in Kombination mit TAR
- BZIP2, auch in Kombination mit TAR
- GZIP, auch in Kombination mit TAR
- LZIP, auch in Kombination mit TAR
- XZ, auch in Kombination mit TAR

Das PDF-Dokument, das durch CDR erzeugt wurde, enthält einen Link, der auf das Originaldokument im Web Portal verweist. Die CDR-fähigen Formate werden in der Inhaltsfilteraktion auf der Registerkarte **Content Disarm** aufgelistet.

WARNUNG:
Der erste CDR-fähige Anhang aus einem Archiv wird in ein PDF-Dokument umgewandelt und an die E-Mail angehängt. Die restlichen Dateien verbleiben im Archiv und werden auf das Web Portal hochgeladen – sofern konfiguriert.

Haben Sie die Option **Verwerfe das Originaldokument** gewählt, wird das Archiv verworfen. Den Verbleib des Originaldokuments können Sie in der Inhaltsfilteraktion konfigurieren.

Schritt 2: Inhaltsfiltereinträge anlegen

1. Klicken Sie unter **Inhaltsfiltereinträge** auf **Hinzufügen**.
2. Vergeben Sie einen eindeutigen und sprechenden Namen für den Inhaltsfiltereintrag.
3. Klicken Sie unter Bedingung auf **Hinzufügen**.
4. Konfigurieren Sie die Bedingung, die für das Auslösen von Inhaltsfilteraktionen erfüllt sein muss und klicken Sie **Speichern und schließen**.

   HINWEIS: Details zu den Konfigurationsmöglichkeiten finden Sie unter **Bedingungen definieren**.

5. Wählen Sie unter **Aktionen** die Inhaltfilteraktionen aus, die auf Basis der Bedingungen ausgelöst werden.
6. Klicken Sie **Speichern und schließen**.

Der Inhaltsfiltereintrag erscheint in der Liste der Inhaltsfiltereinträge. Die Einträge werden von oben nach unten abgearbeitet und können mit den Pfeilen am linken Rand der Liste umsortiert werden.

> Warum muss ich eine Aktion für ausgehende E-Mails konfigurieren?
>
> NoSpamProxy benötigt zwingend eine Kennzeichnung als *vertrauenswürdig* durch Level of Trust, um die Aktion für vertrauenswürdige E-Mails anzuwenden. Da durch ausgehende E-Mails nur Vertrauenspunkte aufgebaut werden, fehlt diese Kennzeichnung, so dass ausgehende E-Mails technisch als nicht vertrauenswürdig angesehen werden.

Schritt 3: Inhaltsfilter zuordnen

Um einen Inhaltsfilter anzuwenden, müssen Sie ihn unter **Partner** oder **Unternehmensbenutzer** zuordnen.

Unter Partner

- in den Standardeinstellungen für Partner
    1. Gehen Sie zu **Identitäten > Partner > Partner > Standardeinstellungen für Partner**.
    2. Klicken Sie **Bearbeiten**.
    3. Wechseln Sie zur Registerkarte **Inhaltsfilter**.

- in einem Domäneneintrag eines Partners
    1. Gehen Sie zu **Identitäten > Partner**.
    2. Klicken Sie unter **Inhaltsfilterung** auf **Bearbeiten**.
- in einer Partner-E-Mail-Adresse
    1. Gehen Sie zu **Identitäten > Partner**.
    2. Öffnen Sie den Domäneneintrag eines Partners und wechseln Sie zur Registerkarte **Benutzereinträge**.
    3. Öffnen Sie den entsprechenden Benutzereintrag und wechseln Sie zur Registerkarte **Inhaltsfilterung**.

Unter Unternehmensbenutzer

- in den Standardeinstellungen für Benutzer
    1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Standardeinstellungen für Benutzer**.
    2. Klicken Sie **Bearbeiten**.
- in den Benutzereinträgen
    1. Gehen Sie zu **Identitäten > Unternehmensbenutzer > Unternehmensbenutzer**.
    2. Öffnen Sie den entsprechenden Benutzer.
    3. Wechseln Sie zur Registerkarte **Inhaltsfilterung**.

> **HINWEIS:** Die Einstellungen auf einer E-Mail-Adresse haben Vorrang vor den Einstellungen auf einer Domäne und die Einstellungen auf einer Domäne haben Vorrang vor den Standardeinstellungen für Partner.

Inhaltsfilterung regelabhängig aktivieren oder deaktivieren

Um die Inhaltsfilterung für einzelne Regeln zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Führen Sie eine der beiden folgenden Aktionen aus:
   - Öffnen Sie eine bestehende Regel.
   - Erstellen Sie eine neue Regel, indem Sie unter **Konfiguration > Regeln > Regeln** auf **Hinzufügen** klicken.
2. Schalten Sie die Inhaltsfilterung unter **Inhaltsfilterung** ein oder aus.
3. Schließen Sie die Regel beziehungsweise konfigurieren Sie diese wie gewünscht.

Siehe auch

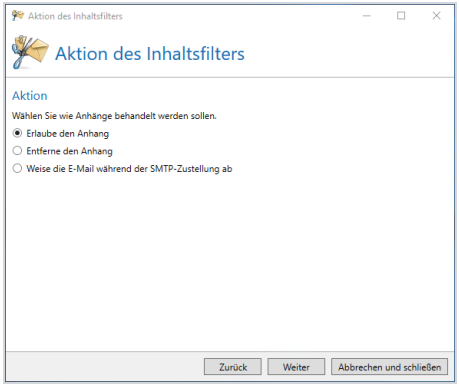
Inhaltsfilter

Inhaltsfilteraktionen anlegen

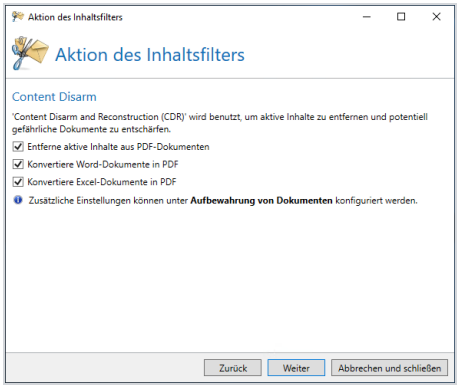
Inhaltsfilteraktionen sind Aktionen, die auf Anhängen sowie den sie enthaltenen E-Mails angewendet werden. Sie werden durch die Erfüllung von **Bedingungen**

definieren ausgelöst. Sowohl die Inhaltsfilteraktionen als auch die Bedingungen werden in Inhaltsfiltereinträgen konfiguriert, die Bestandteil der **Inhaltsfilter** sind. Ein Inhaltsfilter kann mehrere Inhaltsfiltereinträge enthalten.

1. Gehen Sie zu **Konfiguration > Inhaltsfilter > Aktionen des Inhaltsfilters** und klicken Sie **Hinzufügen**.
2. Vergeben Sie einen Namen für die Inhaltsfilteraktion, wählen Sie als Typ **SMTP-E-Mails** und klicken Sie **Weiter**.
3. Wählen Sie unter **Aktion** das grundsätzliche Verhalten für Anhänge (Erlauben/Entfernen/E-Mail abweisen).



4. Bestimmen Sie unter **Anhänge**, ob Sie die Datei in das Web Portal hochladen wollen.



5. Bestimmen Sie, ob Sie den NoSpamProxy Sandbox-Service nutzen wollen. Weitere Informationen finden Sie unter **Aktivieren des NoSpamProxy Sandbox-Service**.

   > **HINWEIS:** Diese Optionen sind nur verfügbar, wenn Sie unter **Aktion** entweder **Entfernen** oder **E-Mail abweisen** gewählt haben.

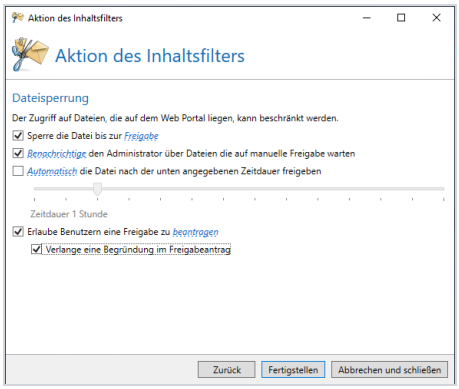
6. Bestimmen Sie, ob Sie ein Passwort für ausgehende Large-Files-Links verlangen oder den Benutzer darüber entscheiden lassen wollen und klicken Sie **Weiter**.
7. Bestimmen Sie unter **Content Disarm**, ob und wie Sie **Content Disarm and Reconstruction (CDR)** einsetzen wollen und klicken Sie **Weiter**.

   > **HINWEIS:** Details zu den Konfigurationsmöglichkeiten finden Sie unter **Hinweise zu Content Disarm and Reconstruction (CDR)**.

8. Geben Sie unter **Aufbewahrung von Dokumenten** an, wie Originaldokumente behandelt werden sollen, falls Anhänge durch CDR entschärft wurden und klicken Sie **Weiter**.

   > **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie **CDR** unter **Content Disarm** aktiviert haben.

9. Bestimmen Sie unter **Dateisperrung**, wie Dateien behandelt werden, die auf dem Web Portal liegen und klicken Sie **Fertigstellen**.



> **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie unter **Anhänge** die Nutzung des Web Portals konfiguriert haben.

> **HINWEIS:** Weitere Optionen finden Sie unter **Aufbewahrung von Dokumenten**.

1. Gehen Sie zu **Konfiguration > Inhaltsfilter > Aktionen des Inhaltsfilters** und klicken Sie **Hinzufügen**.
2. Vergeben Sie einen Namen für die Inhaltsfilteraktion, wählen Sie als Typ **Web-Portal-E-Mails** und klicken Sie **Weiter**.
3. Wählen Sie unter **Aktion** das grundsätzliche Verhalten für Anhänge (Erlauben/Verwerfen).

4. Bestimmen Sie, ob Sie Anhänge auf dem Web Portal behalten wollen und klicken Sie **Weiter**.

> **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie zuvor **Erlaube den Anhang** gewählt haben.

5. Bestimmen Sie unter **Content Disarm**, ob und wie Sie **Content Disarm and Reconstruction (CDR)** einsetzen wollen und klicken Sie **Weiter**.

> **HINWEIS:** Details zu den Konfigurationsmöglichkeiten finden Sie unter **Hinweise zu Content Disarm and Reconstruction (CDR)**.

6. Geben Sie unter **Aufbewahrung von Dokumenten** an, wie Originaldokumente behandelt werden sollen, falls Anhänge durch CDR entschärft wurden und klicken Sie **Weiter**.

> **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie **CDR** unter **Content Disarm** aktiviert haben.

7. Bestimmen Sie unter **Dateisperrung**, wie Dateien behandelt werden, die auf dem Web Portal liegen und klicken Sie **Fertigstellen**.

> **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie unter **Aktion** die Nutzung des Web Portals konfiguriert haben.

> **HINWEIS:** Weitere Optionen finden Sie weiter oben unter **Aufbewahrung von Dokumenten**.

Bedingungen definieren

Jeder Inhaltsfilter besteht aus einem oder mehreren Inhaltsfiltereinträgen. Für jeden dieser Einträge definieren Sie eine oder mehrere Bedingungen bezüglich der

- Dateitypen,
- Dateinamen und
- Dateigrößen,

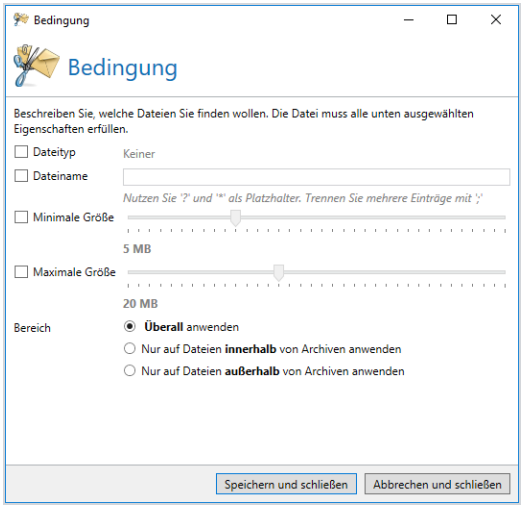
die Sie herausfiltern wollen.

Außerdem bestimmen Sie in den Bedingungen, ob der jeweilige Inhaltsfiltereintrag für Dateien

- innerhalb von Archiven,
- außerhalb von Archiven oder
- überall

angewendet wird.

1. Öffnen Sie in einem Inhaltsfilter einen Inhaltsfiltereintrag.
2. Klicken Sie unter **Bedingung** auf **Hinzufügen**.



3. Bestimmen Sie die Vorgaben bezüglich Typ, Name, Größe und Bereich.
4. Klicken Sie **Speichern und schließen**.

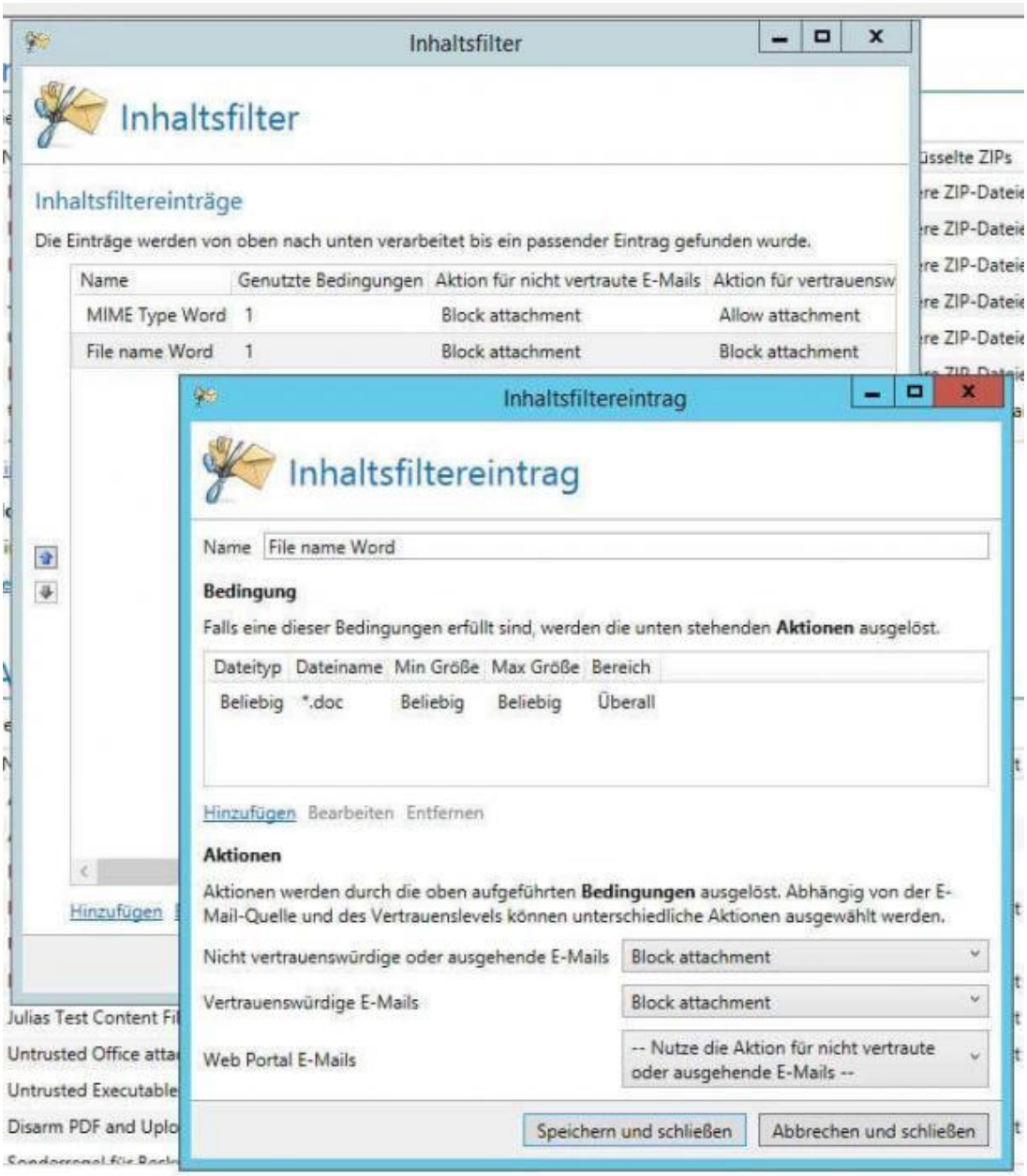
Beispielkonfigurationen des Inhaltsfilters

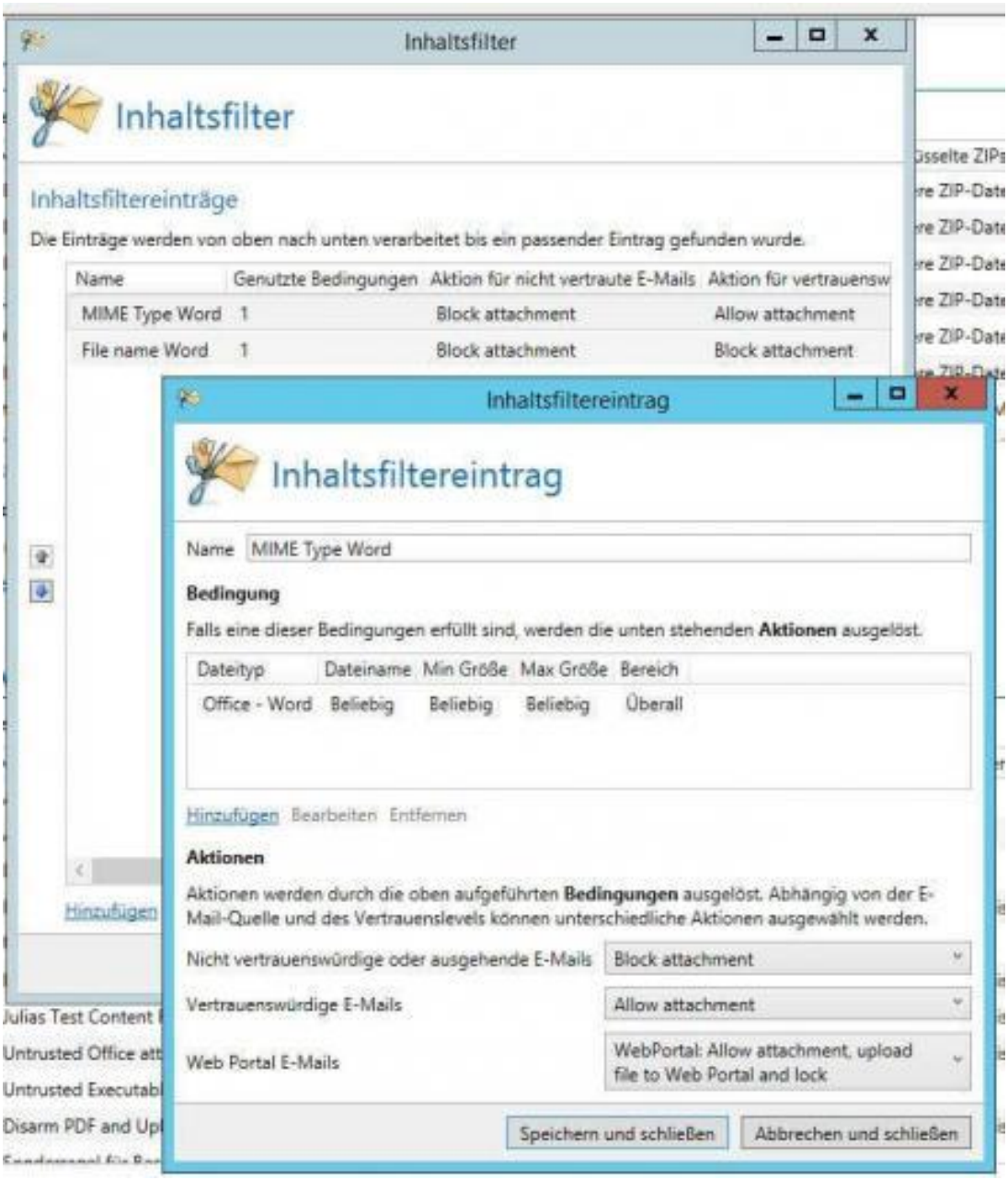
In diesem Artikel möchten wir auf die Vorgehensweise bei der Inhaltsfilter-Konfiguration eingehen. Hierbei sind die Kombinationen der Inhaltsfiltereinträge entscheidend.

Konfigurationsmöglichkeit 1

Man kann mehrere Inhaltsfiltereinträge innerhalb eines Inhaltsfilters definieren. Diese Inhaltsfiltereinträge sind ODER-verknüpft. Diese Einträge werden nach einander von oben nach unten abgearbeitet und sobald der erste Eintrag greift, werden die nachfolgenden nicht mehr berücksichtigt.

> **BEISPIEL:**
> Ein Inhaltsfiltereintrag auf Dateityp (englisch: File type) “Office – Word” und ein Inhaltsfiltereintrag auf Dateiname (englisch: Filename)”*.doc”.


Inhaltsfilter
Inhaltsfilter
Inhaltsfiltereinträge
Die Einträge werden von oben nach unten verarbeitet bis ein passender Eintrag gefunden wurde.
Name
Genutzte Bedingungen
Aktion für nicht vertraute E-Mails
Aktion für vertrauensw
MIME Type Word
1
Block attachment
Allow attachment
File name Word
1
Block attachment
Block attachment
Hinzufügen
Inhaltsfiltereintrag
Inhaltsfiltereintrag
Name
File name Word
Bedingung
Falls eine dieser Bedingungen erfüllt sind, werden die unten stehenden Aktionen ausgelöst.
Dateityp
Dateiname
Min Größe
Max Größe
Bereich
Beliebig
*.doc
Beliebig
Beliebig
Überall
Hinzufügen
Bearbeiten
Entfernen
Aktionen
Aktionen werden durch die oben aufgeführten Bedingungen ausgelöst. Abhängig von der E-Mail-Quelle und des Vertrauenslevels können unterschiedliche Aktionen ausgewählt werden.
Nicht vertrauenswürdige oder ausgehende E-Mails
Block attachment
Vertrauenswürdige E-Mails
Block attachment
Web Portal E-Mails
-- Nutze die Aktion für nicht vertraute oder ausgehende E-Mails --
Speichern und schließen
Abbrechen und schließen
Julias Test Content Fi
Untrusted Office atta
Untrusted Executable
Disarm PDF and Uplo

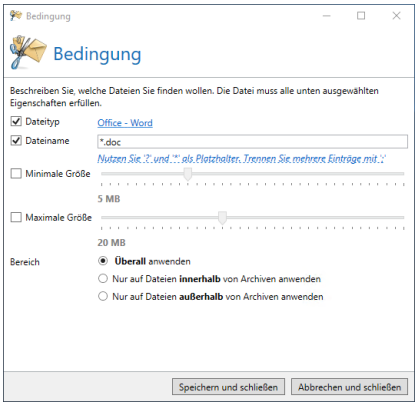

Inhaltsfilter
Inhaltsfilter
Inhaltsfiltereinträge
Die Einträge werden von oben nach unten verarbeitet bis ein passender Eintrag gefunden wurde.
Name
Genutzte Bedingungen
Aktion für nicht vertraute E-Mails
Aktion für vertrauensw
MIME Type Word
1
Block attachment
Allow attachment
File name Word
1
Block attachment
Block attachment
Hinzufügen
Inhaltsfiltereintrag
Inhaltsfiltereintrag
Name
MIME Type Word
Bedingung
Falls eine dieser Bedingungen erfüllt sind, werden die unten stehenden Aktionen ausgelöst.
Dateityp
Dateiname
Min Größe
Max Größe
Bereich
Office - Word
Beliebig
Beliebig
Beliebig
Überall
Hinzufügen
Bearbeiten
Entfernen
Aktionen
Aktionen werden durch die oben aufgeführten Bedingungen ausgelöst. Abhängig von der E-Mail-Quelle und des Vertrauenslevels können unterschiedliche Aktionen ausgewählt werden.
Nicht vertrauenswürdige oder ausgehende E-Mails
Block attachment
Vertrauenswürdige E-Mails
Allow attachment
Web Portal E-Mails
WebPortal: Allow attachment, upload file to Web Portal and lock
Speichern und schließen
Abbrechen und schließen
Julias Test Content
Untrusted Office att
Untrusted Executabl
Disarm PDF and Upl

> In diesem Fall wird zuerst auf den Dateityp geprüft und falls dieser Eintrag übersprungen wird, da der Dateityp nicht übereinstimmt, werden alle Dateien die eine Office Word Dateiendung haben durch den Folgeeintrag abgewiesen. Somit kann keine umbenannte Datei mit einer Office Word Endung zugestellt werden.

Konfigurationsmöglichkeit 2

Man kann mehrere Bedingungen innerhalb eines Filtereintrages definieren. Diese Bedingungen sind UND-verknüpft. Somit müssen beide Bedingungen auf eine Datei zutreffen, damit sie vom Inhaltsfiltereintrag bearbeitet werden

> **BEISPIEL:**
> Inhaltsfiltereintrag auf Dateityp “Office – Word” **und** Dateiname “*.doc”.



> In diesem Fall wird dieser Eintrag nur greifen, wenn die Datei einen Office Word Dateityp hat und auch auf “.doc” endet. Ansonsten wird dieser Eintrag übersprungen und der Anhang wird gegebenenfalls nicht korrekt verarbeitet.

Potentiell schädliche Dateianhänge sperren

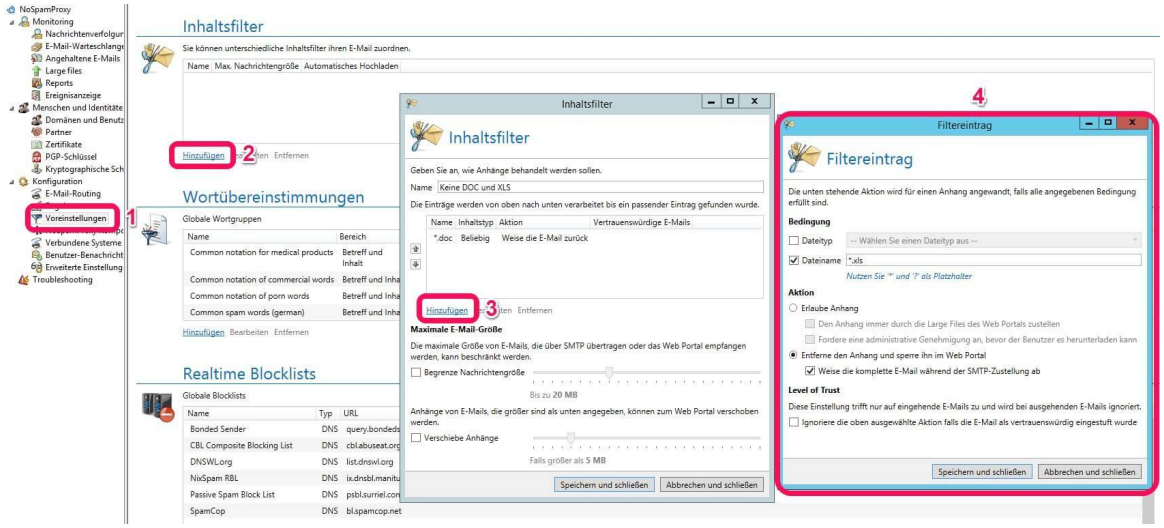
Während die meisten schädlichen Anhänge vom integrierten Malware Scanner zuverlässig erkannt werden, kommt es gelegentlich vor, dass neue Schadsoftware unerkannt bleibt. Mit Hilfe von NoSpamProxy ist es möglich,

- potentiell schädliche Anhänge generell zu blockieren,
- nur vom Level of Trust als vertrauenswürdig angesehene Absender zu erlauben oder
- Anhänge unter Quarantäne zu stellen.

HINWEIS: Beachten Sie bitte, dass die Quarantäne-Funktionalität ein funktionierendes Web Portal sowie eine Large-Files-Lizenz benötigt.

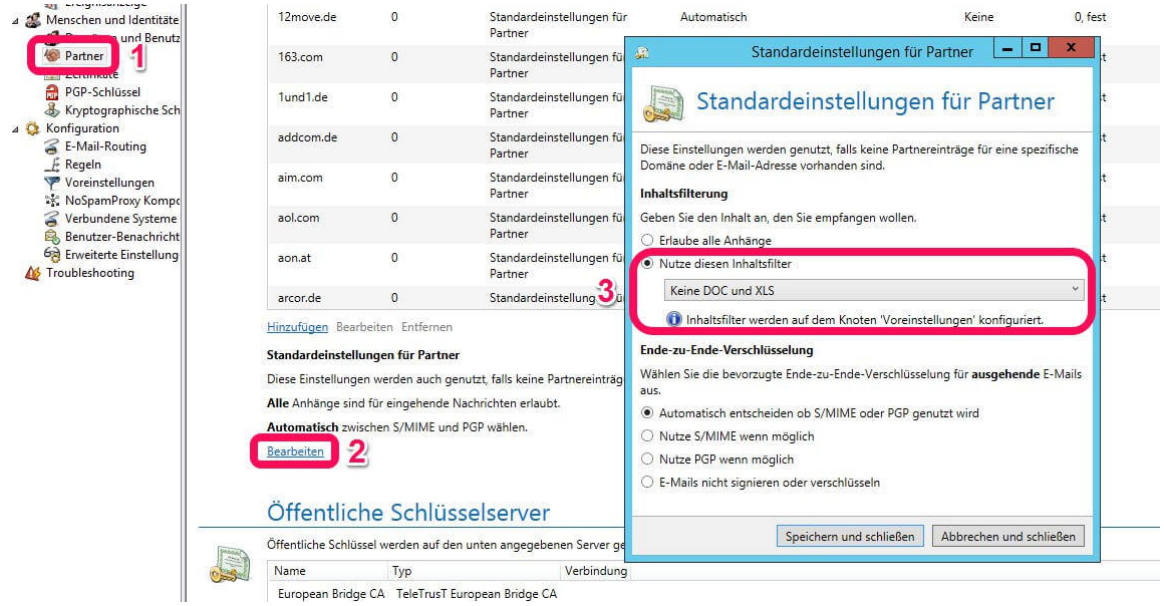
Einen Inhaltsfilter zum Sperren, Filtern oder Quarantäne von Anhängen konfigurieren

1. Gehen Sie zu **Konfiguration > Voreinstellungen**.
2. Klicken Sie auf **Hinzufügen**.
3. Vergeben Sie einen Namen für diesen Inhaltsfilter und klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie das Vorgehen für Anhänge vom gewünschten Typ.
5. Klicken Sie **Speichern und schließen**.
6. (Optional) Wiederholen Sie die Schritte 3, 4 und 5 für alle weiteren Dateitypen.



Den Inhaltsfilter für eingehende E-Mails aktivieren

1. Gehen Sie zu **Identitäten > Partner > Standardeinstellungen für Partner**.
2. Klicken Sie **Bearbeiten**.
3. Wählen Sie unter **Inhaltsfilterung** den neuen Filter aus.
4. Klicken Sie **Speichern und schließen**.



Individuelle Inhaltsfilterung für bestimmte Absender einrichten

1. Gehen Sie zu **Identitäten > Partner > Partner**.
2. Doppelklicken Sie die entsprechende Domäne.
3. Führen Sie eine der beiden Optionen aus:
    - Inhaltsfilter für Domäne einrichten
        1. Klicken Sie unter **Inhaltsfilterung** auf **Bearbeiten**.
        2. Wählen Sie den gewünschten Filter aus.
    - Inhaltsfilter für Benutzereintrag einrichten
        1. Wechseln Sie zur Registerkarte **Benutzereinträge**.
        2. Doppelklicken Sie den gewünschten Benutzer.
        3. Wählen Sie den gewünschten Filter aus.
4. Klicken Sie **Speichern und schließen**.
5. Klicken Sie **Dialog schließen**.

Liste potentiell schädlicher Anhänge und empfohlene Vorgehensweise

WARNUNG: Dies sind nur allgemeine Empfehlungen, die nicht für jedes Szenario geeignet sind. Die Anwendung erfolgt immer auf eigene Gefahr.

Ab Version 11.1 können Sie Dateien automatisiert nach einer Zeitspanne (Standard 2 Stunden) freigeben, nachdem ein erneuter Scan erfolgt ist und dieser wieder unverdächtig war. Diese Vorgehensweise empfiehlt sich insbesondere für Anhänge, die laut untenstehender Liste in der Quarantäne landen sollen.

Üblicherweise werden Schadinhalte spätestens nach 30 Minuten erkannt. Während also bei Ankunft des Inhalts dieser noch nicht als schädlich erkannt wird, kann dies bereits nach kurzer Zeit oftmals der Fall sein.

Hinweise zu Content Disarm and Reconstruction (CDR)

Die PDF-Konvertierung, auch Content Disarm and Reconstruction (CDR) genannt, wandelt Microsoft Word- und Microsoft Excel-Dokumente sowie PDF-Dokumente in PDF-Dateien um, wodurch eventuell vorhandene aktive Inhalte entfernt werden. Die PDF-Datei kann dann ohne Bedenken geöffnet werden, wobei die Originaldatei entweder an der E-Mail belassen oder entfernt werden kann.

CDR ist eine Funktion in NoSpamProxy Protection und bietet in Verbindung mit NoSpamProxy Large Files einen optimalen Weg, unsichere Dokumente zu entschärfen und die originalen Dateien zu behalten.

CDR wird in den Inhaltsfilteraktionen konfiguriert und über die Inhaltsfilter dann auf die entsprechenden E-Mails angewandt. Ein Trainingsvideo zu den Inhaltsfiltern finden Sie unter **Videos**. Siehe auch **Inhaltsfilteraktionen anlegen**.

Dieser Konvertierungsprozess ist sehr aufwendig, und nicht jedes Dokument kann konvertiert werden. Hierfür haben wir einen Schutzmechanismus eingebaut, so dass die unsicheren Anhänge – auch bei fehlgeschlagener Konvertierung – nicht zugestellt werden.

- Wenn nur Protection, aber kein Large Files, lizenziert ist, wird die E-Mail, bei der die Konvertierung nicht funktioniert hat, zunächst unter “Monitoring >

Angehaltene E-Mails” geparkt und der konfigurierte Administrator informiert. Dieser hat dann die Aufgabe, die E-Mail zu prüfen und kann diese dann entweder durch herunterladen als EML-Datei über Outlook weiterleiten oder für diese E-Mail kurzzeitig den Inhaltsfilter deaktivieren/ändern und so die Zustellung erneut erzwingen.

- Wenn Protection und Large Files lizenziert sind, wird bei fehlgeschlagener Konvertierung die Originaldatei auf das Web Portal geladen – wenn gewünscht auch bei erfolgreicher Konvertierung – dort aber dann gesperrt, so dass diese dann ebenfalls durch den Administrator freigegeben werden muss – abweichend von den Einstellungen für die erfolgreiche Konvertierung. Die E-Mail selber wird dem Empfänger zugestellt, mit der entsprechenden Information zum Herunterladen, aber ohne konvertierte PDF-Datei, da dies eben nicht möglich war.

HINWEIS: Dieser Schutzmechanismus kann nicht verändert oder beeinflusst werden.

HINWEIS: Da die Konvertierungskomponente von einem Drittanbieter bereitgestellt wird, haben wir nur sehr begrenzten Einfluss auf diese. Sollte die Konvertierung nicht zu Ihrer Zufriedenheit durchgeführt werden können, senden Sie uns – falls möglich – die zu konvertierende Datei**. Stellen Sie dabei sicher, dass die Datei keinerlei personenbezogenen Daten enthält.** Wir stellen diese Datei dann dem Drittanbieter zwecks Analyse zur Verfügung. Wir weisen darauf hin, dass eine Rückmeldung unsererseits nicht möglich ist, da der Anpassungsprozess sehr langwierig sein kann.

URL Safeguard einrichten

Den URL Safeguard aktivieren

Um den URL Safeguard einzusetzen, müssen Sie ihn als Aktion einer Regel hinzufügen. Siehe **Schritt 5: Aktionen konfigurieren**.

Den URL Safeguard konfigurieren

Weitere Einstellungen nehmen Sie in den Standardeinstellungen für Partner oder für einzelne Partnerdomänen vor. Siehe **Standardeinstellungen für Partner** sowie **Partnerdomänen bearbeiten**.

Allowlisten anpassen

NoSpamProxy-Allowlist

1. Gehen Sie zu **Konfiguration > URL Safeguard > Allowlist für Domänen > NoSpamProxy-Allowlist**.
2. Klicken Sie **Bearbeiten**.
3. Setzen oder entfernen Sie das Häkchen bei **Lade die NoSpamProxy-Allowlist automatisch herunter und nutze sie**.
4. Klicken Sie **Speichern und schließen**.

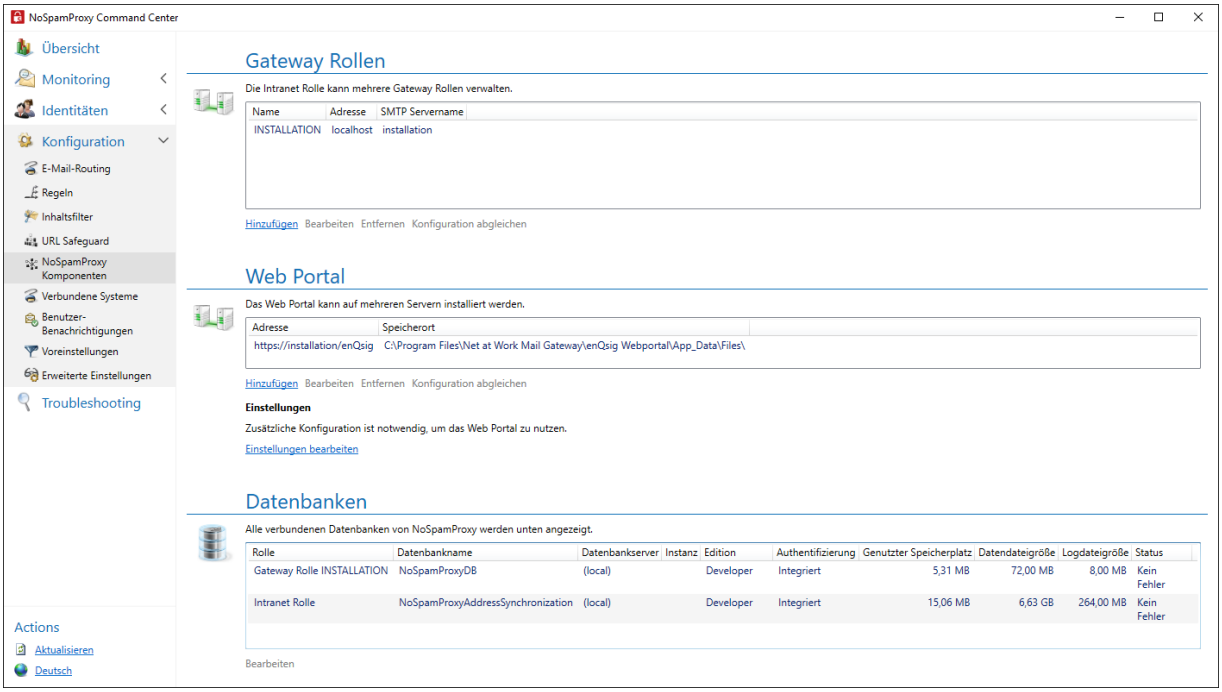
Lokale Allowlist

1. Gehen Sie zu **Konfiguration > URL Safeguard > Allowlist für Domänen > Zusätzliche Domänen**.
2. Klicken Sie **Hinzufügen**.

3. Geben Sie eine oder mehrere Domänen in das Eingabefeld ein und klicken Sie **Hinzufügen**.
4. Klicken Sie **Speichern und schließen**.

NoSpamProxy-Komponenten

Hier konfigurieren Sie die Verbindungen zwischen den einzelnen Komponenten von NoSpamProxy. Informationen zur Auswahl der Komponenten finden Sie in der Installationsanleitung.



Konfigurationsdateien der Rollen

Die Konfiguration von NoSpamProxy wird in einer XML-Datei auf dem Server gespeichert. Diese Datei kann mit einer handelsüblichen Backup-Software ohne Probleme gesichert werden. Allerdings schreibt NoSpamProxy 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 ursprüngliche Datei um, beispielsweise in *GatewayRole.config.backup*. Erst danach benennt NoSpamProxy 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.

> **HINWEIS:** Wir empfehlen, diese Datei zu sichern, bevor Sie Änderungen an der Konfiguration vornehmen. So können Sie jederzeit zum vorherigen Stand zurückkehren.

Konfigurationsdateien der Rollen

Gatewayrolle| `%ProgramData%\Net at Work Mail Gateway\Configuration\GatewayRole.config`

Intranetrolle| `%ProgramData%\Net at Work Mail Gateway\Configuration\IntranetRole.config`

ServerManagement Service| `%ProgramData%\Net at Work Mail Gateway\`

Intranetrolle

Die Intranetrolle enthält die gesamte Konfiguration von NoSpamProxy und verwaltet die kryptographischen Schlüssel.

Benutzerbenachrichtigungen einrichten

Um andere Benutzer zu berechtigen, in NoSpamProxy beispielsweise Monitoring-Funktionen zu übernehmen, müssen Sie diesen Benutzern entprechende Rollen zuweisen.

1. Öffnen Sie die Windows-Computerverwaltung auf dem System, auf dem die Intranetrolle installiert ist.
2. Gehen Sie zu **Lokale Benutzer und Gruppen > Gruppen**.

   Dort finden Sie die folgenden Gruppen:

   - NoSpamProxy Configuration Administrators
   - NoSpamProxy Disclaimer Administrators
   - NoSpamProxy Monitoring Administrators
   - NoSpamProxy People and Identities Administrators
3. Weisen Sie den ensprechenden Benutzern die gewünschten Rollen zu.

Wenn die Benutzer zu einem späteren Zeitpunkt auch Updates durchführen sollen, müssen diese Benutzer in alle Gruppen aufgenommen werden und für die Verwaltung der Datenbank der jeweiligen Rolle berechtigt werden. Siehe **Datenbankberechtigungen einrichten**.

> **HINWEIS:** Wenn NoSpamProxy auf einem Active-Directory-Domänen-Controller installiert wurde, gibt es keine lokalen Benutzergruppen mehr. Dort sind die Gruppen dann mit gleichen Namen im Active Directory zu finden.

Gatewayrolle

Hinter der Gatewayrolle verbirgt sich der eigentliche Kern von NoSpamProxy. Sie kann entweder auf demselben Server wie die Intranetrolle oder auf einem anderem Server installiert werden. In Abhängigkeit von Ihrer Umgebung kann diese Rolle entweder in eine Demilitarisierte Zone (DMZ) oder im Intranet installiert werden.

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

NoSpamProxy Encryption prüft E-Mails an Unternehmensempfänger 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, Deutschland-Online-Infrastruktur und POP3- Postfächern bereit.

HINWEIS: Um ein hochverfügbares System aufzubauen, können mehrere Gatewayrollen auf unterschiedlichen Servern installiert werden. Die aktuelle Konfiguration wird von der Intranetrolle zu allen verbundenen Gatewayrollen übertragen. Siehe **Infrastruktur-Empfehlungen**.

Konfiguration abgleichen

Es kann in Ausnahmefällen dazu kommen, dass die Konfiguration einer Gatewayrolle von der der Intranetrolle abweicht.

- Klicken Sie **Konfiguration abgleichen**, um die Konfiguration mit den markierten Rollen zu synchronisieren.

HINWEIS: Beachten Sie, dass der Datenbestand in der Datenbank der Intranetrolle dabei kurzfristig zunimmt und so zu einer vollen Datenbank führen kann. Dies ist häufig dann der Fall, wenn eine SQL-Express-Datenbank im Einsatz ist. Die Überfüllung baut sich im Normalfall wieder automatisch ab.

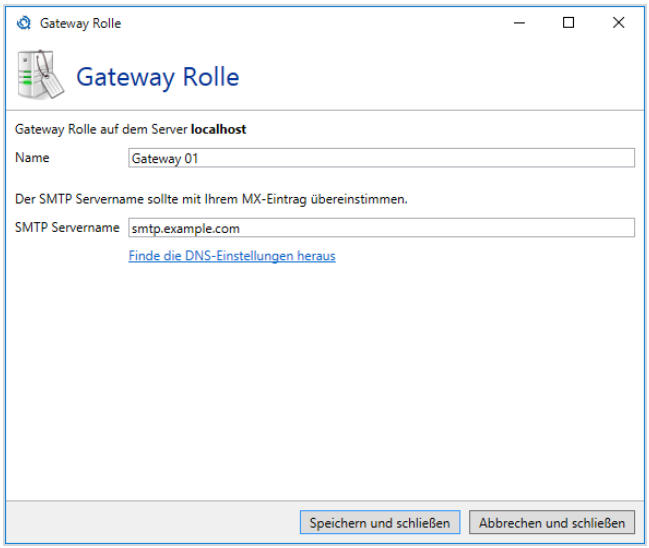
Server-Identität

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

> **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.

1. Um die genannte Einstellung zu ändern, klicken Sie unter **Server-Identität** auf **Bearbeiten**.



2. Geben Sie unter **SMTP-Servername** einen Namen an.

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

3. Klicken Sie **Speichern und schließen**.

Verbindung zu einer Gatewayrolle herstellen

> **HINWEIS:** Wenn die Gatewayrolle auf einem Server außerhalb der eigenen Domäne installiert ist, ist für die Herstellung der Verbindung ein **integriertes Administratorkonto** erforderlich. Damit ist das Windows-eigene Konto *Administrator* gemeint, nicht ein selbst erstelltes Konto mit Administratorrechten.

1. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten > Gatewayrollen**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie Ihre aktuelle Installationskonfiguration an.
4. Führen Sie einen der beiden folgenden Schritte durch:
    - Beide Rollen befinden sich auf dem gleichen Server
        - Klicken Sie **Speichern und schließen**.

- Beide Rollen befinden sich auf unterschiedlichen Servern

    1. Geben Sie unter **Servername** und **Port** den Namen und den Port der Gatewayrolle an, unter dem die Intranetrolle die Gatewayrolle erreichen kann.
    2. (Optional) Wenn das NoSpamProxy Command Center und die Intranetrolle unterschiedliche Verbindungsinformationen für die Verbindung zur Gatewayrolle benötigen, aktivieren Sie den entsprechenden Radio-Button und geben Sie den Servernamen und den Port an.
    3. Klicken Sie **Speichern und schließen**.

Verhalten von Konnektoren beim Hinzufügen von Gatewayrollen

Bei der Installation der ersten Gatewayrolle werden alle eingehenden und ausgehenden Sendekonnektoren automatisch eingeschaltet.

Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- Sendekonnektoren, die auf allen existierenden Rollen eingeschaltet waren, werden auf den neuen Rollen ebenfalls eingeschaltet.
- Sendekonnektoren, die auf einer oder mehreren Rolle(n) ausgeschaltet waren, werden auf den neuen Rollen nicht eingeschaltet.
- Empfangskonnektoren sind nicht betroffen.

Dieses Verhalten verhindert, dass es zu unerwünschtem E-Mail-Verkehr über eine neue Gatewayrolle kommt, deren Konfiguration noch nicht abgeschlossen ist.

Abfragen des Windows Performance Counter mit PRTG

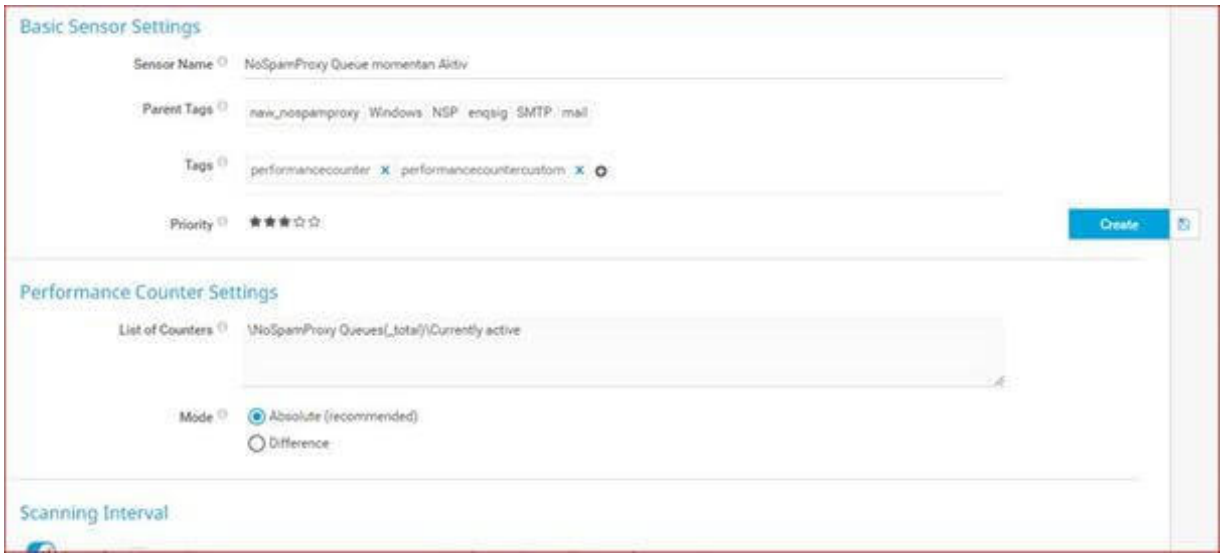
Folgende Performance Counter sind auf dem Server mit der NoSpamProxy Gatewayrolle verfügbar und können in PRTG eingebunden werden

```
\NoSpamProxy Queues(_total)\Currently active
\NoSpamProxy Queues(_total)\Delay notifications sent
\NoSpamProxy Queues(_total)\Network failures
\NoSpamProxy Queues(_total)\Non delivery Reports sent
\NoSpamProxy Queues(_total)\Pending mails
\NoSpamProxy Queues(_total)\Relay notifications sent
```

1. Wählen Sie in PRTG das Gerät (Gatewayrollen-Server) aus.
2. Fügen Sie über die rechte Maustaste einen **PerfCounter Custom Sensor** hinzu.
3. Schränken Sie die Suche nach dem anzulegenden Sensor über **Custom Sensors/Performance Counters** ein.
4. Der Sensor Name kann frei vergeben werden
5. Geben Sie unter **List of Counters** einen der oben genannten an.

   > **HINWEIS:** Das Intervall wird standardmäßig vom Host vererbt; es kann aber auch definiert werden (siehe unten).

6. Klicken Sie **Create**.



Parallele ausgehende Verbindungen setzen

Um die Anzahl der ausgehenden Verbindungen der Gatewayrolle zu ändern, gehen Sie folgendermaßen vor:

1. Stoppen Sie die Gatewayrolle, für die Sie die Änderungen vornehmen wollen.
2. Gehen Sie zu **C:\ProgramData\Net at Work Mail Gateway\Configuration** auf der Gatewayrolle.
3. Öffnen Sie die Datei **Gateway Role.config**.
4. Fügen Sie unterhalb des Tags `<netatwork.nospamproxy.proxyconfiguration ... >`, im Tag `<queueConfiguration>` die folgenden Attribute an:

```
maxConcurrentConnections="AnzahlDerVerbindungen"
```

```
maxConcurrentConnectionsPerDomain="AnzahlDerVerbindungen"
```

5. Speichern Sie die Datei.

Dies begrenzt die Anzahl der parallelen Verbindungen auf 100, wobei pro Domain nur maximal 10 gleichzeitige Verbindungen erlaubt sind.

> **BEISPIEL:** `<queueConfiguration maxConcurrentConnections="100" maxConcurrentConnectionsPerDomain="10" />`

Parallele eingehende Verbindungen setzen

NoSpamProxy legt die Anzahl der parallelen Verbindungen dynamisch selbst fest. Als Grundlage für diese Entscheidung gilt die CPU- und Speicherauslastung. Um dieses Verhalten zu unterbinden, gehen Sie wie folgt vor:

1. Stoppen Sie die Gatewayrolle.
2. Gehen Sie zu **C:\ProgramData\Net at Work Mail Gateway\Configuration** auf der entsprechenden Gatewayrolle.
3. Öffnen Sie die Datei **Gateway Role.config**.
4. Suchen Sie nach der Zeile, die mit folgenden Zeichen beginnt: `<netatwork.nospamproxy.proxyconfiguration...`

5. Fügen Sie unter dieser Zeile den folgenden Wert ein:

```
<connectionLimits
hardUpperConnectionLimit="AnzahlDerVerbindungen"
minimumNumberOfConcurrentSessions="AnzahlDerVerbindung
en" />
```

6. Speichern Sie die Konfigurationsdatei.
7. Starten Sie anschließend die Gatewayrolle.

Wenn die Werte wie in diesem Beispiel nicht angegeben sind, gilt das dynamische Limit (je nachdem wie die CPU Auslastung ist). Beide Werte sind ganzzahlige Werte.

- Mit dem Wert `hardUpperConnectionLimit` legen Sie das maximales Limit an Verbindungen fest.
- Der Wert `minimumNumberOfConcurrentSessions` bestimmt die minimale Anzahl von gleichzeitigen Verbindungen.

> **BEISPIEL:** `<connectionLimits hardUpperConnectionLimit="100" minimumNumberOfConcurrentSessions="50" />`

Anpassen von SMTP-Verbindungseigenschaften

1. Öffnen Sie die Datei **Gateway Role.config** im Verzeichnis “**C:\ProgramData\Net at Work Mail Gateway\Configuration**.
2. Suchen Sie die folgende Zeile: `<netatwork.nospamproxy.proxyconfiguration ... >`

3. Fügen Sie direkt unter dieser Zeile den folgenden Eintrag hinzu:

```
<smtpServicePointConfiguration
maxActiveConnectionsPerEndPoint="25"
maxConnectionIdleTime="00:01:00"
isServicePointRecyclingEnabled="false"
maximumMailsPerSession="2" />
```

4. Passen Sie die Werte auf den gewünschten Wert an.

HINWEIS: Bevor Sie die Datei **Gateway Role.config** abspeichern, müssen Sie den Dienst **NoSpamProxy – Gateway Role** Dienst beenden. Erst dann können Sie die Konfigurationsdatei ordnungsgemäß abspeichern.

Anpassen der Zustellversuche und Wiederholungsintervalle

Die Standardeinstellungen sind wie folgt:

- Der erste Versuch erfolgt nach fünf Minuten.
- Der zweite Versuch erfolgt nach zehn Minuten.
- Der dritte Versuch erfolgt nach 15 Minuten.
- Jeder weitere Versuch erfolgt alle 30 Minuten.
- Die erste Zustellverzögerungsbenachrichtigung wird nach sechs Stunden erzeugt.
- Nach einem Tag wird die Zustellung eingestellt.

Um Änderungen an den Einstellungen vorzunehmen, gehen Sie wie folgt vor:

1. Stoppen Sie die Gatewayrolle.
2. Gehen Sie zu **C:\ProgramData\Net at Work Mail Gateway\Configuration** auf allen Computern, auf denen Gatewayrollen installiert sind.
3. Finden Sie die Datei **Gateway Role.config**.
4. Finden Sie die folgende Zeile in der Datei:
   `<netatwork.nospamproxy.proxyconfiguration ... >`
5. Fügen Sie direkt unter dieser Zeile folgenden Eintrag hinzu, falls er nicht schon in ähnlicher Form existiert:

```
<queueConfiguration firstRetryInterval="00:15:00"
secondRetryInterval="00:30:00"
thirdRetryInterval="01:00:00"
subsequentRetryInterval="04:00:00"
expirationTimeout="3.00:00:00"
sendDelayNotificationAfter="12:00:00" />
```

6. Passen Sie die Werte wie gewünscht an.
7. Speichern Sie die Datei ab.
8. Starten Sie die angehaltene(n) Gatewayrolle(n).

Web Portal

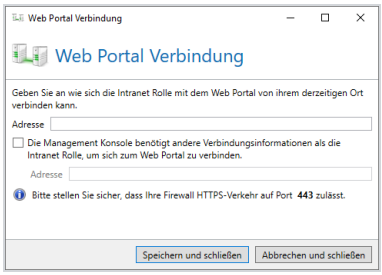
Das Web Portal ermöglicht Benutzern das Hinterlegen von Passwörtern für PDF Mail sowie das Verfassen von Antworten auf PDF Mails.

> **HINWEIS:** Um ein hochverfügbares System aufzubauen, kann das Webportal auf mehreren Servern installiert werden.

Intranetrolle und Web Portal verbinden

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

1. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten > Web Portal**.
2. Klicken Sie **Hinzufügen**.



3. Geben Sie unter **Adresse** die HTTPS-Adresse des Webportals an.
4. Wenn das NoSpamProxy Command Center eine abweichende Adresse für die Verbindung zum Webportal benötigt, setzen Sie das Häkchen in der Checkbox und tragen Sie diese Adresse ein.
5. Klicken Sie **Speichern und schließen**.

Konfiguration abgleichen

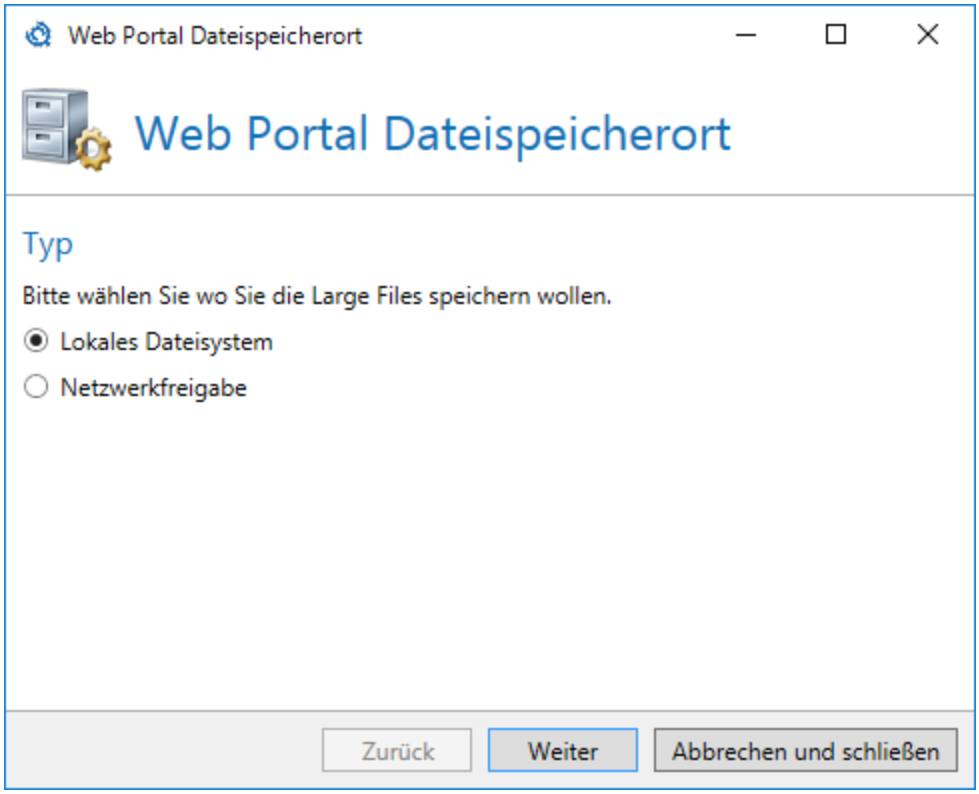
Es kann in Ausnahmefällen dazu kommen, dass die Konfiguration eines Webportals von der der Intranetrolle abweicht.

- Klicken Sie in diesem Fall **Konfiguration abgleichen**, um die Konfiguration mit den markierten Webportalen zu synchronisieren.

> **HINWEIS:** Beachten Sie, dass der Datenbestand in der Datenbank der Intranetrolle dabei kurzfristig zunimmt und so zu einer vollen Datenbank führen kann. Dies ist häufig dann der Fall, wenn eine SQL-Express-Datenbank im Einsatz ist. Die Überfüllung baut sich im Normalfall wieder automatisch ab.

Dateispeicherort konfigurieren

Sie können den Dateispeicherort für große Dateien, die Sie über NoSpamProxy Large Files versenden, nach der Einrichtung der Verbindung anpassen.



Die folgenden Speicherorte stehen zur Verfügung:

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 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.

Amazon S3| Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicher-Service.

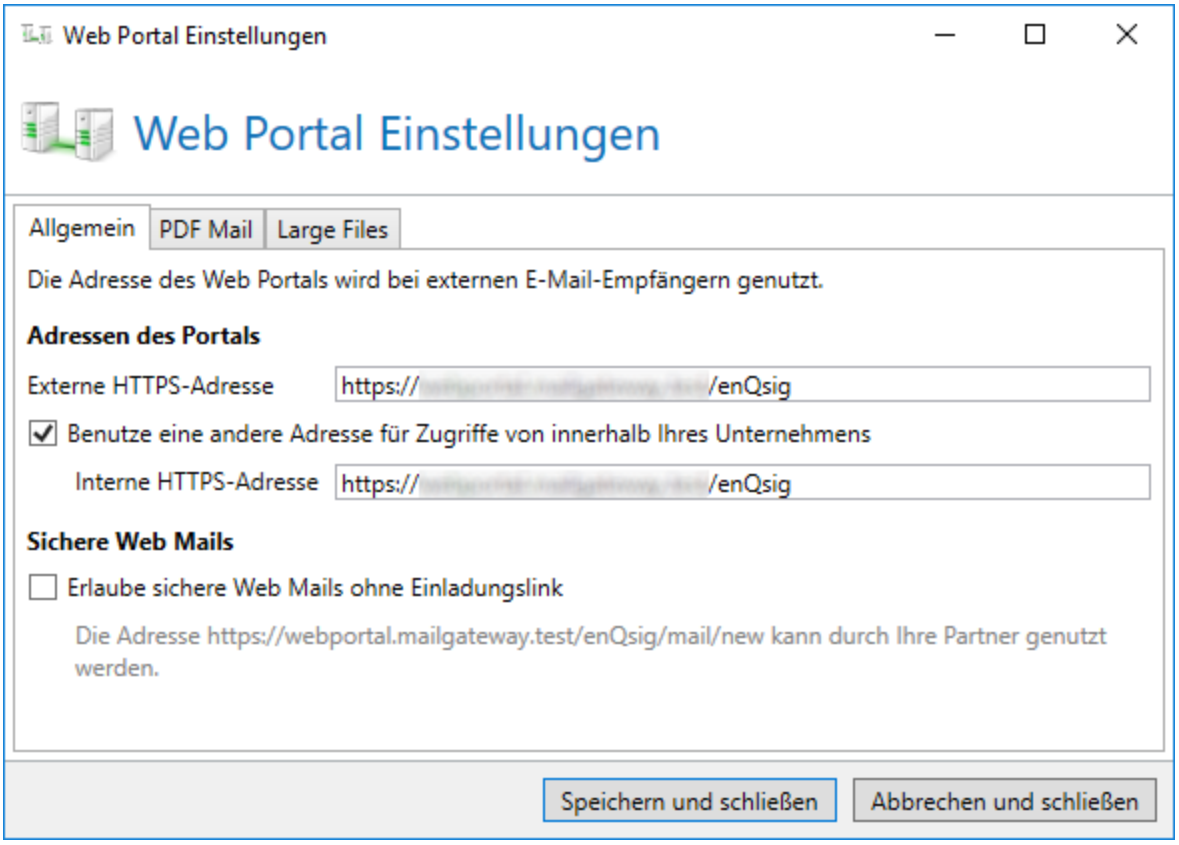
> **HINWEIS:** Um Amazon S3 als Speicherort nutzen zu können, müssen Sie diese Option mit Hilfe des PowerShell-Cmdlets **Set-NspWebPortalSettings** aktivieren.

Allgemeine Einstellungen bearbeiten

Unter **Konfiguration > NoSpamProxy-Komponenten > Webportal > Einstellungen** werden die derzeiten Einstellungen für das Webportal angezeigt.

- Klicken Sie **Einstellungen bearbeiten**, um Änderungen an den Einstellungen vorzunehmen.

Registerkarte Allgemein



Adressen des Portals| Bei Benutzung des Web Portals wird in E-Mails gegebenenfalls ein Link auf das Web Portal eingefügt. Der Link beinhaltet dabei die Adresse, unter der das Web Portal aus dem Internet erreichbar ist

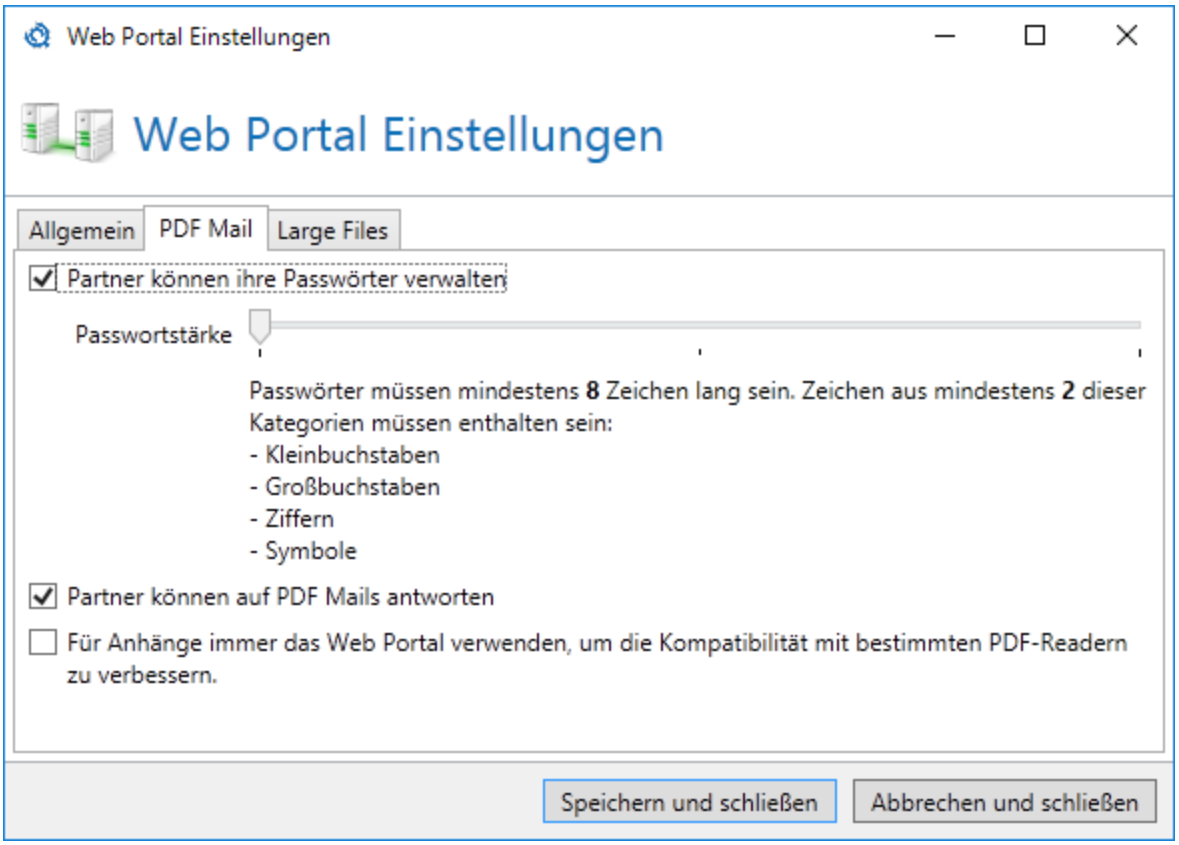
- Geben Sie unter **Externe HTTPS-Adresse** die Adresse ein, unter der das Web Portal erreichbar ist.
- Um für den Zugriff aus dem Firmennetzwerk eine andere Adresse zu verwenden, tragen Sie diese unter **Interne HTTPS-Adresse** ein.

Sichere Web Mails| Untere **Sichere Web Mails** können Sie eine Adresse angeben, über die das Web Portal auch ohne Einladungslink verwendet werden kann. Wird das Webportal auf diese Weise verwendet, so kann ein externer Partner über das

Webportal eine E-Mail an Empfänger in Ihrem Unternehmen senden. Dazu muss er eine Absenderadresse und eine gültige Empfängeradresse eines in NoSpamProxy hinterlegten Unternehmensbenutzers eintragen.

> **HINWEIS:** 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.

Registerkarte PDF Mail

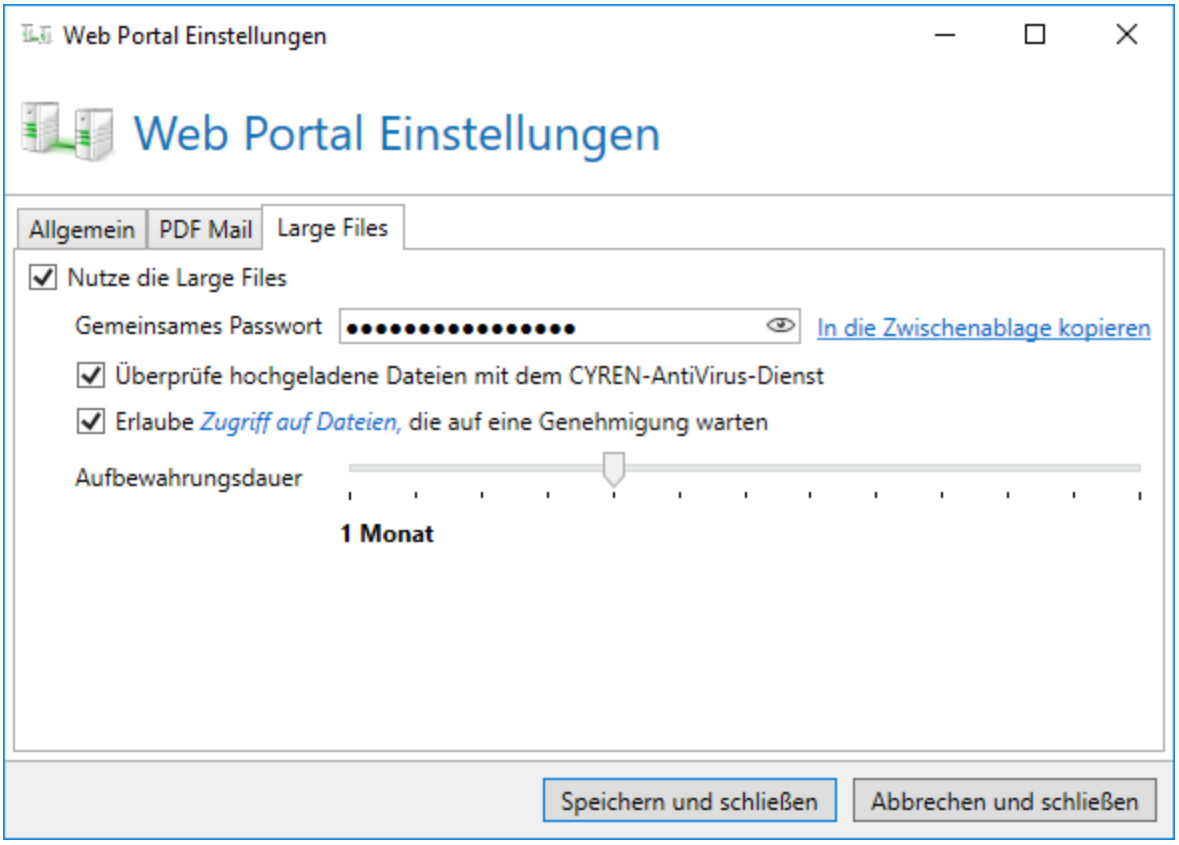


Partner können Ihre Passwörter verwalten| Aktivieren Sie dieses Feature, wenn Sie möchten, dass Kommunikationspartner ihre Passworte für PDF Mails selbst verwalten können. Hat ein Partner noch kein Passwort hinterlegt, so wird er von NoSpamProxy zunächst aufgefordert, eines zu hinterlegen, bevor eine 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.

Partner können auf PDF Mails antworten| Wenn dieses Feature aktiviert ist, können Kommunikationspartner auf PDF Mails über das Webportal Antworten versenden. Damit wird eine sichere Zwei-Wege-Kommunikation ohne Zertifikate ermöglicht.

Für Anhänge immer das Webportal verwenden| Wenn Sie diese Funktion aktivieren, werden Anhänge in PDF Mails immer in das Webportal hochgeladen. In der PDF Mail verbleibt dann lediglich ein Link. Dies verbessert die Kompatibilität mit PDF-Readern, beispielsweise auf Mobilgeräten, die keine Anhänge unterstützen.

Registerkarte Large Files



Nutze Large Files| Aktiviert die Large-Files-Funktion.

Gemeinsames Passwort| Um die Kommunikation zwischen dem Outlook Add-In und dem Webportal abzusichern, ist ein gemeinsames Passwort 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.

Erlaube Zugriff auf Dateien, die auf Genehmigung warten| Wenn Sie Dateien, die auf die Genehmigung warten, vor der Genehmigung überprüfen wollen, müssen Sie dies hier explizit erlauben.

Aufbewahrungszeit| Nachdem die Datei unter **Large Files** genehmigt wurde, ist kein weiterer Zugriff durch die 'Monitoring Administrators'-Gruppe möglich.

Hinweise zur Einbindung des Web Portals

Bei der Einbindung des Web Portals in die Konfiguration müssen in bestimmten Einsatzszenarien besondere Einstellungen beachtet werden:

Das Web Portal wird parallel zur Gatewayrolle und/oder Intranetrolle betrieben

Beachten Sie in diesem Fall den entsprechenden **Artikel KB926642 in der Microsoft-Dokumentation**.

Dabei wird **Methode 1: Erstellen der LSA-Hostnamen (Local Security Authority)**, die in einer NTLM-Authentifizierungsanforderung referenziert werden können empfohlen. Dies gilt insbesondere für Produktivumgebungen.

> **WARNUNG: Methode 2: Deaktivieren der Loopback-Funktionalität für die Authentifizierung** sollte nur auf Testumgebungen angewandt werden!

> **HINWEIS:** Die Artikel bei Microsoft vertauschen die Methoden in der englischen und deutschen Variante. Prüfen Sie immer die genaue Bezeichnung.

Das Web Portal wird auf einem System in der DMZ/auf Computer(n) außerhalb der Domäne betrieben

Beachten Sie hier den entsprechenden **Artikel KB951016 in der Microsoft-Dokumentation**.

Webportal-Design ändern

Dieser Artikel beschreibt, wie Sie in NoSpamProxy 10 die verwendeten Farben und das Logo des Web Portals ändern können.

> **HINWEIS:** Sie benötigen zumindest rudimentäre HTML-Kenntnisse, um die Anpassungen durchführen zu können.

- Die entsprechenden Dateien liegen im Verzeichnis **%Program Files%\Net at Work Mail Gateway\enQsig Webportal**.
- Änderungen nehmen Sie in den Dateien **..\Content\Site.css** (Farbanpassungen) und die Datei "**..\Views\Shared_Layout.cshtml**" (Logo und anderes).

Ändern der Farben

Um die Farben zu editieren, editieren Sie die Datei `Site.css`. Es gibt vier relevante Stellen für die Farbe:

Oberer Bereich

```
header
{
     margin: 0 auto 0 auto;
     border-bottom: 10px solid #C01B1B;
     width: 100%;
     background-color: white;
}
```

- Diese Stelle markiert den farbigen Balken im oberen Bereich. Ändern Sie den Wert `#C01B1B` auf einen anderen Wert, um die Farbe zu ändern.
- Um die Stärke des Balkens zu ändern, erhöhen oder reduzieren Sie den Wert `10px`.

Fortschrittsbalken

```
.dz-upload
{
     height: 2px;
     background-color: #C01B1B;
     width: 0;
}
```

- Dieser Bereich bestimmt die Farbe des Fortschrittsbalkens, sobald eine Datei auf das Web Portal übertragen wird. Mit `height` verändern Sie die Stärke des Balkens, mit `background-color` ändern Sie die Farbe.

Actionbuttons

```
.actionRow .button
{
     background: #C01B1B;
     padding-top: 16px;
     padding-bottom: 16px;
     padding-left: 24px;
     padding-right: 24px;
     clear: both;
     margin: 15px 0 0 0;
     color: white;
     text-decoration: none;
     border: none;
}
```

- Dieser Bereich bestimmt das Aussehen der Actionbuttons, wie zum Beispiel der Button **Anmelden**. Sie können hier die Farbe mit `background` ändern oder die Größe mit `padding`.

Schriftfarbe der Auflistung aller bereits hochgeladenen Dateien

```
.FileName
{
     color: #C01B1B;
     padding: 4px 0 4px 0;
}
```

Ändern des Logos

Um das angezeigte Logo zu ändern, editieren Sie die Datei **_Layout.cshtml**. Die folgende Zeile ist für die Darstellung des Logos verantwortlich:

```
<img class="logo" src="@Url.Content
("~/Content/Images/NoSpamProxy.png")" alt="Logo" title="Logo"
/>
```

Benennen Sie hier die Position und den Namen der neuen Datei und speichern die Einstellungen ab.

Datenbanken

Unter Datenbanken nehmen Sie Änderungen der Verbindung zur Datenbank der entsprechenden Rolle vor.

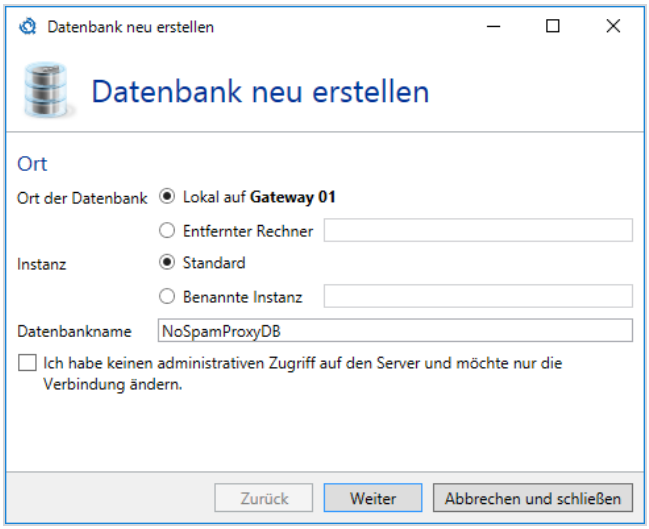
> **HINWEIS:** Die Datenbank wird während des Setups eingerichtet. Änderungen müssen Sie nur im Falle eines Umzugs der Datenbank auf einen anderen SQL-Server vornehmen.

Verbindungseinstellungen der Datenbank ändern

> **HINWEIS:** Bevor Sie die Verbindungseinstellungen ändern, sichern Sie die bestehende Datenbank und spielen Sie diese Sicherung auf dem neuen Datenbank-Server ein.

HINWEIS: Jede Datenbank der Rollen ist eigenständig und darf nicht zwischen den Rollen geteilt werden. Das heißt, dass Sie bei zwei Gatewayrollen 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.

1. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten > Datenbanken**.
2. Klicken Sie **Bearbeiten**.



3. Geben Sie unter **Ort der Datenbank** an, auf welchem Server sich die Datenbank befindet.

> **HINWEIS:** Wenn sich die Datenbank auf demselben Server wie die Gatewayrolle befindet, wählen Sie **Lokaler Server**. Ist die Datenbank auf einem anderen Server eingerichtet, wählen Sie zunächst die Option **Entfernter Rechner** und geben Sie dann im Eingabefeld entweder die IP-Adresse oder den voll qualifizierten Domänennamen (FQDN) des Servers ein, auf dem sich die Datenbank befindet.

4. Geben Sie unter **Instanz** an, ob für die Datenbank der Gatewayrolle die Standardinstanz des SQL-Servers oder eine benannte Instanz genutzt wird.

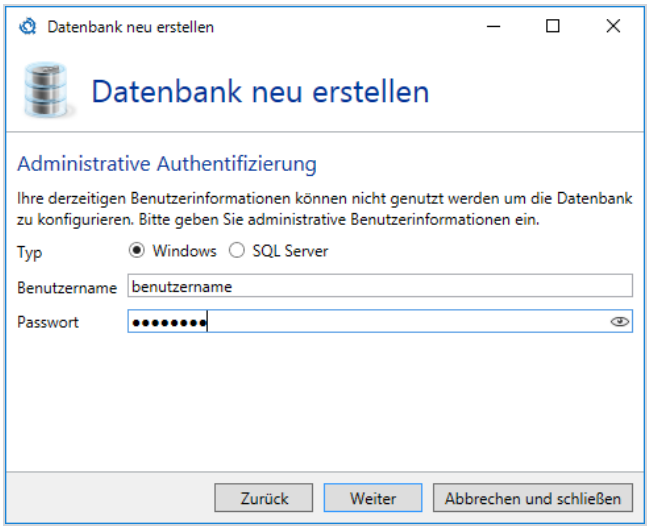
   > **HINWEIS:** Wenn es sich um die Standardinstanz des SQL-Servers handelt, wählen Sie die Option **Standard**. Anderenfalls klicken Sie **Bekannte Instanz** und tragen anschließend im Eingabefeld den Namen der entsprechenden Instanz ein.

5. Tragen Sie unter **Datenbankname** den Namen der entsprechenden Datenbank (en) ein.
   Die folgenden Datenbanknamen werden standardmäßig verwendet:

   - Gatewayrolle
     `NoSpamProxyGatewayRole`
   - Intranetrolle
     `NoSpamProxyIntranetRole`

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

6. Klicken Sie **Weiter**.
7. Geben Sie auf der Seite **Administrative Authentifizierung** an, mit welchem Benutzerkonto Änderungen an der gewählten Datenbank durchgeführt werden sollen, geben Sie die entsprechenden Anmeldeinformationen ein und kicken Sie **Weiter**.



8. Legen Sie unter **Service-Authentifizierung** fest, wie sich die Gatewayrolle beim SQL-Server anmelden soll.

> **HINWEIS:** 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.

9. Wählen Sie auf der nächsten Seite die gewünschte Aktion aus. Abhängig von den vefügbaren Datenbanken stehen hier unterschiedliche Optionen zur Verfügung.
10. Klicken Sie **Fertigstellen**.

Datenbanken sichern

Die Rollen von NoSpamProxy verwenden folgende Datenbanken:

- **Gatewayrolle** NoSpamProxyGatewayRole
- **Intranetrolle** NoSpamProxyIntranetRole
- **Web Portal** NoSpamProxyWebPortal

HINWEIS: Wenn NoSpamProxy Ihren bestehenden 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 per Skript die Datenbank sichern und bei Bedarf wiederherstellen.

Sichern der Datenbanken über die Kommandozeile

Geben Sie die folgenden Zeilen in die Kommandozeile ein:

Für die Datenbank der Gatewayrolle `osql -S (local)\NameDerInstanz-E -Q "BACKUP DATABASE NoSpamProxyGatewayRole TO DISK = 'c:\NoSpamProxyGatewayRole.bak'"` >

Für die Datenbank der Intranetrolle `osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE NoSpamProxyIntranetRole TO DISK = 'c:\NoSpamProxyIntranetRole.bak'"` >

Für die Datenbank des Web Portal `osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE NoSpamProxyWebPortal TO DISK = 'c:\NoSpamProxyWebPortal.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.

Eine Rücksicherung erstellen

Geben Sie die folgenden Zeilen in die Kommandozeile ein:

Für die Datenbank der Gatewayrolle `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyGatewayRole FROM DISK = 'c:\NoSpamProxyGatewayRole.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Für die Datenbank der Intranetrolle `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyIntranetRole FROM DISK = 'c:\NoSpamProxyIntranetRole.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Für die Datenbank des Web Portal `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyWebPortal FROM DISK = 'c:\NoSpamProxyWebPortal.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

Die Datenbanken müssen für die Wiederherstellung bereits bestehen.

HINWEIS: 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.

Datenbankberechtigungen einrichten

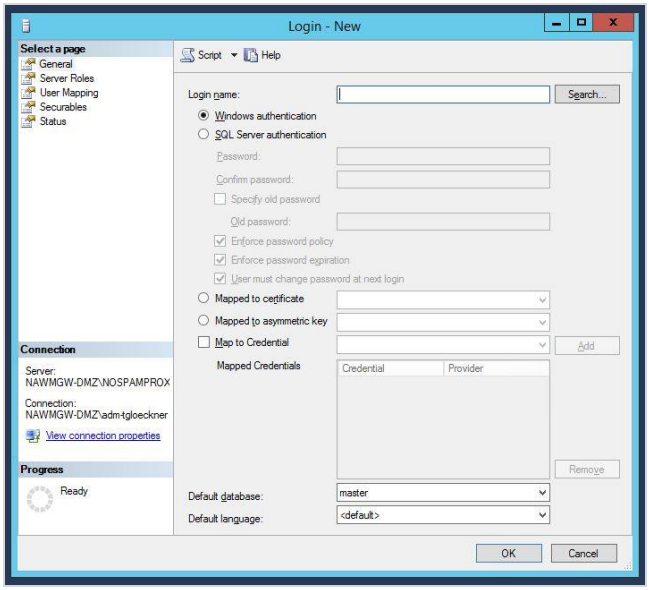
Es kommt häufiger vor, dass nicht nur der Benutzer, der ursprünglich die Installation durchgeführt hat, Updates durchführen soll, sondern auch andere Administrator-Accounts. Hierzu ist es notwendig, für diese weiteren Benutzer die entsprechenden Berechtigungen auf die Datenbanken zu einzurichten. Nachfolgend sind die entsprechenden Schritte beschrieben:

HINWEIS:

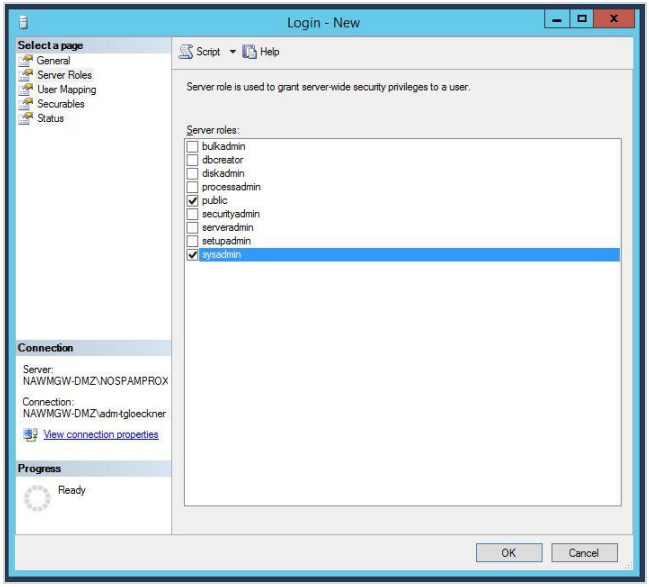
- Alle Schritte gelten für alle Rollen von NoSpamProxy; sie unterscheiden sich nur in den Datenbanknamen.
  - Datenbank Intranetrolle: NoSpamProxyIntranetRole
  - Datenbank Gatewayrolle: NoSpamProxyGatewayRole
  - Datenbank Web Portal: NoSpamProxyWebPortal
- Es können Benutzer sowie Benutzergruppen (lokal oder in der Domäne) registriert werden

1. Melden Sie sich mit dem Benutzer am System an, mit dem die Installation durchgeführt wurde.
2. Installieren Sie das SQL Management Studio.
3. Öffnen Sie das SQL Management Studio und melden Sie sich an der lokalen Instanz mit Windows-Authentifizierung an, in dem die NoSpamProxy-Datenbank(en) liegen.
4. Erweitern Sie den Ordner **Sicherheit** (“Security”) und **Anmeldungen** (“Logins”).
5. Rechtsklicken Sie den Ordner **Anmeldungen** (“Logins”).
6. Wählen Sie im Kontextmenü **Neue Anmeldung** (“New Login”).
7. Wählen Sie unter **Allgemein** den Benutzer aus, der hinzugefügt werden soll. Behalten dabei den Punkt **Windows Authentifizierung** (“Windows

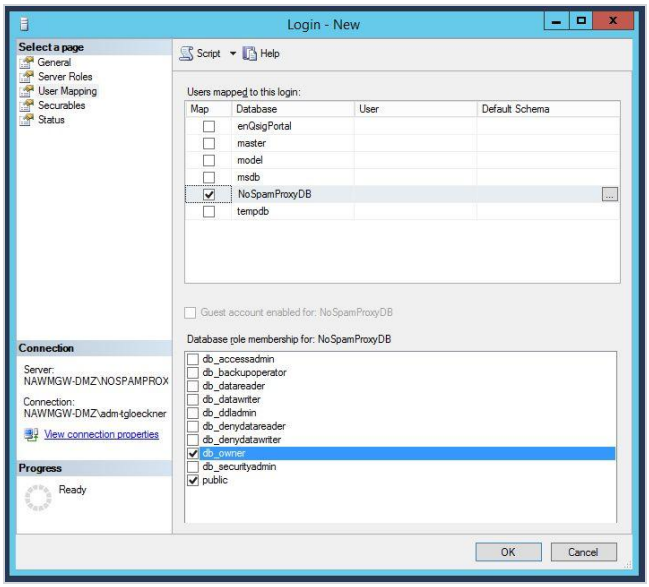
Authentication”) bei.



8. Setzen Sie unter **Serverrollen** (“Server Roles”) den Haken bei **sysadmin**.



9. Setzen Sie unter **Benutzerzuordnung** (“User Mapping”) den Haken bei der entsprechenden Datenbank. Aktivieren Sie zusätzlich die Rolle **db_owner**.



10. Nehmen Sie bei Bedarf weitere, optionale Einstellungen vor.
11. Speichern Sie den neuen Login ab und schließen Sie das SQL Management Studio.

Um den Zugriff zu verifizieren, melden Sie sich mit dem hinzugefügten Benutzer am System an, öffnen das SQL Management Studio und prüfen, ob Sie sich die Tabellen der Datenbank anschauen können. Wenn dies funktioniert, ist der Zugriff eingerichtet.

Überprüfen der Datenbankintegrität

Dieser Artikel beschreibt, wie Sie die Integrität der Datenbank überprüfen und im Fehlerfall reparieren können.

HINWEIS: Sie benötigen für diese Aktion das Microsoft SQL-Server Management Studio.

1. Öffnen Sie das Microsoft SQL-Server Management Studio.
2. Erweitern Sie den Menüpunkt **Datenbanken**.
3. Klicken Sie auf die Datenbank **NoSpamProxyGatewayRole** und anschließend links oben **Neue Abfrage**. Auf der rechten Seite erscheint nun ein weißes Fenster.
4. Um eine verdächtige Datenbank auf Fehler zu überprüfen, verwenden Sie im SQL Management Studio den folgenden Befehl:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole')
```

5. Der folgende Befehl korrigiert eventuelle Fehler:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole', REPAIR_
REBUILD)
```

> **HINWEIS:** Sie müssen vor dem Ausführen des Befehls in den Eigenschaften der Datenbank unter Optionen den Zugriffs-Modus („Restrict Access“) von MULTI_USER auf SINGLE_USER umstellen.

6. Kontrollieren Sie den Erfolg der Aktion mit folgendem Befehl:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole')
```

> **HINWEIS:** In der Ausgabe sollten jetzt keine rot geschriebenen Fehlermeldungen mehr auftauchen. Wenn die Datenbank nicht erfolgreich repariert werden konnte und weiterhin rote Fehlermeldungen auftauchen, führen Sie bitte den etwas aggressiveren Befehl **DBCC CHECKDB ('NoSpamProxyGatewayRole', REPAIR_ALLOW_DATA_LOSS)** aus. Auch danach sollten Sie wieder den Erfolg mit dem oben genannten Befehl überprüfen. Falls die Datenbank nicht repariert werden kann, können Sie auch über die NoSpamProxy-Oberfläche eine neue Datenbank erstellen. Unter Umständen liegt ein defekt am SQL Server vor.

Hinweise zur Datenbankgröße

> **HINWEIS:** Wenn Sie Microsoft SQL Server Express einsetzen und auf die Version 14 oder höher von NoSpamProxy Server updaten, darf die Auslastung der verwendeten Datenbank nicht mehr als 70 Prozent (7 GB) betragen.

Im Folgenden finden Sie einige Hinweise dazu, wie Sie auf eine entsprechende Meldung im NoSpamProxy Command Center reagieren können:

Warnstufen

In den folgenden zwei Stufen warnt Sie NoSpamProxy ab Version 13 über eine volle Datenbank

Wenn die Datenbank zu 70% gefüllt ist

- wird ein Hinweis in die Ereignisanzeige geschrieben,
- wird auf der Startseite des NoSpamProxy Command Center ein Hinweis unter “Vorfälle” angezeigt und es
- wird eine Benachrichtigung an die eingestellte Administrator-E-Mail-Adresse gesendet.

Wenn die Datenbank zu 90% gefüllt ist

- wird ein Hinweis in die Ereignisanzeige geschrieben,
- wird auf der Startseite des NoSpamProxy Command Center eine Warnung unter “Vorfälle” angezeigt und es

- wird eine Benachrichtigung an die eingestellte Administrator-E-Mail-Adresse gesendet.

Gründe für eine vollgelaufene Datenbank

Im Folgenden sind die Gründe für eine volle Datenbank aufgeführt.

- Der konfigurierte Zeitraum der Nachrichtenverfolgung und deren Details (Monitoring) ist zu groß.
- Es gibt Probleme bei der Kommunikation zwischen zwei oder mehreren NoSpamProxy-Rollen.
- Abgelaufene Daten wurden nicht ordnungsgemäß aus der Datenbank gelöscht.

Wie kann man die Datenbank analysieren?

Um herauszufinden, warum die Datenbank die jeweilige Größe erreicht hat, gehen Sie folgendermaßen vor:

1. Installieren Sie das Microsoft SQL Management Studio auf dem System, auf dem die betroffene Datenbank installiert ist. Das Microsoft SQL Management Studio ist auf der Microsoft-Website kostenlos erhältlich.
2. Starten Sie das SQL Management Studio.
3. Melden Sie sich an der SQL-Instanz an, in der die Datenbank läuft. Meist heißen diese Instanzen **(local)\SQLEXPRESS** oder **(local)\NOSPAMPROXY**.
4. Führen Sie nach erfolgreicher Anmeldung die folgenden SQL-Abfragen aus (abhängig von der betroffenen NoSpamProxy-Rolle); hierzu muss die erste Zeile immer nur auf die folgenden Datenbanken geändert werden:

- Intranetrolle: `USE [NoSpamProxyIntranetRole]`
- Gatewayrolle: `USE [NoSpamProxyGatewayRole]`
- Webportal: `USE [NoSpamProxyWebPortal]`

```
USE [NoSpamProxyIntranetRole] / USE
[NoSpamProxyIntranetRole] / USE
[NoSpamProxyWebPortal]
GO
SELECT
isnull(t.NAME, 'Total') AS TableName,
s.name as SchemaName,
p.rows AS RowCounts,
CAST(ROUND(((SUM(a.used_pages) * 8) / 1024.00),
2) AS
NUMERIC(36, 2)) AS SizeInMB
FROM
sys.tables t
INNER JOIN
sys.indexes i ON t.OBJECT_ID = i.object_id
INNER JOIN
sys.partitions p ON i.object_id = p.OBJECT_ID
AND i.index_id = p.index_id
INNER JOIN
sys.allocation_units a ON p.partition_id =
```

```
a.container_id
LEFT OUTER JOIN
sys.schemas s ON t.schema_id = s.schema_id
WHERE
t.NAME NOT LIKE 'dt%'
AND t.is_ms_shipped = 0
AND i.OBJECT_ID > 255
GROUP BY
ROLLUP(t.Name, s.Name, p.Rows)
HAVING p.rows is not null or (p.rows is null
and t.name is null)
ORDER BY
sum(a.used_pages) desc
GO
```

Wie kann man die Ergebnisse deuten und lösen?

In der Ausgabe des SQL-Skriptes ist eine Übersicht über alle existierenden Tabellen der Datenbank zu finden, sowie Informationen zu deren Größe.

	TableName	SchemaName	RowCounts	SizeInMB
1	Total	NULL	NULL	25789.40
2	UrlVisit	MessageTracking	104839460	15549.06
3	Operation	MessageTracking	4257612	6485.40
4	MessageTrackEntry	MessageTracking	1236374	935.69
5	MessageOperation	MessageTracking	4254899	581.94
6	Action	MessageTracking	5832197	538.54
7	MessageAddress	MessageTracking	2530697	473.00
8	DeliveryAttempt	MessageTracking	2272604	403.08
9	Filter	MessageTracking	3124350	389.36
10	Url	MessageTracking	866710	258.39
11	Attachment	MessageTracking	367485	58.34
12	LevelOfTrust	MessageTracking	751502	38.86
13	UserAndDomainStatistic	MessageTracking	155662	32.83
14	Certificate	CertificateStore	4759	16.75
15	Association	LargeFileTransfer	14095	7.59
16	Certificate	MessageTracking	8138	3.80

Hierbei gibt es zwei besondere Tabellen, die im Normalbetrieb leer sein sollten beziehungsweise deren Einträge sich stetig ändern sollten – und zwar bei jedem erneuten Aufruf:

- DataReplication.Artefact

PendingRequest	CertificateEnroll...	45	0.16
Artefact	DataReplication	0	0.16
Rule	Disclaimer	17	0.08

- MessageTracking.LegacyMessageTrackEntry

Mapping	AddressRewriting	54	0.08
LegacyMessageTrack...	MessageTracking	0	0.05
Key	Dkim	2	0.03

Wenn sich in diesen Tabellen Daten ansammeln, aber nicht abbauen, deutet dies auf Probleme hin. Diese müssen durch den NoSpamProxy-Support geklärt und gelöst werden. Wenden Sie sich in diesem Fall bitte an den für Sie zuständigen Partner oder – falls Sie Hersteller-Support erworben haben – direkt an den NoSpamProxy-Support.

Alle anderen Szenarien deuten auf einen zu großen Speicher-Zeitraum für die Nachrichtenverfolgung hin, welchen Sie im NoSpamProxy Command Center unter **Konfiguration > Erweiterte Einstellungen > Monitoring** bearbeiten und reduzieren können. Die Reduzierung dauert in der Regel bis zu 24 Stunden, so dass ein Ergebnis meist erst am nächsten Tag zu sehen ist.

Datenbanken sichern

Die Rollen von NoSpamProxy verwenden folgende Datenbanken:

- **Gatewayrolle** NoSpamProxyGatewayRole
- **Intranetrolle** NoSpamProxyIntranetRole
- **Web Portal** NoSpamProxyWebPortal

HINWEIS: Wenn NoSpamProxy Ihren bestehenden 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 per Skript die Datenbank sichern und bei Bedarf wiederherstellen.

Sichern der Datenbanken über die Kommandozeile

Geben Sie die folgenden Zeilen in die Kommandozeile ein:

- Für die Datenbank der Gatewayrolle

```
osql -S (local)\NameDerInstanz-E -Q "BACKUP DATABASE
NoSpamProxyGatewayRole TO DISK =
'c:\NoSpamProxyGatewayRole.bak'" >
```

- Für die Datenbank der Intranetrolle

```
osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE
NoSpamProxyIntranetRole TO DISK =
'c:\NoSpamProxyIntranetRole.bak'" >
```

- Für die Datenbank des Web Portal

```
osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE
NoSpamProxyWebPortal TO DISK =
'c:\NoSpamProxyWebPortal.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.

Eine Rücksicherung erstellen

Geben Sie die folgenden Zeilen in die Kommandozeile ein:

- Für die Datenbank der Gatewayrolle

```
osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE
NoSpamProxyGatewayRole FROM DISK =
'c:\NoSpamProxyGatewayRole.bak' WITH FILE= 1,
NOUNLOAD, REPLACE "
```

- Für die Datenbank der Intranetrolle

```
osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE
NoSpamProxyIntranetRole FROM DISK =
'c:\NoSpamProxyIntranetRole.bak' WITH FILE= 1,
NOUNLOAD, REPLACE "
```

- Für die Datenbank des Web Portals

```
osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE
NoSpamProxyWebPortal FROM DISK =
'c:\NoSpamProxyWebPortal.bak' WITH FILE= 1, NOUNLOAD,
REPLACE "
```

Die Datenbanken müssen für die Wiederherstellung bereits bestehen.

> **HINWEIS:** 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.

Eine Encryption Dump erstellen

Sie können NoSpamProxy so konfigurieren, dass es entschlüsselte Daten in einer Datei speichert, bevor diese Daten in einer E-Mail weiterverarbeitet werden. Dies kann bei der Analyse von Formatierungsproblemen im Zusammenhang mit der Ver- und Entschlüsselung sehr hilfreich sein.

Um die Encryption-Dump zu erstellen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **C:\ProgramData\Net at Work Mail Gateway\Configuration**.
2. Öffnen Sie die Datei **Gateway Role.config**.
3. Suchen Sie die folgende Zeile:
   `</configSections>`
4. Fügen Sie unterhalb der eben genannten Zeile die folgenden Zeilen hinzu:

```
<netatwork.nospamproxy.cryptography>
<debugging dumpDecryptedContentToDisk="true"/>
</netatwork.nospamproxy.cryptography>
```

> **HINWEIS:** Falls der Abschnitt `netatwork.nospamproxy.cryptography` schon vorhanden ist, fügen Sie nur die Zeile `<debugging dumpDecryptedContentToDisk="true"/>` hinzu.

> **HINWEIS:** Bevor Sie die Konfigurationsdatei abspeichern, müssen Sie den Gatewayrollen-Dienst beenden. Erst dann können Sie die Konfigurationsdatei ordnungsgemäß abspeichern.

> **HINWEIS:** Die entschlüsselten Inhalte werden nun im Temp-Ordner des lokalen Dienstes abgespeichert. Üblicherweise ist dies der Ordner **C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp**. Falls die Dateien dort nicht erstellt werden, prüfen Sie bitte den Ordner **C:\Windows\Temp**.

Eine Memory Dump erstellen

Dieser Artikel beschreibt, wie Sie auf einem Windows 2008 Server R2 oder höher eine Memory Dump für den NoSpamProxy-Support erstellen.

1. Öffnen Sie auf dem entsprechenden Server den Task Manager.
2. Wechseln Sie zur Registerkarte **Details** und sortieren Sie die Einträge nach Namen.
3. Rechtsklicken Sie den entsprechenden Prozess und wählen Sie **Create dump file**.

Die Memory Dump schicken Sie dann bitte an den NoSpamProxy Support unter **support@nospamproxy.de**.

Statische Domänenvertrauensstellungen exportieren

Um die statischen Einträge aus den Vertrauensstellungen auszulesen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das SQL Management Studio (Express) für die Verwaltung Ihrer NoSpamProxy-Datenbank.
2. Verbinden Sie sich mit dem Datenbank-Server auf dem die NoSpamProxyGatewayRole-Datenbank liegt.
3. Klicken Sie **Neue Abfrage / New query**, um eine neue SQL-Abfrage für die NoSpamProxyGatewayRole zu erstellen.
4. Fügen sie diese Abfrage in den Abfrage- oder Query-Editor ein:

```
USE NoSpamProxyGatewayRole;
SELECT Domain, Gravity, LevelOfTrust
FROM DomainTrustEntry
WHERE (Gravity = 0);
```

5. Führen Sie die Abfrage aus, in dem Sie beispielsweise auf das rote Ausrufezeichen klicken.

Mit dieser Abfrage werden Ihnen alle statischen Einträge im Domain Trust aufgelistet. Falls Sie ein Programm für den Import in die Version 7.6 benötigen,

oder es beim Ausführen dieser Befehle Probleme gibt, melden Sie sich bitte bei mir. Mit dieser Abfrage können Sie den Einsatz unseres Mail Gateway API Samples für das Auslesen der Domain Trusts umgehen.

HINWEIS: Bei einer Neuinstallation werden die statischen Domain-Trust-Einstellungen für bekannte E-Mail-Provider automatisch vom Setup eingetragen.

Ändern des Web Ports

Der Web Port ist der Port, mit dem sich das NoSpamProxy Command Center beim Zugriff auf die einzelnen Rollen verbindet. Des Weiteren unterhalten sich die Rollen über den konfigurierten Port und zählen 1 hinzu. Wird der WebPort auf 6060 konfiguriert, verbinden sich die Dienste über 6061.

WARNUNG: Diesen Port sollten Sie nur ändern, wenn es unbedingt nötig ist. Lesen in jedem Fall den gesamten hier vorliegenden Artikel.

Um den WebPort zu ändern, gehen Sie folgendermaßen vor:

1. Stoppen Sie alle NoSpamProxy-Dienste.
2. Gehen Sie zu **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

   HINWEIS: Falls Sie auch das Webportal einsetzen, gehen Sie zu **%Program Files%\Net at Work Mail Gateway\enQsig Webportal\App_Data**.

3. Suchen Sie die beiden Konfigurationsdateien **intranet role.config** und **gateway role.config**. In diesen Dateien nehmen Sie die entsprechenden Einstellungen vor.
4. Suchen Sie nach der Zeile, die mit folgenden Zeichen beginnt: `<netatwork.nospamproxy.webservices`
5. Fügen Sie dort das folgende Attribut hinzu:

```
port="NeuerPortwert"
```

> **HINWEIS:** Das Attribut `serverCertificateThumbprint` unterscheidet sich auf jedem NoSpamProxy-Server.

6. Ändern Sie über netssh die URL-Reservierung. Nutzen Sie dafür **HTTPSYSMANAGER** von **http://httpsysmanager.codeplex.com/**. Alternativ geben Sie folgenden Befehl über die Kommandozeile ein:

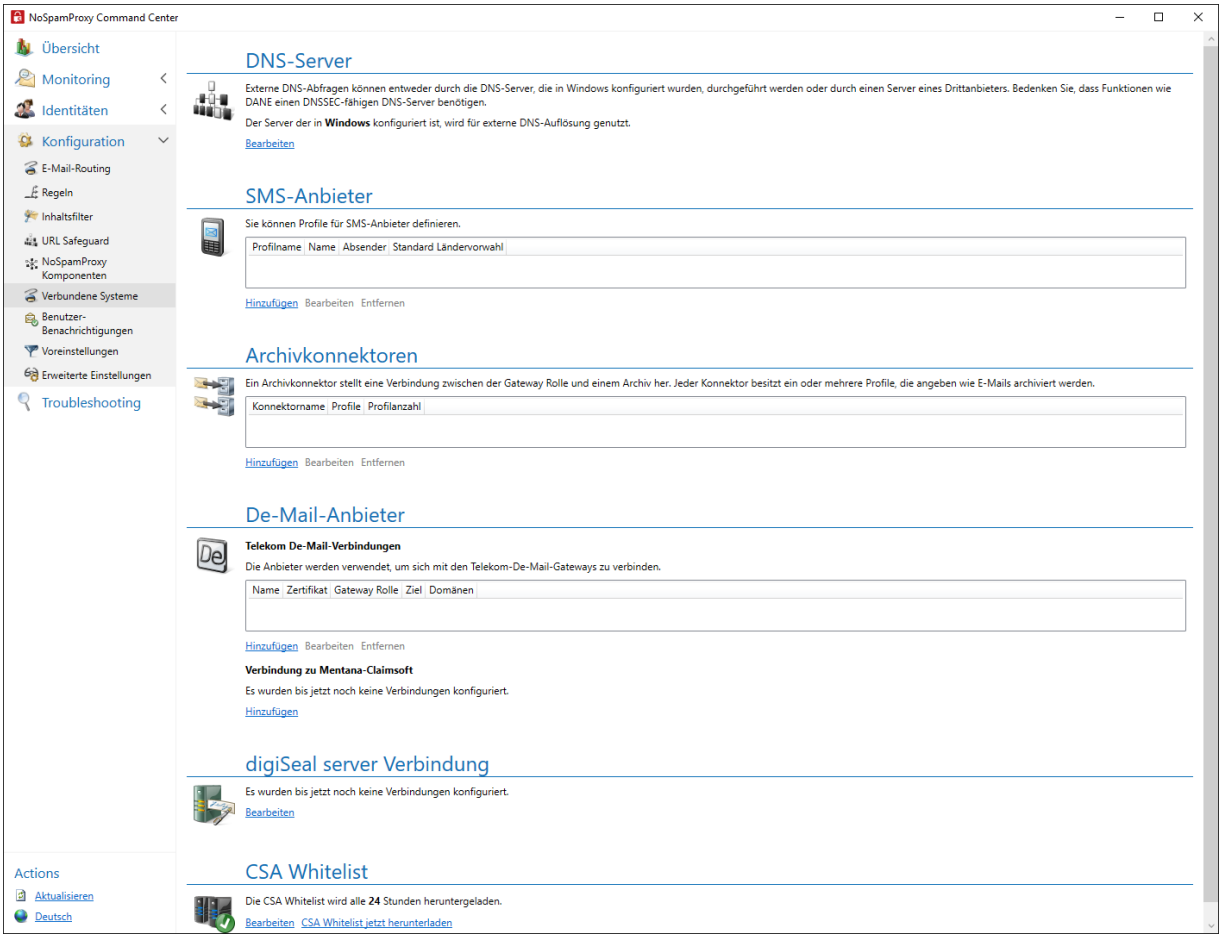
```
netsh http add urlacl url=http://+:8060/NoSpamProxy/
sddl=D:(A;;GX;;;LS)(A;;GX;;;NS)
```

7. Starten Sie jetzt alle Dienste neu.
8. Rechtsklicken Sie im NoSpamProxy Command Center **NoSpamProxy** und klicken Sie dann **Server ändern**.
9. Passen Sie in diesem Dialog den Port an.

10. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten** und erstellen Sie die Rollenverbindungen neu.

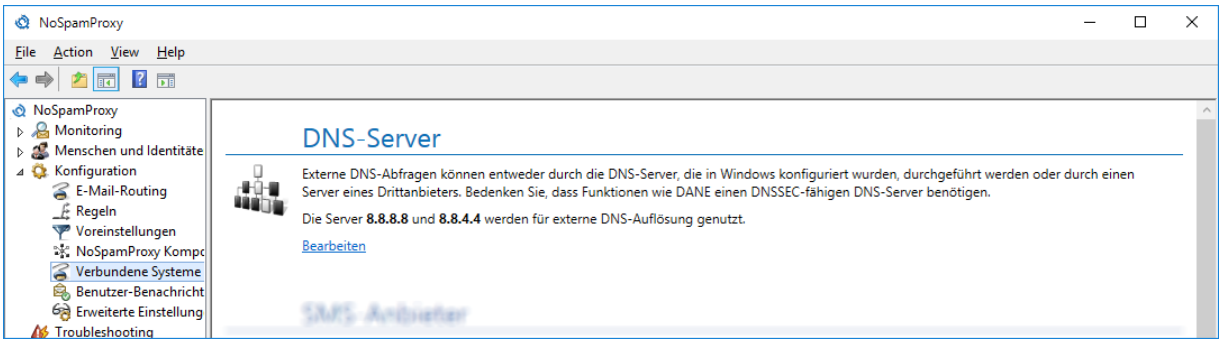
Verbundene Systeme

Hier verwalten Sie Verbindungen zu Drittanbieterprodukten, die mit NoSpamProxy interagieren.



DNS-Server

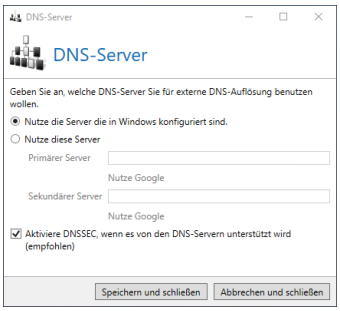
Beim Einsatz von DANE benötigen Sie einen DNS-Server, der DNSSEC unterstützt. Da die in Windows-Server-Betriebssystemen mitgelieferten DNS-Server diese Funktion derzeit nicht unterstützen, können Sie hier eine Verbindung zu einem solchen Server einrichten.



DNS-Server konfigurieren

Um die IP-Adressen eines primären und sekundären Servers mit DNSSEC-Unterstützung einzutragen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > DNS-Server**.
2. Klicken Sie **Bearbeiten**.



3. Führen Sie eine der beiden folgenden Schritte durch:
   - Wählen Sie **Nutze die Server, die in Windows konfiguriert sind**, wenn Sie Windows-eigene Server nutzen wollen.
   - Wählen **Nutze diese Server**, wenn Sie den Server eines Drittanbieters nutzen wollen. Geben Sie dann die entsprechenden Adressen ein.

> **TIPP:** Klicken Sie **Nutze Google**, um den öffentlich erreichbaren DNS-Server von Google in die Konfiguration eintragen zu lassen.

4. Wählen Sie, ob Sie **DNSSEC** aktivieren wollen (empfohlen).

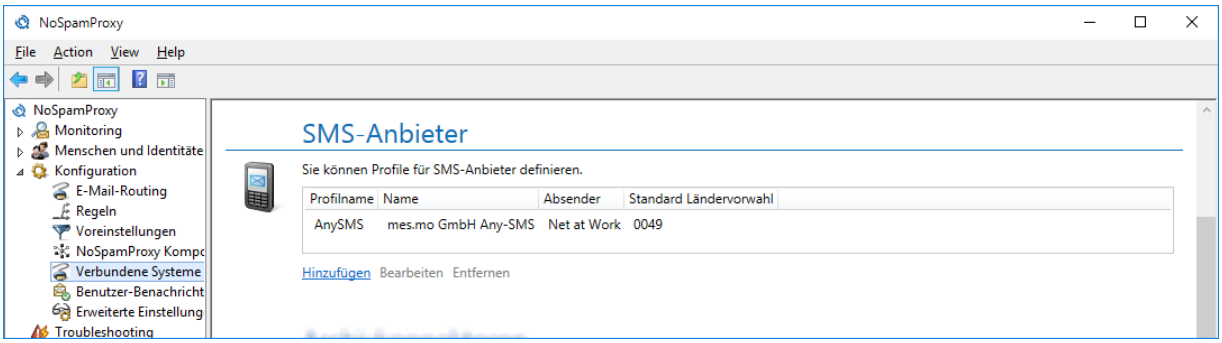
> **HINWEIS:** DNSSEC sichert die Übertragung von Resource Records durch digitale Signaturen ab. So wird die Authentizität dieser Resource Records sichergestellt.

5. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** DANE wird für die Überprüfung der Transportverschlüsselung bei der Zustellung von E-Mails zu Ihren Partnern verwendet. Siehe **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, müssen Sie mindestens ein Profi konfigurieren.



Unterstützte SMS-Anbieter

Derzeit werden folgende Anbieter unterstützt:

- mes.mo GmbH Any-SMS - **http://www.any-sms.de**
- tyntec - **http://www.tyntec.com**
- CM Telecom - **http://www.cmtelecom.com**

SMS-Anbieter konfigurieren

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > SMS-Anbieter**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie den gewünschten SMS-Anbieter aus und klicken Sie **Weiter**.

> **HINWEIS:** Es werden nun technische Details zum gewählten Provider angezeigt. In der Regel brauchen Sie diese Einstellungen nicht zu ändern. Klicken Sie ansonsten **Eigenschaften bearbeiten** und nehmen Sie die gewünschten Änderungen vor.

4. Klicken Sie **Weiter**.

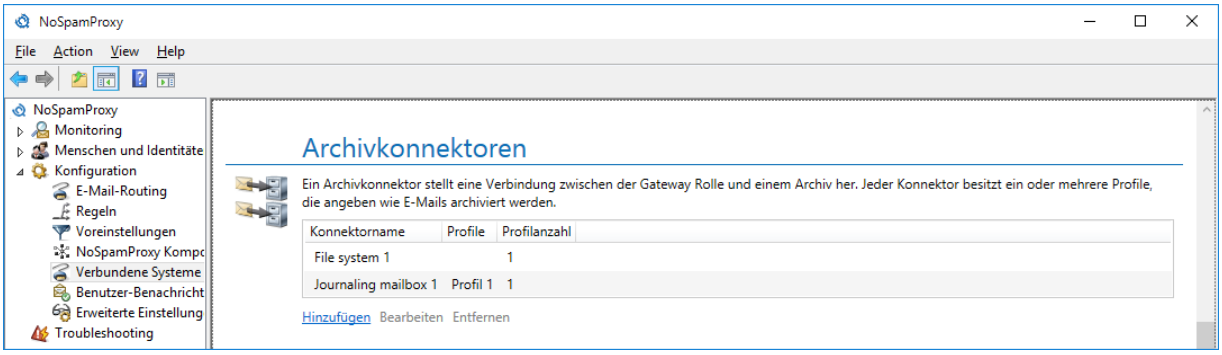
5. Geben Sie einen Namen für das Profil an, legen Sie den Absender fest und geben Sie eine Standard Landesvorwahl an.

   > **HINWEIS:** Sie können entweder die Telefonnummer eines Mobiltelefons angeben oder eine alphanumerische Zeichenkette mit einer maximalen Länge von 11 Zeichen, z.B. den Namen Ihrer Firma. Die Landesvorwahl wird verwendet, wenn beim Versenden eine Telefonnummer ohne Landesvorwahl verwendet wurde.

6. Klicken Sie **Weiter**.
7. Geben Sie die Zugangsdaten ein, die Sie von dem gewählten Anbieter bekommen haben.
8. Klicken Sie **Fertigstellen**.

Archivkonnektoren

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



Die Konfiguration eines Archivkonnektors umfasst zwei Bereiche:

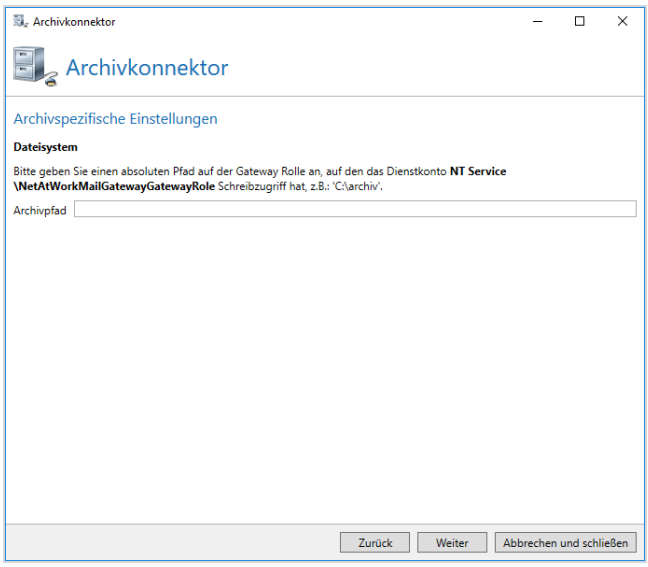
Archivkonnektoren| Konnektoren definieren die Schnittstelle zu einem externen Archivsystem wie beispielsweise dem Dateisystem.

Profile| Innerhalb eines Konnektors werden ein oder mehrere Profile erstellt. Darin können Eigenschaften wie beispielsweise der genaue Speicherort für E-Mails und Dokumente festgelegt werden. Außerdem wird hier gegebenenfalls eine Zuordnung von Metadaten von E-Mails auf Metadaten des Archivsystems durchgeführt.

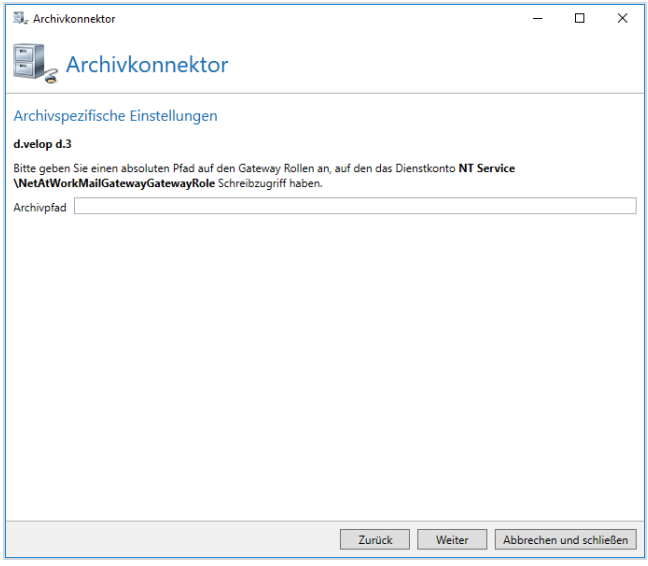
HINWEIS: E-Mails werden so archiviert, wie sie von NoSpamProxy empfangen werden. NoSpamProxy nimmt weder eine Ver- oder Entschlüsselung vor noch lädt NoSpamProxy Anhänge in das Webportal. Beachten Sie, dass E-Mails nur dann archiviert werden, wenn NoSpamProxy die E-Mail nicht ablehnt. Schlägt beispielsweise der Malwarescanner an oder kann die E-Mail nicht entschlüsselt werden, so wird die jeweilige E-Mail nicht archiviert.

Archivkonnektoren konfigurieren

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > Archivkonnektoren**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie das Archivsystem aus und geben Sie dem Konnektor einen Namen.
4. Nehmen sie die entsprechende Konfiguration für das gewählte Archivsystem vor und klicken Sie **Weiter**.
    - Bei einer Ablage von E-Mails und Dokumenten im Dateisystem müssen Sie nur einen Pfad angeben. E-Mails und Dokumente werden in Ordnern unterhalb dieses Pfades abgespeichert.



- 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 müssen Sie lediglich einen Pfad angeben. E-Mails und Dokumente werden in dieses Verzeichnis geschrieben und von dort durch das d.velop d.3-System abgeholt.



5. (Optional) Legen Sie Profile für den Konnektor an.

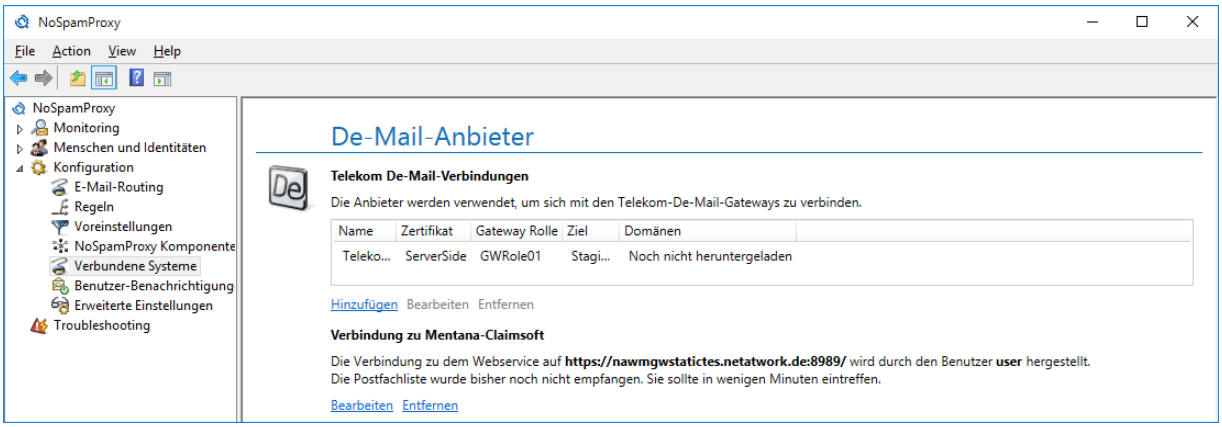
> **HINWEIS:** Der Inhalt der Seite für die Profilkonfiguration hängt vom gewählten Archivsystem ab.

> **HINWEIS:** Profile ermöglichen es Ihnen zum Beispiel, E-Mails und Dokumente innerhalb eines Archivsystems auf verschiedene Ordner zu verteilen. Geben Sie dem neuen Profil einen Namen und Sie aus, welche E-Mails durch dieses Profil archiviert werden. Beachten Sie, dass E-Mails mit einem qualifiziert signierten Anhang immer archiviert werden. Sie können optional auch alle anderen E-Mails archivieren.

6. Klicken Sie **Fertigstellen**.

De-Mail-Anbieter

Hier können Sie die Verbindungen zum De-Mail-System hinterlegen.



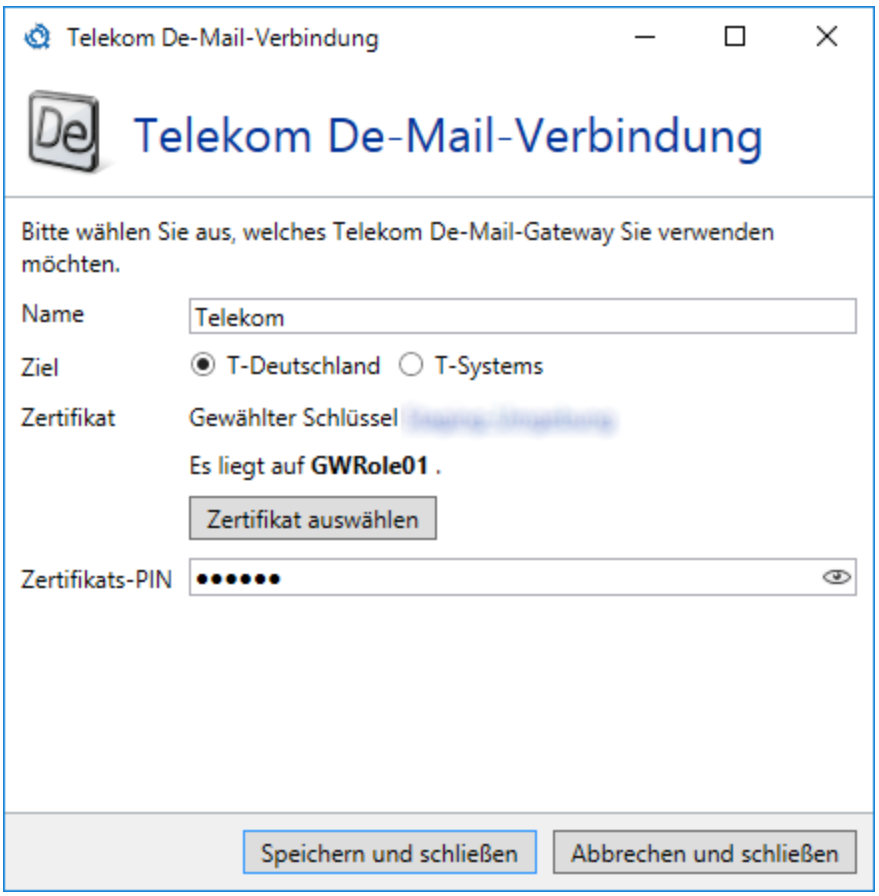
> **HINWEIS:** Die in diesem Abschnitt eingegebenen Informationen sind sowohl für die De-Mail-Sendekonnektoren als auch für die Empfangskonnektoren sofort verfügbar. Das heißt, dass Sie die Verbindung nur einmal konfigurieren müssen und sie Ihnen sofort in allen Konnektoren bereitsteht.

Telekom De-Mail-Verbindungen

Um Konnektoren für De-Mail über die Telekom zu erstellen, müssen zunächst die Verbindungen zum Diensteanbieter konfiguriert werden.

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > De-Mail-Anbieter**.
2. Klicken Sie unter **Telekom De-Mail-Verbindungen** auf **Hinzufügen**.



3. Geben Sie den Namen des Profils ein und wählen Sie, ob Sie die Verbindung über T-Deutschland oder T-Systems herstellen.
4. Wählen Sie das Zertifikat aus, das für die Absicherung der Verbindung zum Diensteanbieter verwendet wird.
5. Geben Sie die Zertifikat-PIN (Smartcard-PIN) ein.
6. Klicken Sie **Speichern und schließen**.

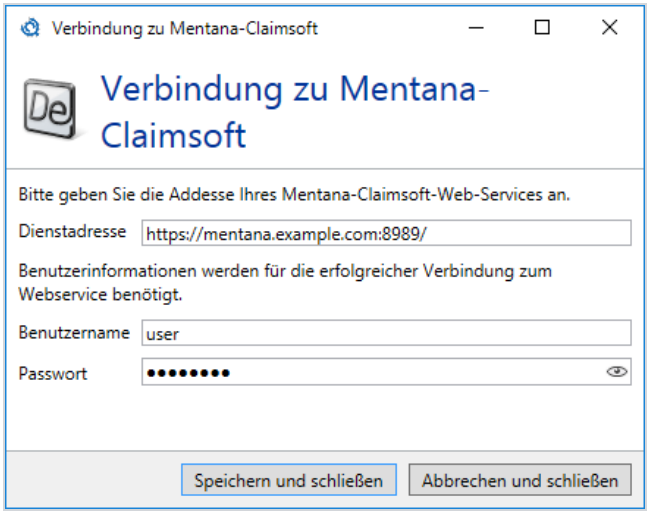
> **HINWEIS:** Durch die Auswahl des Zertifikats ergibt sich automatisch die Bindung des Profils an eine Gatewayrolle. Konnektoren, die das Profil verwenden, werden automatisch der Gatewayrolle zugeordnet, auf der das Zertifikat liegt.

Verbindung zu Mentana-Claimsoft

Für die De-Mail-Konnektoren von Mentana-Claimsoft müssen Sie eine Verbindung zu dem Webservice dieses Anbieters einrichten.

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > De-Mail-Anbieter**.
2. Klicken Sie unter **Verbindung zu Mentana-Claimsoft** auf **Hinzufügen**.

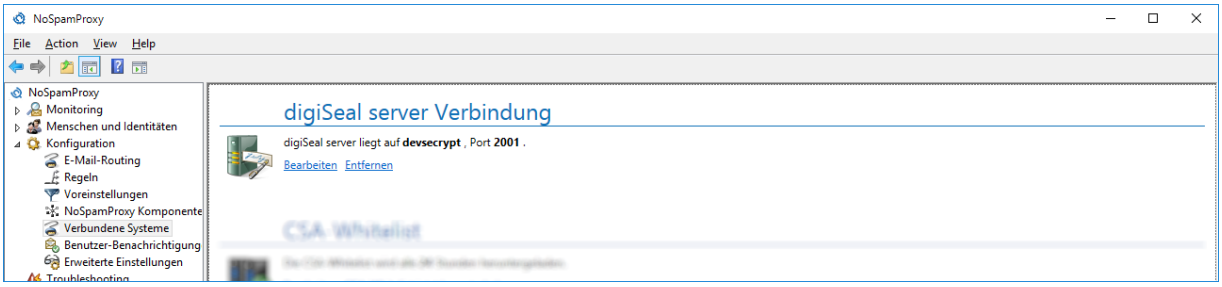


3. Geben Sie die Dienstadresse ein, unter der der Webservice erreicht werden kann.
4. Geben Sie die Anmeldeinformationen für den Zugriff auf den Dienst ein.
5. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** 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.

digiSeal-server-Verbindung

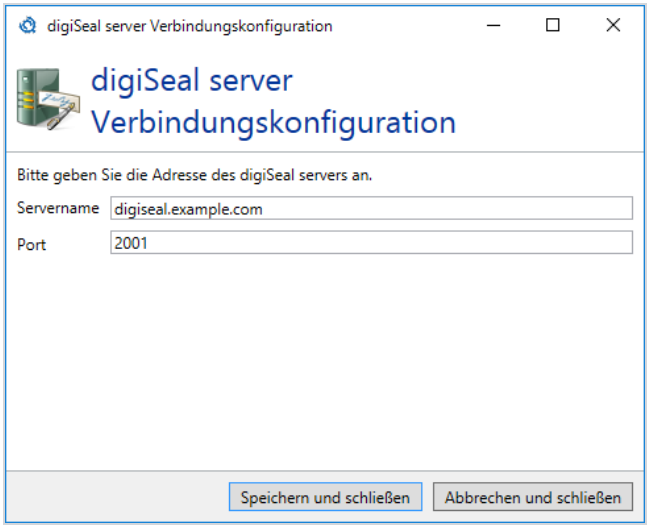
Bei der Nutzung der digiSeal-server-Dienste für die qualifizierte Dokumentensignatur benötigt NoSpamProxy Encryption die Verbindungsinformationen zu diesem Server.



digiSeal server Verbindung konfigurieren

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > digiSeal server Verbindung**.

2. Klicken Sie **Bearbeiten**.



3. Geben Sie die folgenden Informationen an:

   Servername| Der Name des Zielsystems.

   Port| Der Netzwerk-Port, unter dem die digiSeal server Dienste erreichbar sind.

4. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** Um die Anbindung an den digiSeal server vollständig durchzuführen, beachten Sie bitte die Hinweise unter **Anbindung an digiSeal server**.

CSA Certified IP List

Um den Filter CSA Certified IP List zu verwenden, müssen Sie den Download der Liste konfigurieren.

CSA Certified IP List konfigurieren

1. Gehen Sie zu **Konfiguration > Verbundene Systeme > CSA Certified IP List**.
2. Klicken Sie **Bearbeiten**.
3. Wählen Sie **Tägliches herunterladen der CSA Certified IP List einschalten**, wenn Sie **CSA Certified IP List** verwenden wollen.

   > **HINWEIS:** Wenn Sie CSA Certified IP List nicht verwenden wollen, wählen Sie **Herunterladen abschalten**.

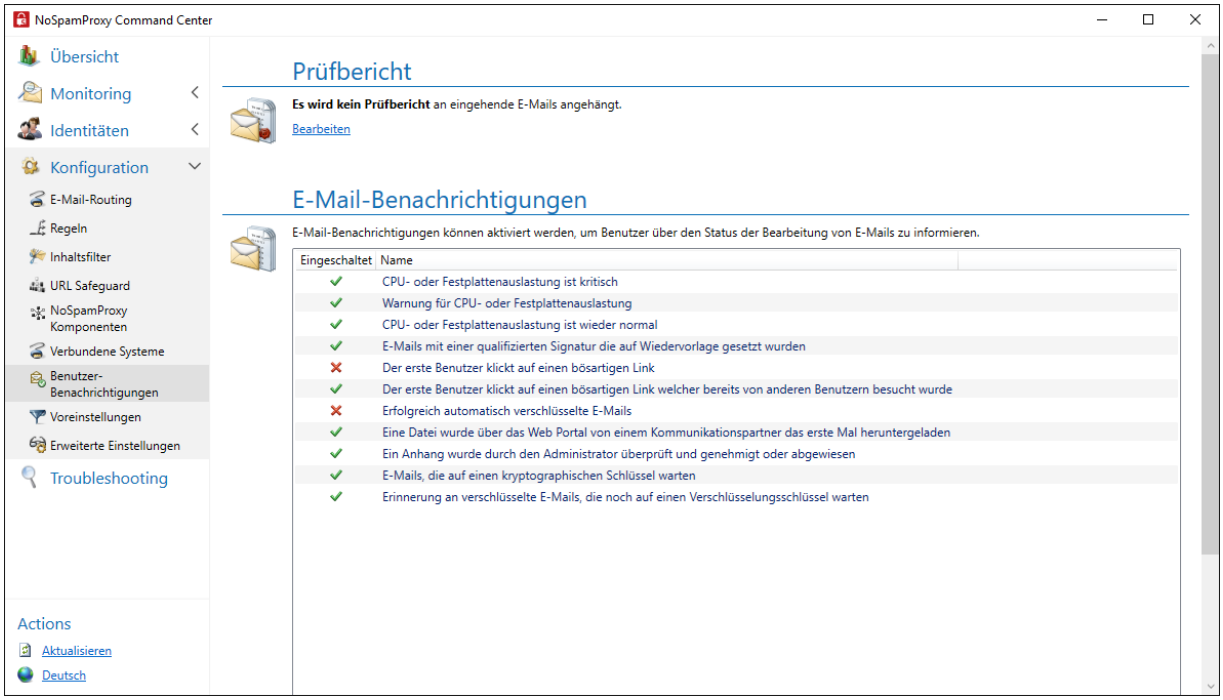
4. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** Um die CSA Certified IP List manuell herunterzuladen, klicken Sie **CSA Certified IP List jetzt herunterladen** unter **Konfiguration > Verbundene Systeme > CSA Certified IP List**.

> **HINWEIS:** Die CSA Certified IP List wird von der Domäne `service.nospamproxy.de` heruntergeladen. Damit NoSpamProxy diese Liste laden kann, ist Zugriff auf diese Adresse notwendig. Stellen Sie sicher, dass die Einstellungen Ihrer Firewall dies erlauben.

Benutzerbenachrichtigungen

Hier legen Sie fest, welche Nachrichten NoSpamProxy an interne und externe Kontakte versendet und welche Absenderadressen verwendet werden.



Prüfbericht

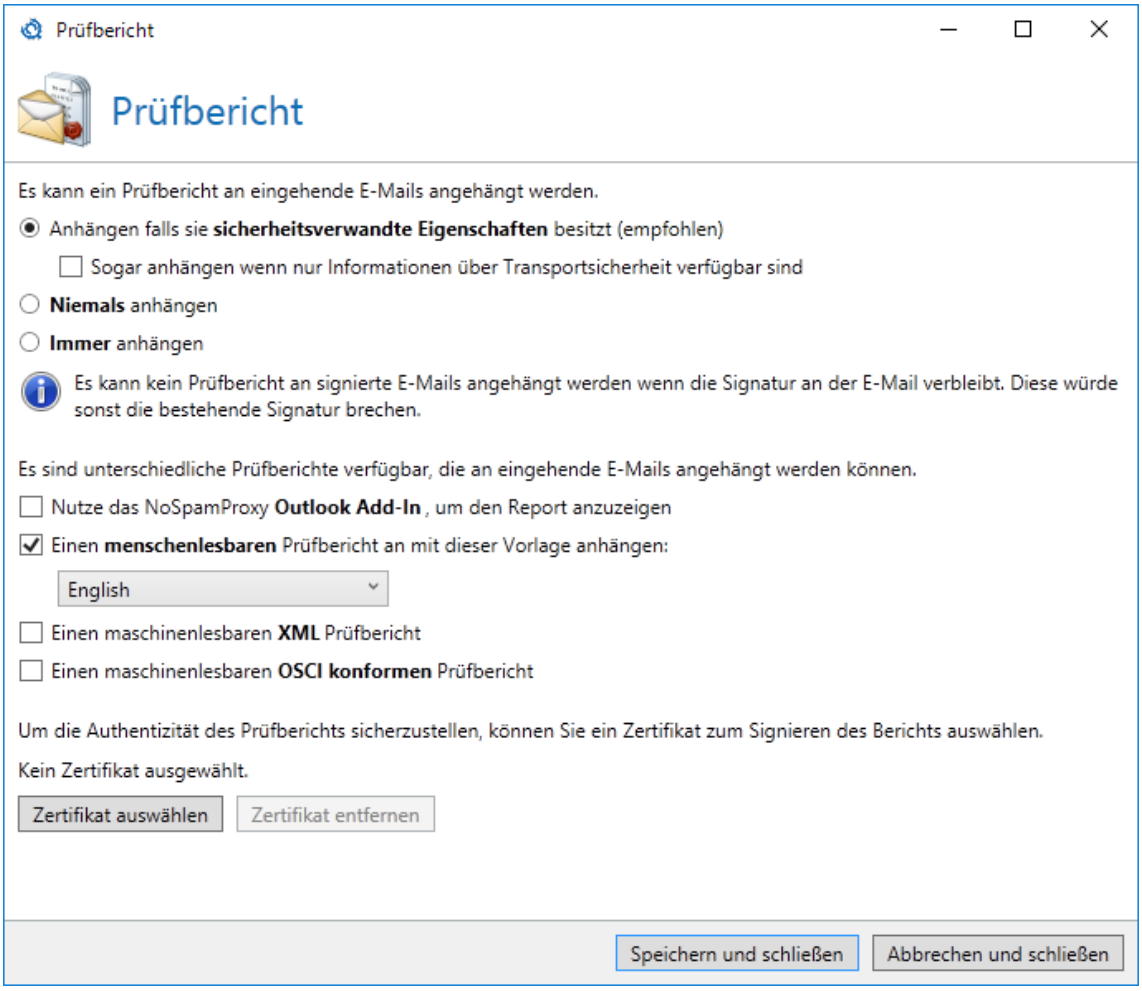
> Dieser Bereich ist verfügbar, wenn Sie die entsprechende Lizenz erworben haben.

Der Prüfbericht enthält Informationen über sicherheitsrelevante Eigenschaften und Vorgänge bei der E-Mail-Verarbeitung. Er kann an E-Mails an lokale Adressen angehängt werden. Die aktuell eingestellten Werte werden unter **Prüfbericht** angezeigt.

HINWEIS: Es kann kein Prüfbericht an signierte E-Mails angehängt werden, wenn die Signatur an der E-Mail verbleibt. Diese Signatur würde ansonsten die bestehende Signatur brechen. Um das Entfernen von Signaturen zu konfigurieren, beachten Sie die Informationen unter **S/MIME- und PGP-Überprüfung sowie Entschlüsselung**.

Prüfbericht konfigurieren

1. Gehen Sie zu Konfiguration > Benutzerbenachrichtigungen > Prüfbericht.
2. Klicken Sie Bearbeiten.



3. Wählen Sie, an welche E-Mails der Bericht angehängt werden soll.
4. Wählen Sie die Art des Prüfberichts.
   - **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 NoSpam Proxy angezeigt werden.

> Wir empfehlen die Verwendung dieses Prüfberichts, da bei allen anderen Arten des Prüfberichts ein Anhang an die jeweilige E-Mail angehängt wird.

- **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 Gatewayrolle und haben die Erweiterung `HtmlProcessCardTemplate`. Falls Sie die Vorlagen anpassen wollen, ändern Sie 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.

5. (Optional) Wählen Sie ein privates E-Mail-Zertifikat aus.

> **HINWEIS:** Sie können den Prüfbericht digital signieren, um die Authentizität sicher zu stellen. Diese Signatur ist für den OSCI-Laufzettel zwingend erforderlich, für alle anderen Prüfberichte ist sie optional.

6. Klicken Sie **Speichern und schließen**.

> **HINWEIS:** Um das Erstellen des Prüfberichts regelbasiert zu unterdrücken, beachten Sie die Informationen unter **Schritte beim Erstellen**.

E-Mail-Benachrichtigungen

Hier konfigurieren Sie die Benachrichtigungen zum Status der E-Mail-Bearbeitung.

1. Gehen Sie zu **Konfiguration > Benutzerbenachrichtigungen > E-Mail-Benachrichtigungen**.
2. Markieren Sie eine oder mehrere Benachrichtigungen.
3. Klicken Sie **Markierte aktivieren/Markierte deaktivieren**, um die jeweiligen Benachrichtigungen ein- oder auszuschalten.

Benutzerbenachrichtigungen anpassen

Diese Änderungen müssen Sie nur auf der Intranetrolle vornehmen. Die Inhalte werden automatisch auf alle angeschlossenen Gatewayrollen repliziert.

HINWEIS: Die entsprechenden CSHTML-Dateien liegen im Verzeichnis %Program Files%\Net at Work Mail Gateway\Intranet Role\Templates, oder bei Neuinstallationen mit Version 10 im Verzeichnis %Program Files%\NoSpamProxy\Intranet Role\Templates.

HINWEIS: Sie benötigen zumindest rudimentäre HTML-Kenntnisse, um die Anpassungen durchführen zu können.

Übersicht der verfügbaren Template-Dateien

ApplySymmetricEncryptionPasswordNotice.cshtml

Wenn ein Benutzer eine E-Mail als PDF-Mail verschickt, bekommt er eine Benachrichtigung über das verwendete Passwort, oder eine Info, dass dem Empfänger das Passwort per SMS zugeschickt wurde oder dass die Erstellung der PDF-Mail fehlgeschlagen ist. Der Text der Benachrichtung steht in dieser Datei. Das Aussehen wird über das CommonMailTemplate festgelegt.

AttachmentManager.cshtml

Wenn NoSpamProxy einen Dateianhang von einer E-Mail entfernt, wird eine Ersatzdatei an die E-Mail gehängt, um den Benutzer auf die Entfernung der Originaldatei hinzuweisen. Der entsprechende Hinweistext kann in der Attachment Manager.cshtml Datei editiert werden.

AttachmentQuarantine.cshtml

Wenn NoSpamProxy einen Dateianhang von einer E-Mail entfernt und in Quarantäne legt, wird eine Ersatzdatei an die E-Mail gehängt, um den Benutzer auf die Entfernung der Originaldatei hinzuweisen. Der Benutzer hat die Möglichkeit, die entfernte Datei direkt über einen Downloadlink aus der Quaratäne herunterzuladen. Der entsprechende Hinweistext kann in der Attachment Quarantine.cshtml Datei editiert werden.

AttachmentQuarantineApproval.cshtml

Wenn NoSpamProxy einen Dateianhang von einer E-Mail entfernt und in Quarantäne legt, wird eine Ersatzdatei an die E-Mail gehängt, um den Benutzer auf die Entfernung der Originaldatei hinzuweisen. Der Benutzer hat die Möglichkeit, die entfernte Datei nach Freigabe durch den Administrator über einen Downloadlink aus der Quaratäne herunterzuladen. Der entsprechende Hinweistext kann in der Attachment QuarantineApproval.cshtml Datei editiert werden.

CommonMailTemplate.cshtml

In dieser Datei wird das generelle Aussehen von Benachrichtigungen festgelegt. Hier werden zum Beispiel die Farben und die zu verwendenden Logos als HTML-Tag hinterlegt. Alle anderen Dateien außer der “ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml” enhalten nur die Textbausteine.

ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml

Das Aussehen der PDF-Datei wird in dieser Datei festgelegt. Hier müssen erneut Farben und Logos definiert werden.

ConvertMailContentToPdfAttachmentActionTeaser.cshtml

In dieser Datei steht der Text für die Träger-Mail der PDF-Datei. Der Empfänger einer PDF-Mail wird darüber informiert, dass der eigentliche Inhalt der E-Mail im angehängten PDF-Dokument steht. Das Aussehen wird über das CommonMailTemplate festgelegt.

DeliveryNotificationReport.cshtml

Hier steht der Inhalt des Sendeberichts, wenn ein Benutzer diesen in Outlook angefordert hat. Das Aussehen wird über das CommonMailTemplate festgelegt.

DeMailConnectorIssueEscalationMail.cshtml

Wenn NoSpamProxy über einen gewissen Zeitraum keine De-Mails vom DMDA herunterladen kann, wird eine Benachrichtung an die administrative E-Mail-Adresse geschickt. Der Inhalt dieser Benachrichtung kann hier editiert werden.

Deutsch.HtmlProcessCardTemplate

Der Inhalt des deutschen Prüfberichts, kann in dieser Datei editiert werden. Prüfberichte werden auf Wunsch des Administrator erzeugt, wenn eine E-Mail beispielswese signiert und / oder verschlüsselt war.

EncryptedMailNotificationTemplate.cshtml

Wenn ein Benuzter eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig verfügt über keinen kryptografischen Schlüssel, wird der Empfänger darüber informiert. In dieser Info-Mail steht, welche Optionen er hat. Der Inhalt dieser E-Mail wird in dieser Vorlage festgehalten. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionDelayedNotificationForSender.cshtml

Wenn ein Benuzter eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig hat keinen kryptografischen Schlüssel, wird der Absender über die Verzögerung informiert. Der Inhalt der Verzögerungsnachricht wird hier festgelegt. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionFailureNotificationForSender.cshtml

Wenn ein Benuzter eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und es tritt ein Fehler bei der Verschlüsselung auf, wird der Absender darüber informiert. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionSucceededNotificationForSender.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet, bekommt er eine Benachrichtigung, sobald die E-Mail verschlüsselt wurde. Das Aussehen wird über das CommonMailTemplate festgelegt.

English.HtmlProcessCardTemplate

Der Inhalt des englischen Prüfberichts, kann in dieser Datei editiert werden. Prüfberichte werden auf Wunsch des Administrator erzeugt, wenn eine E-Mail beispielswese signiert und / oder verschlüsselt war.

LargeFileDownloadNotification.cshtml

Wenn ein Benutzer eine Datei über Large Files verschickt, bekommt er eine Benachrichtigung, sobald der Empfänger die Datei heruntergeladen hat. Den Inhalt der Benachrichtung kann man hier editieren.

MailOnHoldExpired.cshtml

Wenn ein Benuzter eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig hat keinen kryptografischen Schlüssel und der Empfänger der E-Mail hinterlegt innerhalb von 5 Tagen keinen kryptografischen Schlüssel, wird die E-Mail verworfen und der Absender darüber informiert. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

MailValidationError.cshtml

Wenn eine De-Mail nicht über den De-Mail Konnektor versendet werden kann, wird der Absender darüber benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

PolicyFailureNonDeliveryMessage.cshtml

Verstößt eine E-Mail gegen Richtlinien im Regelwerk, wird der Absender darüber benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

QualifiedSignatureIssueEscalationMail.cshtml

Wenn die Prüfung oder Erstellung einer qualifizierten Signatur fehlschlägt, wird eine Benachrichtigung an eine festgelegte Adresse geschickt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

SampleAutoReply.cshtml

Seit NoSpamProxy 10 ist es möglich, eine automatische Antwort erzeugen zu lassen, wenn zum Beispiel eine bestimmte E-Mail-Adresse angeschrieben wird. Der Inhalt dieser automatischen Antwort kann hier angepasst werden.

Diese Datei können Sie kopieren und unter anderem Namen ablegen. Im Regelwerk von NoSpamProxy geben Sie die Vorlagendatei für den jeweiligen Zweck dann an.

SymmetricPasswordUpdateNotification.cshtml

Wenn ein externer Empfänger ein Passwort für die PDF-Mail auf dem WebPortal hinterlegt hat, wird er über die Änderung benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

WordFilterMatchNotification.cshtml

Seit NoSpamProxy 10 ist es möglich, eine Benachrichtung an eine bestimmte E-Mail-Adresse zu schicken, sobald bestimmte Wörter in einer E-Mail auftauchen. In dieser Datei legen Sie den Inhalt der Benachrichtigung fest.

Anpassung der Template-Dateien

Fangen Sie mit der Datei “CommonMailTemplate” an. Hier bestimmen Sie das Aussehen aller E-Mails. Passen Sie die StyleSheets in den jeweiligen Dateien entsprechend Ihrer Bedürfnisse an. Auch die Einbindung des entsprechenden Logos erfolgt in dieser Datei. Im späteren Wirkbetrieb, müssen die Logodateien mit dem korrekten Namen ebenfalls im Ordner Templates-Ordner verfügbar sein.

Alle übrigen Dateien enthalten lediglich die Textbausteine.

Nach dem Neustart der Intranetrolle werden die neuen Designs verwendet und auf die Gatewayrolle(n) repliziert.

> **HINWEIS:** Beachten Sie, dass die Dateien beim Patchen/Upgraden überschrieben werden können. Kontrollieren Sie nach einem Patch/Upgrade, ob Ihre angepassten Dateien immer noch vorhanden sind.

Unterschiedliche Designs bei Absenderdomänen verwenden

Dieser Artikel beschreibt, wie Sie ab NoSpamProxy 11.x die Templates für das Design der System-Mails von NoSpamProxy (inkl. der PDF-Mails) so anpassen, dass auf Basis der Absenderdomäne unterschiedliche Designs verwendet werden. Als Basis für die dynamische Änderung verwendet NoSpamProxy die Template-Engine für .NET “Razor”.

Die zu editierenden CSHTML-Dateien liegen im Verzeichnis %Program Files%\Net at Work Mail Gateway\Intranet Role\Templates. Nach der Änderung werden die Dateien automatisch auf alle angeschlossenen Gatewayrolle repliziert.

> **HINWEIS:** Sie benötigen zumindest rudimentäre HTML-Kenntnisse, um die Anpassungen durchführen zu können.

Anpassung der Template-Dateien

HINWEIS: Vorgefertigte Beispieldateien mit unterschiedlichen Designs können Sie gerne beim NoSpamProxy Support anfordern. Diese Datei ist erst ab NoSpamProxy 11.0 verwendbar. In diesem Beispiel werden zwei unterschiedliche Designs für die Absenderdomänen netatwork.de und nospamproxy.de angewandt. Sie können die Anzahl der Domänen jederzeit erweitern oder reduzieren.

1. Entpacken Sie nach dem Herunterladen die ZIP-Datei zunächst in einen temporären Ordner. Sie enthält folgende Dateien:
   - CommonMailTemplate.cshtml
   - CommonMailTemplateNaw.cshtml
   - CommonMailTemplateNsp.cshtml
   - ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml
   - ConvertMailContentToPdfAttachmentActionTeaser.cshtml
   - EncryptedMailNotificationTemplate.cshtml
2. Fangen Sie mit den Dateien an, die mit “CommonMailTemplate” beginnen. Hier bestimmen Sie das Aussehen aller E-Mails, die bei der PDF-Mail erforderlich sind.

> **HINWEIS:** Achten Sie darauf, dass Sie das Standarddesign in der **CommonMailTemplate.cshtml** hinterlegen. Passen Sie die Stylesheets in den jeweiligen Dateien entsprechend Ihrer Bedürfnisse an. Auch die Einbindung der entsprechenden Logos erfolgt in diesen Dateien. Im späteren Wirkbetrieb, müssen die Logodateien mit dem korrekten Namen ebenfalls im Ordner Templates-Ordner verfügbar sein.

3. Passen Sie die Datei **ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml** an. Diese Datei bestimmt das Layout der PDF-Datei. Im Gegensatz zu den CommonMailTemplate-Dateien benötigen Sie hier nur eine Datei, um die Ausnahmen zu definieren. Die Anpassungen finden im oberen Teil statt. Ein Beispiel für drei unterschiedliche Designs ist eingebaut.

   > **HINWEIS:** Sie legen das Design für die unterschiedlichen Domänen fest. Falls NoSpamProxy im Wirkbetrieb die entsprechende Absende-Domäne nicht findet, wird das Standard-Design angewendet, das Sie mit dem Template-Editor in der Admin-GUI bestimmen können.

4. Kopieren Sie sämtliche CSHTML-Dateien in den Templates-Ordner Ihrer Programmversion.

HINWEIS: Sichern Sie vorher alle enthaltenen Dateien.

HINWEIS: Beachten Sie, dass die Dateien beim Patchen/Upgraden überschrieben werden. Kopieren Sie nach einem Versionsupgrade nicht die älteren, angepassten Dateien über die neueren, sondern passen diese neu an. Ansonsten besteht die Gefahr, dass neue, notwendige Angaben in den Vorlagendateien fehlen.

Übersicht der verfügbaren Template-Dateien

Die folgende Auflistung vermittelt einen Überblick über die Funktion der einzelnen Dateien:

ApplySymmetricEncryptionPasswordNotice.cshtml

Wenn ein Benutzer eine E-Mail als PDF-Mail verschickt, bekommt er eine Benachrichtigung über das verwendete Passwort, oder eine Info, dass dem Empfänger das Passwort per SMS zugeschickt wurde oder dass die Erstellung der PDF-Mail fehlgeschlagen ist. Der Text der jeweiligen Benachrichtigung steht in dieser Datei. Das Aussehen bzgl. Farben und Logo wird über das CommonMailTemplate festgelegt.

AttachmentManager.cshtml

Wenn über die Inhaltsfilter-Regeln eine Datei von einer E-Mail entfernt wird, erhält der Empfänger eine Info darüber. Der Anhang kann entweder entfernt und gelöscht werden, er kann in das Web Portal hochgeladen werden und er kann ins Web Portal hochgeladen und mit einer Admin-Freigabe belegt werden. Für jede der drei vorgesehenen Aktionen ist ein eigener Text verfügbar, der in dieser Datei editiert werden kann. Das Aussehen bzgl. Farben und Logo wird über das CommonMailTemplate festgelegt.

AttachmentManagerNotificationForBlockedAttachmentsModel.cshtml

Wenn über die Inhaltsfilter-Regeln E-Mails mit bestimmten Datei-Anhängen abgewiesen werden, erhält der Absender eine Info über die Abweisung. Der Inhalt dieser Nachricht kann in dieser Datei festgelegt werden. Das Aussehen bzgl. Farben und Logo wird über das CommonMailTemplate festgelegt.

AttachmentQuarantine.cshtml

Wenn über die Inhaltsfilter-Regeln eine Datei in das Web Portal verschoben und mit einer Admin-Freigabe belegt wird, erhält der Administrator eine Info-Mail darüber. Der Inhalt dieser E-Mail wird in dieser Datei festgelegt. Das Aussehen bzgl. Farben und Logo wird über das CommonMailTemplate festgelegt.

AttachmentQuarantineApproval.cshtml

Wenn über die Inhaltsfilter-Regeln eine Datei in das Web Portal verschoben, mit einer Admin-Freigabe belegt und anschließend durch den Administrator freigegeben wird, erhält der eigentliche Empfänger der Datei eine Info über die

Freigabe. Der Inhalt dieser E-Mail wird in dieser Datei festgelegt. Das Aussehen bzgl. Farben und Logo wird über das CommonMailTemplate festgelegt.

CommonMailTemplate.cshtml

In dieser Datei wird das generelle Aussehen von Benachrichtigungen festgelegt. Hier werden zum Beispiel die Farben und die zu verwendenden Logos als HTML-Tag hinterlegt. Alle anderen Dateien außer der **ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml** enthalten nur die Textbausteine.

ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml

Das Aussehen der PDF-Datei wird in dieser Datei festgelegt. Hier müssen erneut Farben und Logos definiert werden.

ConvertMailContentToPdfAttachmentActionTeaser.cshtml

In dieser Datei steht der Text für die Träger-Mail der PDF-Datei. Der Empfänger einer PDF-Mail wird darüber informiert, dass der eigentliche Inhalt der E-Mail im angehängten PDF-Dokument steht. Das Aussehen wird über das CommonMailTemplate festgelegt.

ConvertOfficeDocumentToPdfPreface.cshtml

Mit der “ConvertOfficeDocumentToPDF”-Action ist es möglich, Office-Dokumente in PDF zu wandeln, um dem Empfänger eine Voransicht ohne

aktive Inhalte zur Verfügung zu stellen. Vor das erzeugte PDF-Dokument wird eine Information gestellt. Der Inhalt dieser Information wird mit dieser Datei festgelegt.

DeliveryNotificationReport.cshtml

Hier steht der Inhalt des Sendeberichts, wenn ein Benutzer diesen in Outlook angefordert hat. Das Aussehen wird über das CommonMailTemplate festgelegt.

DeMailConnectorIssueEscalationMail.cshtml

Falls NoSpamProxy wiederholt keine De-Mail abholen oder senden kann, wird ein Administrator darüber benachrichtigt. Der Inhalt dieser Nachricht kann hier festgelegt werden.

EncryptedMailNotificationTemplate.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig verfügt über keinen kryptografischen Schlüssel, wird der Empfänger darüber informiert. In dieser Info-Mail steht, welche Optionen er hat. Der Inhalt dieser E-Mail wird in dieser Vorlage festgehalten. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionDelayedNotificationForSender.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig hat keinen kryptografischen Schlüssel, wird der Absender über die Verzögerung informiert. Der Inhalt der Verzögerungsnachricht wird hier

festgelegt. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionFailureNotificationForSender.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und es tritt ein Fehler bei der Verschlüsselung auf, wird der Absender darüber informiert. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

EncryptionSucceededNotificationForSender.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet, bekommt er eine Benachrichtigung, sobald die E-Mail verschlüsselt wurde. Das Aussehen wird über das CommonMailTemplate festgelegt.

LargeFileDownloadNotification.cshtml

Wenn der Empfänger einer Datei, die zuvor in das Web Portal verschoben wurde, sie herunterlädt, wird der Absender darüber benachrichtigt. Der Inhalt dieser Information wird mit dieser Datei festgelegt.

MailOnHoldExpired.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und enQsig hat keinen kryptografischen Schlüssel und der Empfänger der E-Mail hinterlegt innerhalb von 5 Tagen keinen kryptografischen Schlüssel, wird die E-Mail verworfen und der Absender darüber informiert. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

MailValidationError.cshtml

Wenn eine De-Mail nicht über den De-Mail Konnektor versendet werden kann, wird der Absender darüber benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

PolicyFailureNonDeliveryMessage.cshtml

Verstößt eine E-Mail gegen Richtlinien im Regelwerk, wird der Absender darüber benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

QualifiedSignatureIssueEscalationMail.cshtml

Wenn die Prüfung oder Erstellung einer qualifizierten Signatur fehlschlägt, wird eine Benachrichtigung an eine festgelegte Adresse geschickt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das CommonMailTemplate festgelegt.

SampleAutoReply.cshtml

Mit der Aktion “AutoReply” ist es möglich, E-Mails mit einer automatisch erzeugten E-Mail zu beantworten. Der Inhalt dieser Antwort wird hier festgelegt.

SymmetricPasswordUpdateNotification.cshtml

Wenn ein externer Empfänger ein Passwort für die PDF-Mail auf dem WebPortal hinterlegt hat, wird er über die Änderung benachrichtigt. Der Inhalt dieser Nachricht steht hier. Das Aussehen wird über das

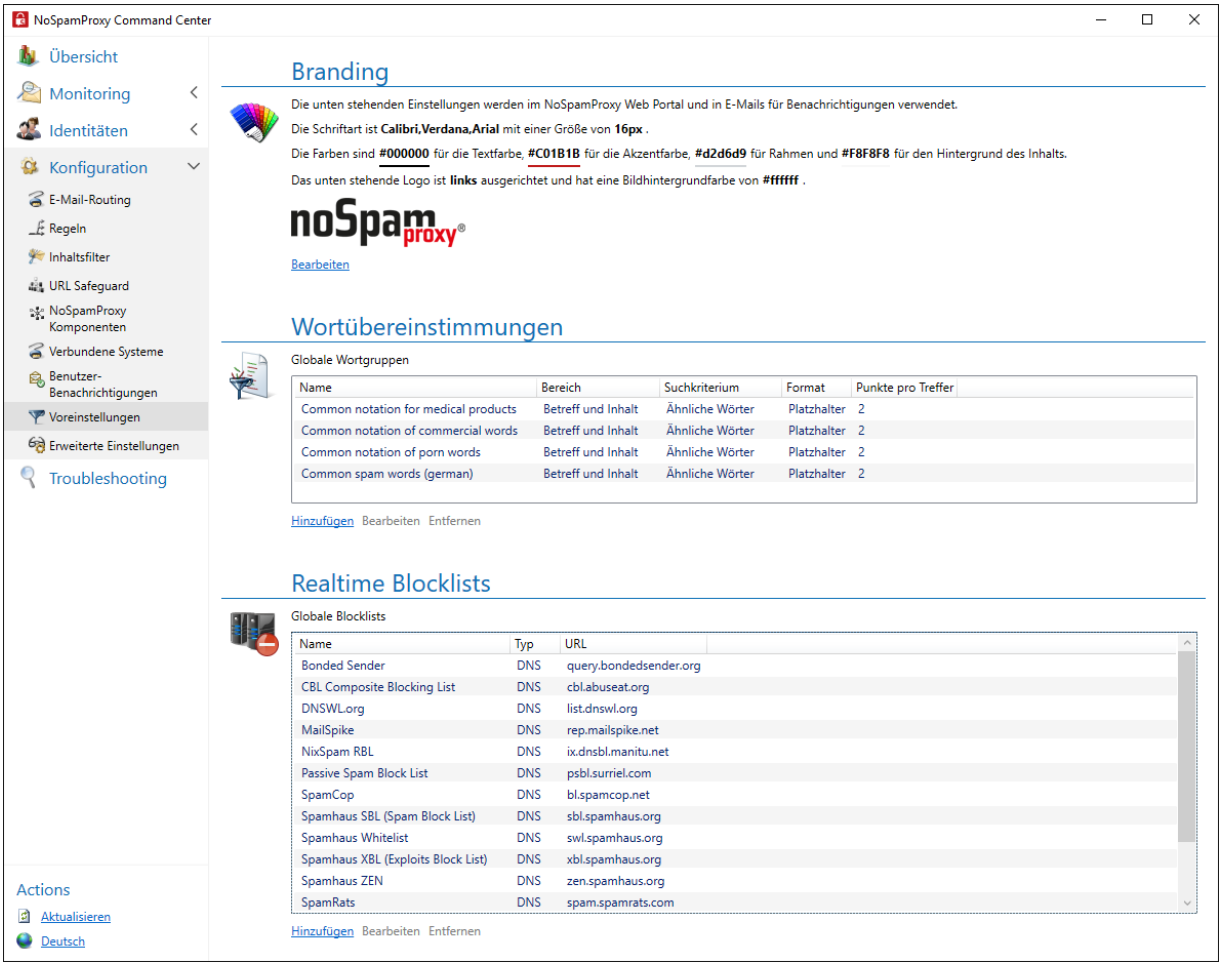
CommonMailTemplate festgelegt.

WordFilterMatchNotification.cshtml

Der Wortfilter bietet die Möglichkeit einer Benachrichtigung an eine beliebige E-Mail-Adresse, wenn bestimmte Wörter in E-Mails gefunden werden. Der Inhalt dieser Benachrichtigung kann hier definiert werden.

Voreinstellungen

Dieser Bereich beinhaltet globale Einstellungen, die in anderen Bereichen der Konfiguration – beispielsweise **Regeln**, **Partner** oder **Unternehmensbenutzer** – benutzt werden können.



HINWEIS: Die hier vorgenommenen Änderungen wirken sich auch auf bestehende Regeln, Partner oder Unternehmensbenutzer aus. Die Einstellungen gelten immer für alle Konfigurationen, in denen sie referenziert werden.

Branding

Das Branding bestimmt das Aussehen der von NoSpamProxy generierten E-Mails sowie das des Webportals.

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

Das Branding wird auf folgende Element angewendet:

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

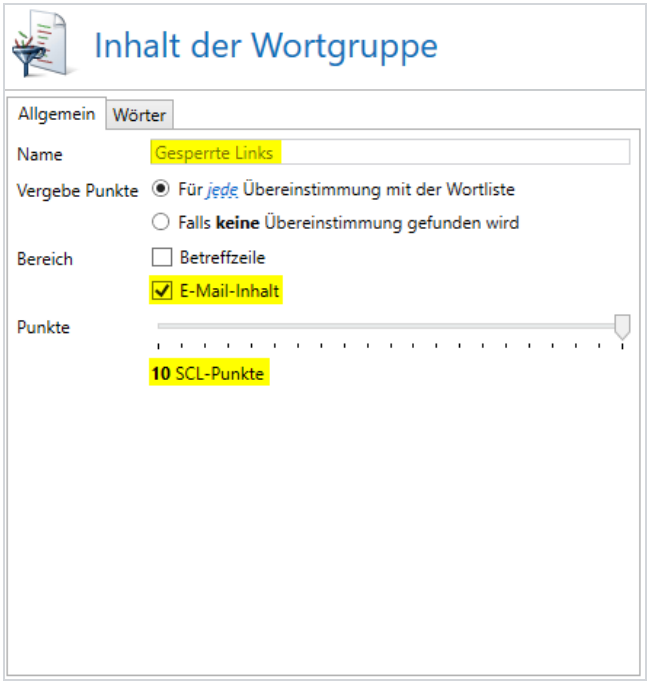
Wortübereinstimmungen

In diesem Bereich haben Sie die Möglichkeit, Listen mit Ausdrücken zu pflegen, für die Sie mit Hilfe des Filter **Wortübereinstimmungen** positive oder negative SCL-Punkte vergeben möchten. Die Ausdrücke werden in einzelnen Wortgruppen zusammengefasst, die Sie dann später in den einzelnen Regeln verwenden können. Pro Wortgruppe legen Sie fest, ob für die Begriffe die entsprechenden SCL-Punkte vergeben werden sollen. So haben Sie die Möglichkeit, Gruppen mit gewollten und ungewollten Ausdrücken zu erstellen.

Neue Wortgruppe hinzufügen

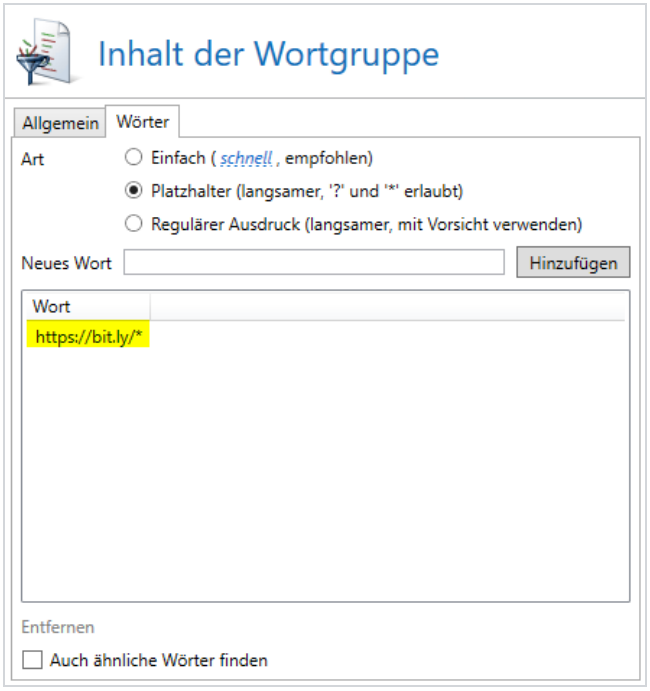
1. Gehen Sie zu **Konfiguration > Voreinstellungen > Wortübereinstimmungen**.
2. Klicken Sie **Hinzufügen**.
3. Bestimmen Sie auf der Registerkarte **Allgemein**
    - den Namen der Wortgruppe,
    - ob für Übereinstimmungen oder für nicht auftretende Übereinstimmungen Punkte vergeben werden,
    - den Bereich, auf den die Wortgruppe angewendet wird sowie

- die vergebenen SCL-Punkte.



4. Bestimmen Sie auf der Registerkarte **Wörter**
    - ob Sie nach exakten Treffern suchen wollen (einfach) oder Platzhalter oder Reguläre Ausdrücke einsetzen wollen,
    - die Wörter, die in der Wortliste enthalten sind und

- ob Sie auch nach ähnlichen Wörtern suchen wollen.



5. Klicken Sie auf **Fertigstellen**.

Realtime Blocklists

Realtime Blocklists (RBL) verwalten Listen mit verdächtigen Spam-IP-Adressen. RBLs können in den Regeln einzeln ausgewählt werden.

Neue Blocklist hinzufügen

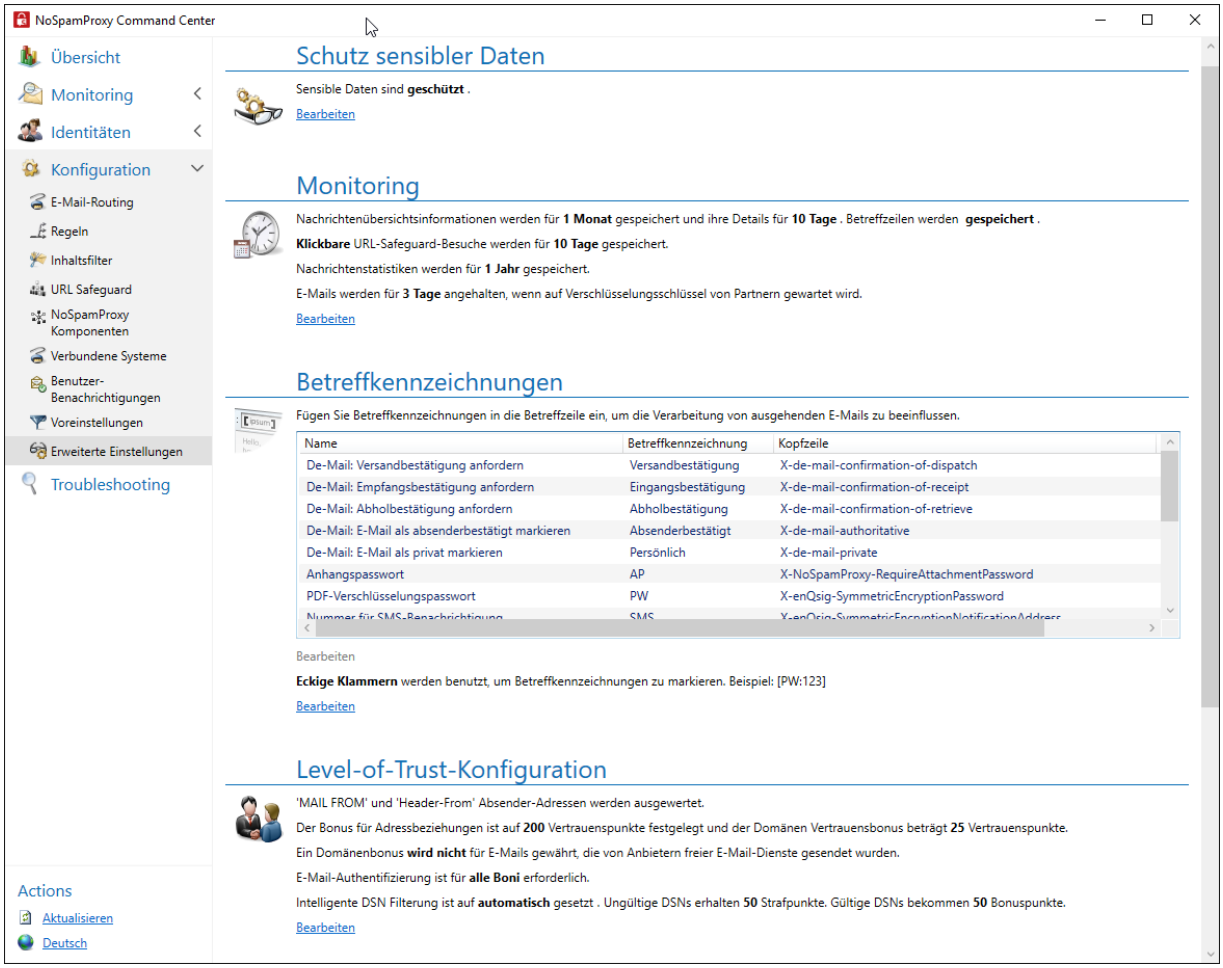
1. Gehen Sie zu **Konfiguration > Voreinstellungen > Realtime Blocklists**.
2. Klicken Sie **Hinzufügen**
3. Geben Sie unter Allgemeine Einstellungen einen Namen und eine Beschreibung ein.

4. Geben Sie unter **Blocklist-Ziel** an,
    - ob es sich um eine RBL-Liste handelt, die per DNS oder HTTP angesprochen wird sowie
    - im Feld Adresse entweder die IP-Adresse oder den Servername des abzufragenden Servers.
5. Definieren Sie unter **Antworten**
    - die möglichen Antworten des angefragten Servers und deren Bedeutung,
    - wieviele SCL-Punkte aus ihr resultieren sowie
    - einen beschreibenden Fehlertext.

    > **HINWEIS:** Ein negativer Wert entspricht Bonuspunkten, ein positiver Wert entspricht Maluspunkten. Der Text der Antwort taucht gegebenenfalls im Unzustellbarkeitsbericht auf, wenn der erstellende Server dies unterstützt. So weiß der Versender der abgewiesenen E-Mail, auf welcher Blacklist er aus welchem Grund steht. Die Antwort kann auch deaktiviert werden.

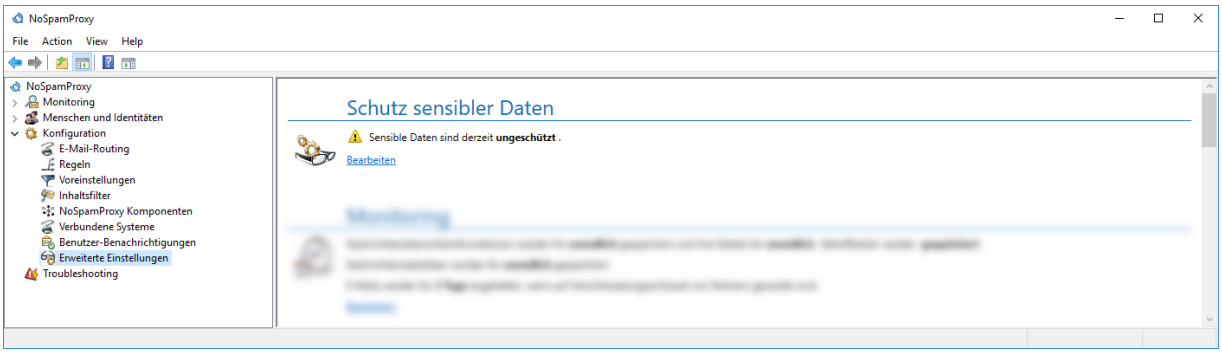
6. Klicken Sie **Fertigstellen**.

Erweiterte Einstellungen



Hier finden Sie Konfigurationsmöglichkeiten, die Sie im Normalfall nicht anpassen müssen.

Schutz sensibler Daten



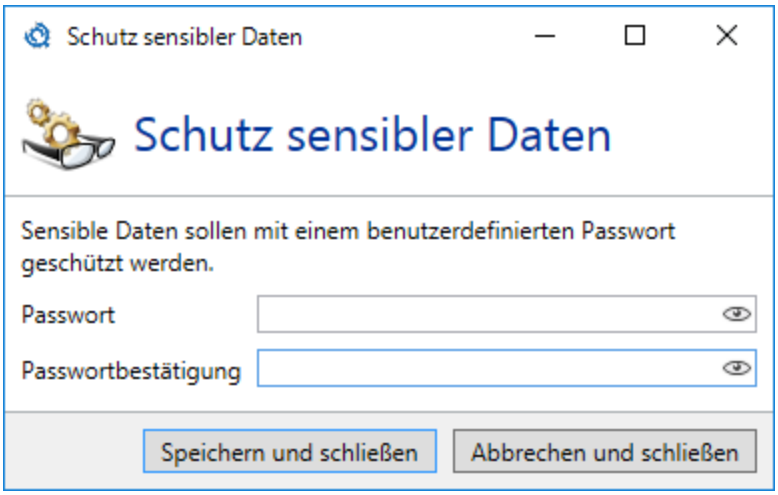
Um sensible Daten wie beispielsweise kryptographische Schlüssel oder Authentifizierungsinformationen vor dem Zugriff durch Dritte zu schützen, müssen Sie diese verschlüsseln.

> **HINWEIS:** Nach der Aktivierung kann der Schutz nicht rückgängig gemacht werden.

Schutz sensibler Daten aktivieren

1. Gehen Sie **Konfiguration > Erweiterte Einstellungen > Schutz sensibler Daten**.

2. Klicken Sie **Bearbeiten**.

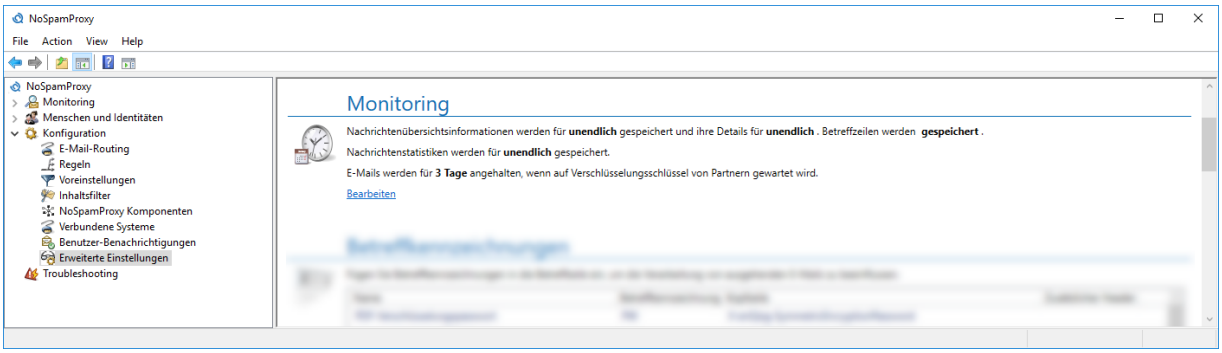


3. Geben Sie ein Passwort für den Schutz ein.
4. Klicken Sie **Speichern und schließen**.

HINWEIS: Sie können das Passwort zu einem späteren Zeitpunkt ändern.

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

Monitoring



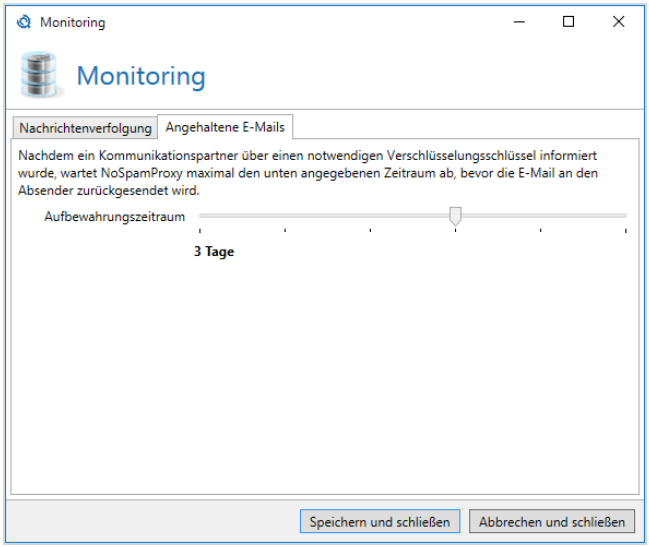
NoSpamProxy kann jede Verbindung in der Nachrichtenverfolgung mitprotokollieren. So können Sie nachvollziehen, wie die einzelnen E-Mails verarbeitet wurden.

Nachrichtenverfolgung aktivieren

1. Gehen Sie zu **Konfiguration > Erweiterte Einstellungen > Monitoring**.
2. Klicken Sie **Bearbeiten**.

3. Aktivieren Sie die Option **Nachrichtenverfolgungsdatensätze erfassen** auf der Registerkarte **Nachrichtenverfolgung**.
4. Konfigurieren Sie die folgenden Optionen:
   Speichere die Zusammenfassungen| Der Zeitraum, für den Sie E-Mails zurückverfolgen können. 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.
   Speichere die Details| Die Speicherdauer für die dazu gehörenden Nachrichtendetails. In den Details 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.
   URL Safeguard| Die Speicherdauer für Besuche von klickbaren Links beziehungsweise weiteren URLs wie nicht eingebetteten Bildern. Wenn Sie die Option **Speichere alle Besuche** wählen, wird eine große Menge an Daten erzeugt. Sie sollten diese Option nicht aktivieren, wenn Sie die Express-Edition von Microsoft SQL Server einsetzen.
   Speichere die Statistiken| Der Zeitraum, für den Sie Reports erstellen können. Um einen aussagekräftigen Report erstellen zu können, empfehlen wir eine Mindestaufbewahrungsfrist von 12 Monaten.
5. Konfigurieren Sie auf der Registerkarte **Angehaltene E-Mails** den Aufbewahrungszeitraum für E-Mails, für die auf einen

Verschlüsselungsschlüssel gewartet wird.



6. Klicken Sie **Speichern und schließen**.

Hinweise

> **HINWEIS:** Bitte beachten Sie die in Ihrem Unternehmen bestehenden Datenschutzvorschriften bei der Konfiguration dieses Abschnittes.

> **HINWEIS:** Um die Datenbankgröße der Nachrichtenverfolgung und der Reports nicht unkontrolliert wachsen zu lassen, räumt die Intranetrolle die Datenbank in einem regelmäßigen Intervall auf. Dabei werden alle Elemente, die ein vorgegebenes Alter überschritten haben, aus der Datenbank gelöscht.

HINWEIS: Wenn alle Nachrichtenverfolgungsdatensätze und die statistischen Daten verworfen werden sollen, wählen Sie bitte die Option **Nachrichtenverfolgung vollständig abschalten** unter dem **Erweiterte Einstellungen** der Gatewayrolle. In diesem Fall werden keinerlei 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.

HINWEIS: 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 kürzere Aufbewahrungsfristen der Nachrichtenverfolgungsdatensätze gewählt werden oder eine SQL-Server-Datenbank ohne diese Beschränkung installiert werden.

Betreffkennzeichnungen

In Abhängigkeit der von Ihnen lizenzierten Funktionen können Ihnen unterschiedliche Kennzeichnungen zur Verfügung stehen.

Betreffkennzeichnungen sind Schlüsselworte, die die Verarbeitung von einzelnen E-Mails zu steuern. Das Einfügen eines Schlüsselwortes in den Betreff einer E-Mail löst bestimmte Aktionen aus. Diese Schlüsselworte werden vor dem Versand von NoSpamProxy aus der Betreffzeile entfernt.

Betreffkennzeichnungen einfügen

- Fügen Sie der Betreffzeile am Beginn oder am Ende die gewünschten Schlüsselworte in Klammern hinzu.

HINWEIS: Leerzeichen und Unterschiede zwischen Groß- und Kleinschreibung in Schlüsselworten werden ignoriert.

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

Beispiele für den Einsatz

BEISPIEL:

- Die folgenden beiden Beispiele ergeben das gleiche Resultat:
  `[pw:geheim4312]` Hiermit sende ich Ihnen das verschlüsselte Dokument
  `[ PW : geheim4312 ]` Hiermit sende ich Ihnen das verschlüsselte Dokument
- Mehrere Kennzeichnungen gleichzeitig in einer Klammer:
  `[Unverschlüsselt, PDF, PW:geheim4312]` Hiermit sende ich Ihnen das verschlüsselte Dokument
- Mehrere Kennzeichnungen gleichzeitig in unterschiedlichen Klammern:
  `[Unverschlüsselt] [PDF] [PW:geheim4312]` Hiermit sende ich Ihnen das verschlüsselte Dokument

Verfügbare Betreffkennzeichnungen

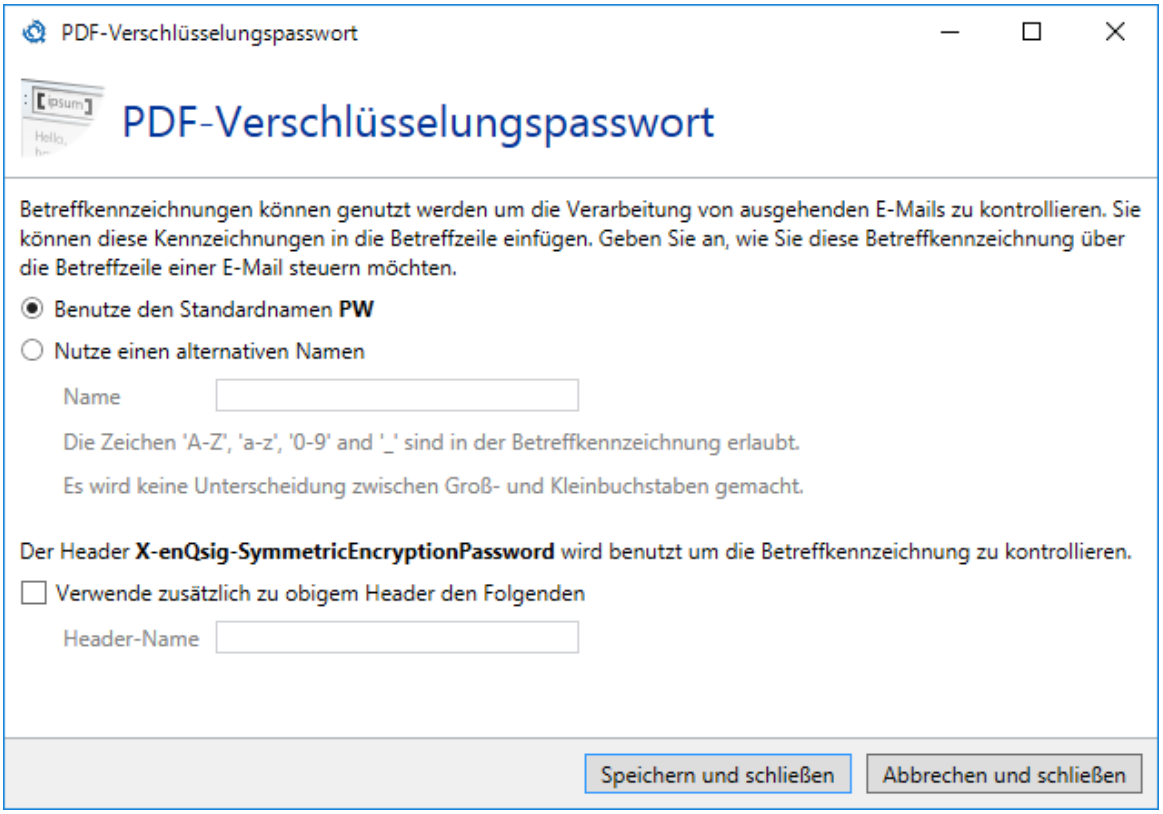
Betreffkennzeichnung	Ausgelöste Aktion
[Versandbestätigung]	De-Mail: Fordert eine Versandbestätigung von De-Mail an. Entspricht einem Einschreiben bei Briefen.
[Eingangsbestätigung]	De-Mail: Fordert eine Empfangsbestätigung von De-Mail an. Entspricht einem Einwurf-Einschreiben bei Briefen.
[Abholbestätigung]	De-Mail: Fordert eine Abholbestätigung von De-Mail an.

Betreffkennzeichnung	Ausgelöste Aktion
[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 beispielsweise das Passwort 'geheim4937'.
[SMS:Nr]	SMS-Benachrichtigung: Die Telefonnummer wird in der Aktion Anhänge mit einem Passwort schützen genutzt, um ein 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.

Betreffkennzeichnung	Ausgelöste Aktion
	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.
[AP]	Anhangspasswort: Schützt alle Anhänge durch ein Passwort, welches vor dem Herunterladen der Anhänge vom Empfänger eingegeben werden muss. Dieses Feature ist in NoSpamProxy Large Files verfügbar.

Betreffkennzeichnungen anpassen

Sie können Betreffkennzeichnungen an Ihre Bedürfnisse anpassen und sie jederzeit auf ihre Standardwerte zurücksetzen.



> **WARNUNG:** Im NoSpamProxy 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.

Besonderheiten beim automatischen Versand von E-Mails

Beim automatisierten Versand von E-Mails können Sie anstatt der Betreffkennzeichnungen auch E-Mail-Header verwenden.

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Erweiterte Einstellungen > Betreffkennzeichnungen**.
2. Öffnen Sie die gewünschte Betreffkennzeichnung.
3. Setzen Sie das Häkchen bei **Verwende zusätzlich zu obigem Header den folgenden**.
4. Geben Sie den gewünschten Header in das Eingabefeld ein.
5. Klicken Sie **Speichern und schließen**.

Der angegebene Header wird nun zusätzlich zum normalen Header verwendet.

NoSpamProxy Outlook Add-In

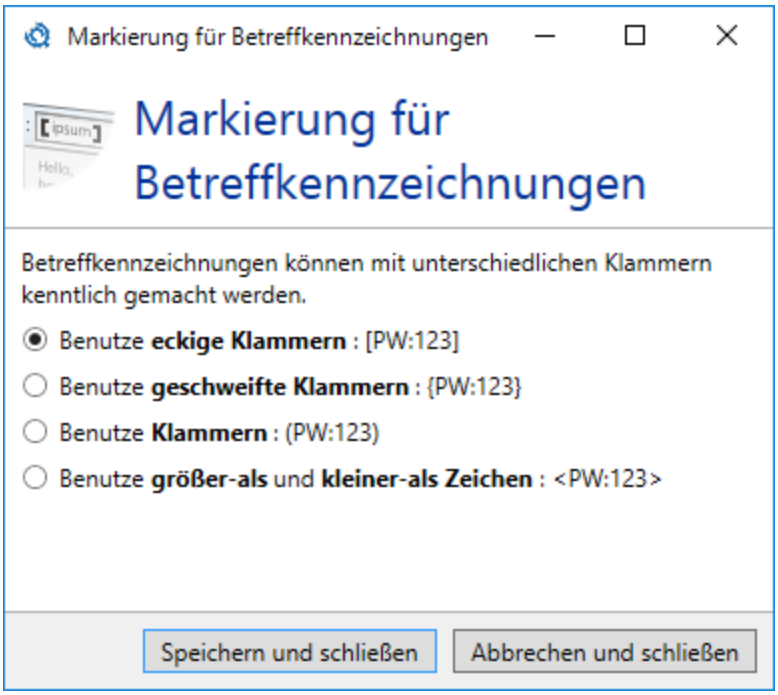
An Stelle der Betreffkennzeichnungen können Sie auch das Outlook Add-In für NoSpamProxy installieren. Das Outlook Add-In wird an Stelle der Betreffkennzeichnungen mit Microsoft Outlook verwendet.

Marker für Betreffkennzeichnungen anpassen

Standardmäßig werden eckige Klammern verwendet, um die Betreffkennzeichnungen kenntlich zu machen. Um dies zu ändern, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Erweiterte Einstellungen > Betreffkennzeichnungen**.

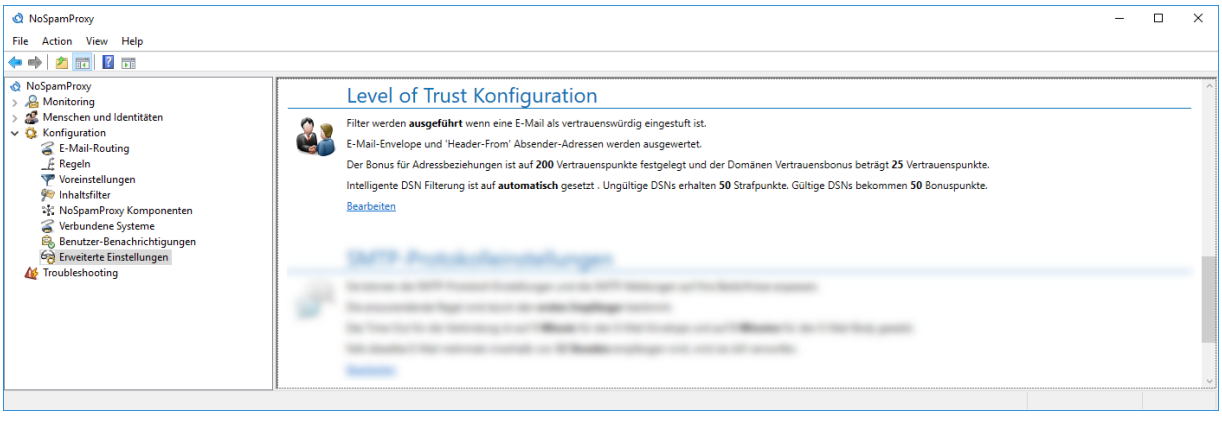
2. Klicken Sie **Bearbeiten**.



3. Wählen Sie den gewünschten Markertyp aus.

4. Klicken Sie **Speichern und schließen**.

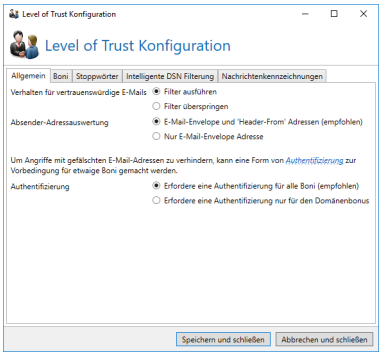
Level-of-Trust-Konfiguration



Um Level of Trust zu konfigurieren, gehen sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Erweiterte Einstellungen > Level-of-Trust-Konfiguration**
2. Klicken Sie **Bearbeiten**.
3. Nehmen Sie die Einstellungen auf den einzelnen Registerkarten vor (siehe unten).
4. Klicken Sie **Speichern und schließen**.

Registerkarte Allgemein

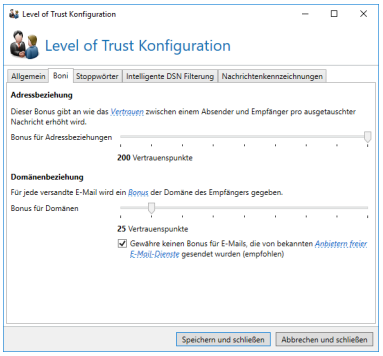


- **Verhalten für vertrauenswürdige E-Mails**| Bestimmt, ob E-Mails an lokale Adressen mit einer hinreichend hohen Level-of-Trust-Bewertung als vertrauenswürdig markiert und die in einer Regel konfigurierten Filter übersprungen werden. Lediglich Aktionen können die Annahme der E-Mail dann noch verhindern.
- **Absender-Adressauswertung**| Bestimmt, welche Adressen für die Analyse genutzt werden, falls sich die **MAIL FROM-Adresse** und die **Header-From-Adresse** unterscheiden. Falls beide Adressen überprüft

werden, wird die E-Mail abgewiesen, sobald eine der beiden Adressen nicht vertrauenswürdig ist.

- **Authentifizierung**| Bestimmt, ob eine erfolgreiche Authentifizierung durch DKIM-, S/MIME- und SPF-Prüfungen die Vorbedingungen für alle Boni oder nur für den Domänenbonus ist (siehe Registerkarte **Boni**).

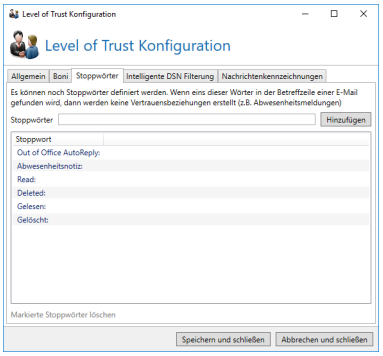
Registerkarte Boni



- **Adressbeziehung**| Bestimmt, um wie viele Punkte das Vertrauen zwischen einem Absender und einem Empfänger pro Nachricht erhöht wird. Mit dem Schieberegler können Sie hier einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht dabei (-0,1) Punkten für den **Spam Confidence Level (SCL)**. Für jede E-Mail an externe Adressen wird nicht nur der sogenannte Adressbeziehungsbonus erhöht, sondern auch ein Bonus für die jeweilige Empfängerdomäne.
- **Domänenbeziehung**| Bestimmt, um wie viele Punkte der Domänenbonus erhöht wird. Dieser Wert sollte kleiner sein als der Bonus für Adressbeziehungen. Auch hier können Sie mit dem Schieberegler einen

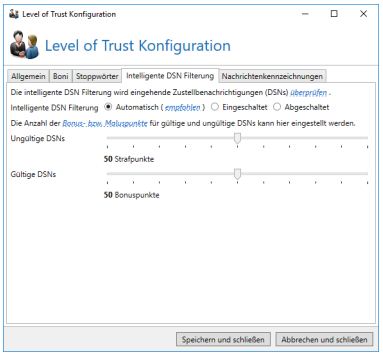
Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht dabei (-0,1) Punkten für den **Spam Confidence Level (SCL)**.

Registerkarte Stoppwörter



Sobald die Gatewayrolle eines der hier definierten Wörter im Betreff einer E-Mail an externe Adressen findet, bleiben sowohl der Adressbeziehungsbonus als auch der Domänenbonus unverändert und werden nicht erhöht. Bei automatisch generierten E-Mails wie Abwesenheitsnotizen ist dies eine sinnvolle Einstellung.

Registerkarte Intelligente DSN-Filterung



Die intelligente DSN-Filterung überprüft Delivery Status Notifications (DSNs) an lokale Adressen. Da NoSpamProxy weiß, welche E-Mails aus dem Unternehmen versendet wurden, kann es auch feststellen, ob für die gerade vorliegende DSN eine entsprechende E-Mail das Unternehmen verlassen hat.

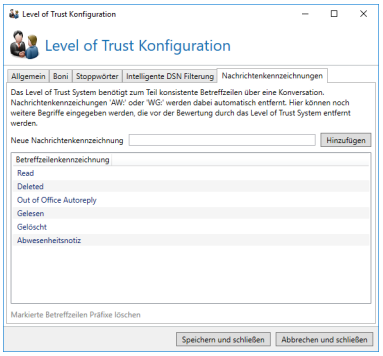
- **Intelligente DSN-Filterung|** Bestimmt, ob und wie die intelligente DSN-Filterung arbeitet.
- **Automatisch|** NoSpamProxy überprüft zuerst, ob sich in der Level-of-Trust-Datenbank Elemente befinden, die älter als sieben Tage sind. Erst dann bewertet NoSpamProxy ankommende DSNs.
- **Aktiviert|** NoSpamProxy bewertet den DSN in jedem Fall; auch, wenn noch keine Datensätze in der Level-of-Trust-Datenbank existieren.
- **Deaktiviert|** Die intelligente DSN-Filterung ist abgeschaltet.

BEISPIEL:
Es kommt ein DSN an und NoSpamProxy stellt fest, dass die Originalnachricht für diesen DSN von **schmidt@example.com** an **schulze@netatwork.de** gesendet wurde. NoSpamProxy prüft nun, ob es ein Adresspaar **schmidt@example.com/schulze@netatwork.de** in der Level-of-Trust-Datenbank gibt.

Ist dies nicht der Fall ist kann der vorliegende DSN nicht gültig sein und erhält Maluspunkte. Findet sich ein passendes Adresspaar, erhält der DSN Bonuspunkte. Damit diese Überprüfung stattfinden kann, müssen zwei Voraussetzungen gegeben sein:

- Es muss ein RFC-konformer DSN vorliegen. Das bedeutet, dass die Originalnachricht als Anhang an dem DSN hängt, damit NoSpamProxy das Original-Adresspaar ermitteln kann.
- Es muss sichergestellt sein, dass das Mail Gateway alle E-Mails an externe Adressen wirklich kennt. In Netzwerken mit verteilten Internetanbindungen kann das unter Umständen ein Problem sein.

Registerkarte Nachrichtenkennzeichnungen



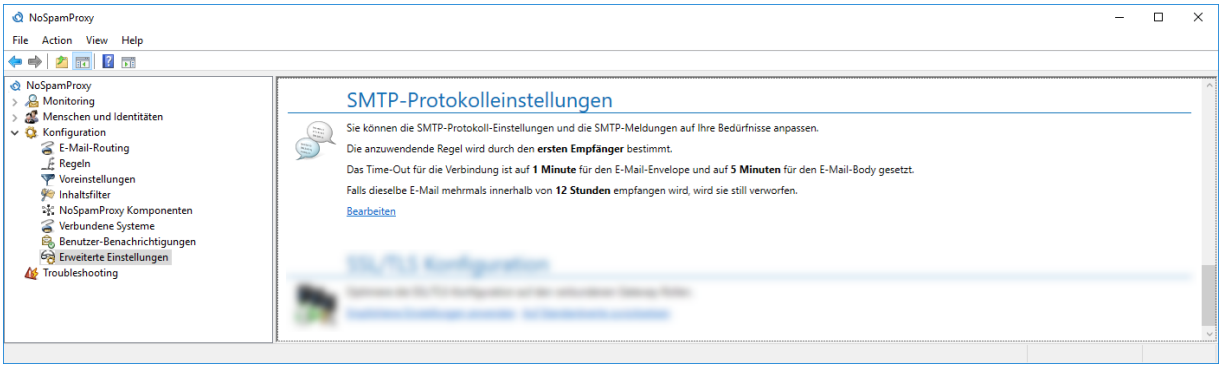
Das Level-of-Trust-System benötigt zum Teil konsistente Betreffzeilen über eine Konversation. Nachrichtenbezeichnungen wie beispielsweise **AW:** oder **WG:** müssen dazu entfernt werden. Hier konfigurieren Sie alle Kennzeichnungen, die Ihr E-Mail-System verwendet.

Siehe auch

Level of Trust

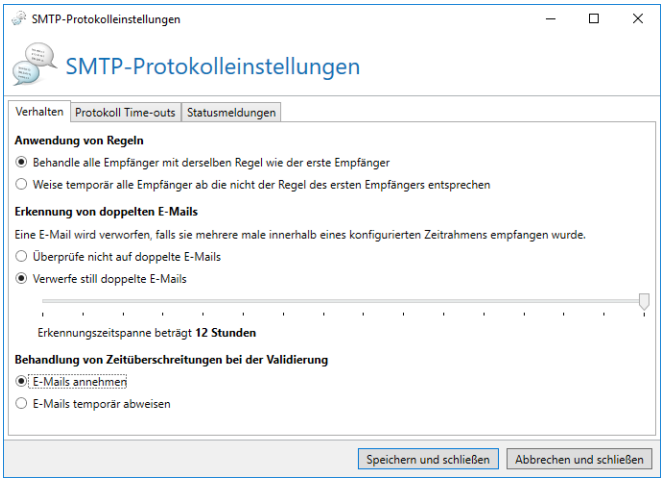
Punktevergabe für Domänen bei Level of Trust

SMTP-Protokolleinstellungen



Die Protokolleinstellungen regeln das Verhalten beim Empfang von E-Mails, die SMTP-Timeouts und die SMTP-Statusmeldungen.

Registerkarte Verhalten



Anwendung von Regeln

Wenn eine E-Mail an mehrere Empfänger gesendet wird, kann es vorkommen, dass unterschiedliche Regeln für diese E-Mail greifen. NoSpamProxy kann 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.

> **HINWEIS:** 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.

Behandle alle Empfänger mit derselben Regel wie der erste Empfänger| Die Regel, die für den ersten Empfänger zutrifft, wird auf alle Empfänger dieser E-Mail angewendet.

Weise temporär alle Empfänger ab, die nicht der Regel des ersten Empfängers entsprechen| Alle Empfänger, auf die nicht die Regel des ersten Empfängers zutrifft, werden temporär abgewiesen. NoSpamProxy sendet an das einliefernde System die Fehlermeldung **Too many Recipients**. Für die abgewiesenen E-Mails wird ein erneuter Zustellversuch unternommen. So kann NoSpamProxy für jeden Empfänger die passende Regel anwenden. Allerdings werden die E-Mails entsprechend mehrfach vom Absender eingeliefert.

> **HINWEIS:** Diese Funktion erlaubt Ihnen die Steuerung der E-Mail-Bewertung. Nachteil sind die mehrfache Übertragung sowie ein nicht vollständig RFC-konformes Verhalten.

Erkennung von doppelten E-Mails

NoSpamProxy kann erkennen, wenn dieselbe E-Mail mehrere Male empfangen wird. Das mehrfache Versenden derselben E-Mail tritt üblicherweise bei falscher Konfiguration wie beispielsweise 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.

Prüfe nicht auf doppelte E-Mails| Es findet keine Prüfung auf doppelte E-Mails statt.

Verwerfe still doppelte E-Mails| Doppelte E-Mails, die im konfigurierten Zeitraum empfangen werden, werden still verworfen.

Behandlung von Zeitüberschreitungen bei der Validierung

Sie können bestimmen, wie E-Mails behandelt werden sollen, deren Validierungszeit die unter Protokoll Time-out konfigurierten Maximalwerte überschreitet.

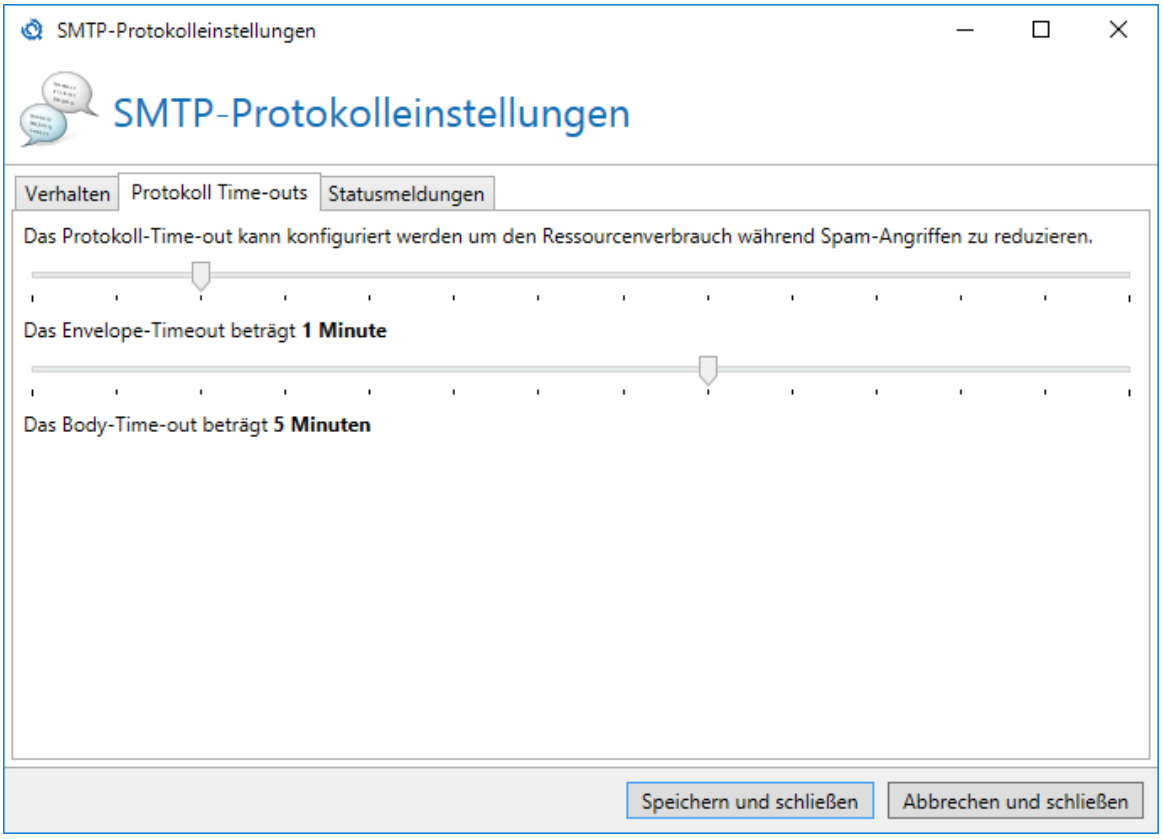
E-Mails annehmen| E-Mails, deren Validierungszeit die Maximalwerte überschreitet, werden angenommen.

E-Mails temporär abweisen| E-Mails, deren Validierungszeit die Maximalwerte überschreitet, werden temporär abgewiesen.

HINWEIS: Falls die Malwareüberprüfung nicht abgeschlossen ist, wenn ein Validierungs-Timeout erfolgt, wird die jeweilige E-Mail in jedem Fall temporär abgewiesen.

HINWEIS: E-Mails werden in jedem Fall abgewiesen, wenn sie zuvor durch eine Aktion temporär oder permanent abgewiesen wurden.

Registerkarte Protokoll-Timeouts



> **HINWEIS:** Das Anpassen der Timeouts hat großen Einfluss auf den Ressourcenbedarf Ihres Servers bei starkem E-Mail-Verkehr.

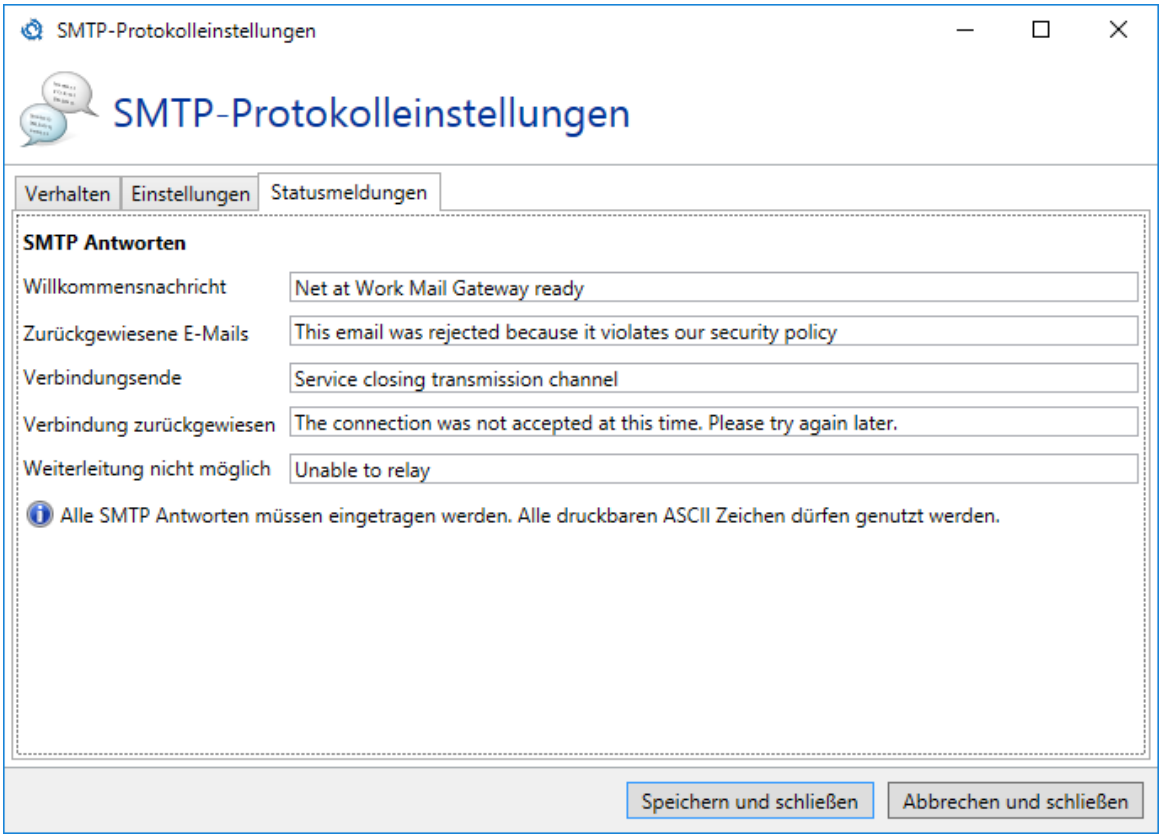
Im Abschnitt SMTP Protokoll Timeout Einstellungen können Sie festlegen, ab wann NoSpamProxy bei Inaktivität eine Verbindung trennt. Dies wird für zwei Abschnitte innerhalb des SMTP-Protokolls festgelegt.

Envelope-Timeout| Bestimmt den Timeout für die Kommandos innerhalb des sogenannten Envelope. Dies betrifft alle Kommandos bis zum DATA-Befehl (HELO/EHLO, MAIL FROM, RCPT TO).

Body-Timeout| Sobald der DATA-Befehl gesendet wurde, gilt die Einstellung unter **Body-Timeout**.

HINWEIS: 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.

Registerkarte Statusmeldungen



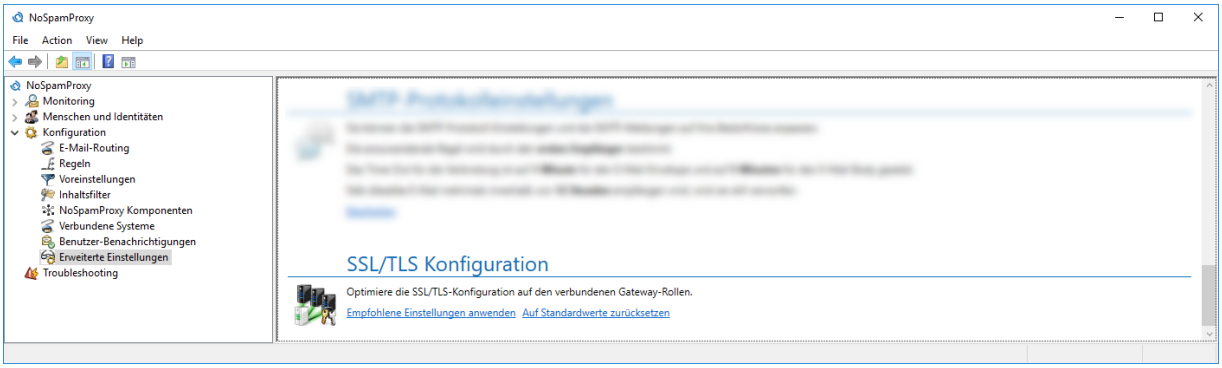
Die Statusmeldungen bestimmen, welche Texte NoSpamProxy an andere Server sendet. Die SMTP-Antworten sind Standardangaben im SMTP-Handshake, die für den normalen Anwender in der Regel nicht sichtbar sind. Dennoch kann es sinnvoll sein, die Angaben nach eigenem Bedarf zu ändern. Dies kann Administratoren bei der Fehlersuche und -analyse unterstützen.

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 in das zugehörige Eingabefeld und ändern den Text.

> **HINWEIS:** Für SMTP-Meldungen dürfen Sie keine Umlaute verwenden. Umlaute werden von dem verwendeten SMTP-Protokoll nicht unterstützt.

SSL-/TLS-Konfiguration

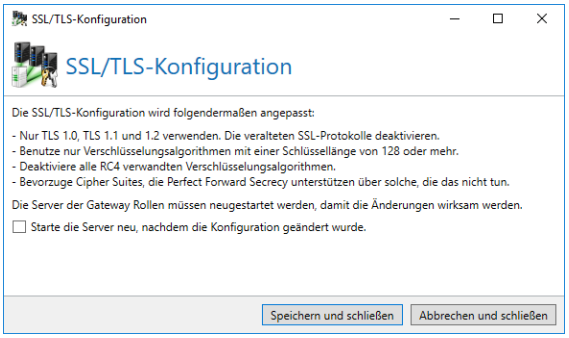


Bei der Transportverschlüsselung wird die Verbindung über SSL oder TLS abgesichert. Dabei greift die Gatewayrolle auf das Betriebssystem zurück. Dessen Einstellungen werden bei Verbindungen verwendet.

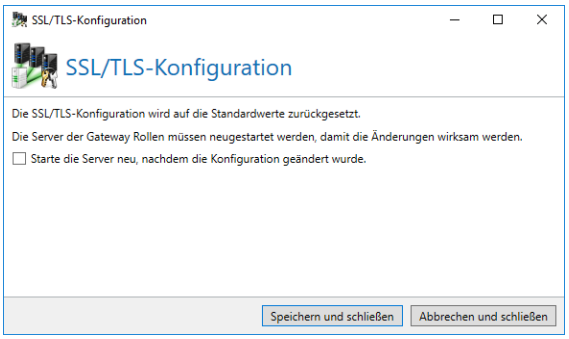
> **HINWEIS:** In letzter Zeit haben sich einige Verschlüsselungsverfahren (z.B. DES oder RC4) als nicht mehr sicher herausgestellt. Daher ist sinnvoll, diese zu deaktivieren. Einige Cipher Suites unterstützen ein Verfahren namens Perfect Forward Secrecy. Dies verhindert - kurz gesagt - dass die Inhalte 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.

SSL-/TLS-Konfiguration anpassen

Sie können hier in der Oberfläche die empfohlenen Einstellungen anwenden. Damit die Änderungen wirksam werden, muss der Server neu gestartet werden:

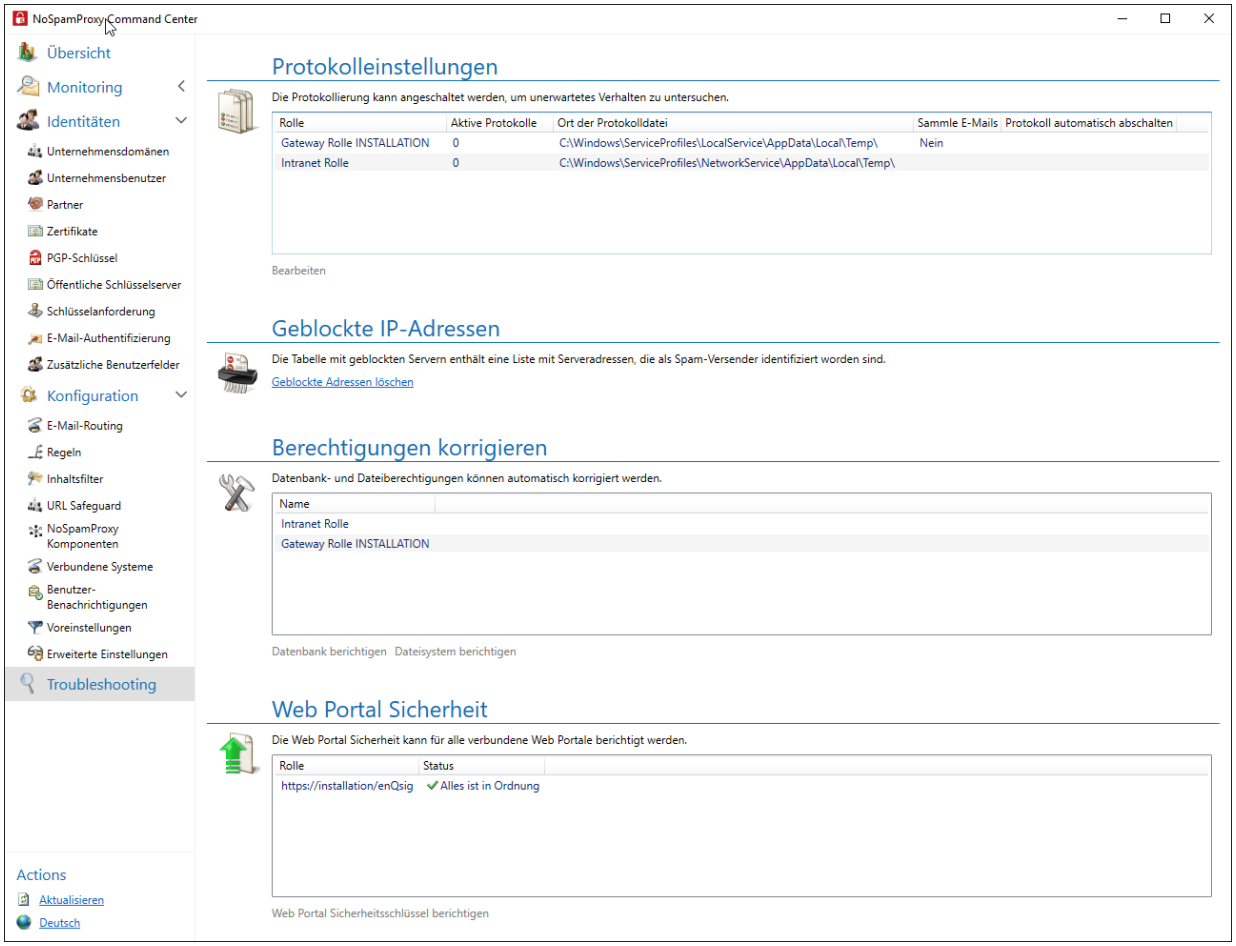


Sie haben in diesem Bereich außerdem die Möglichkeit, die Standardwerte von Windows wiederherzustellen:



HINWEIS: Hierbei handelt es sich um eine systemweite Änderung, die sich auch auf andere Programme auswirken kann.

Troubleshooting



Dieser Bereich bietet Ihnen Zugriff auf Werkzeuge, um Protokolle der Aktivitäten oder auch eine neue Datenbank für die einzelnen Rollen von NoSpamProxy zu erstellen. Das erneute Erstellen einer Datenbank kann notwendig werden, falls die alte Datenbank Schaden genommen hat.

Protokolleinstellungen

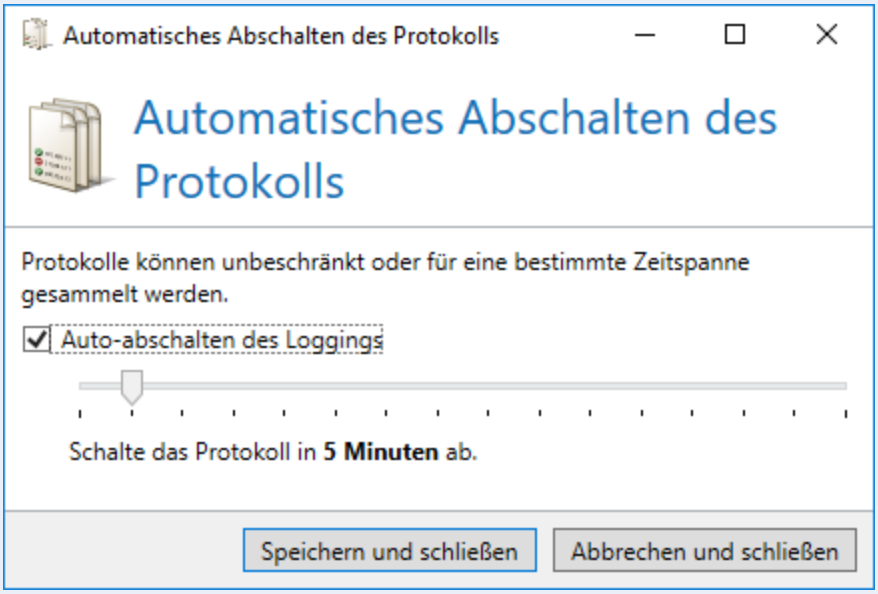
Um die Protokolleinstellungen für die jeweilige Gateway- oder Intranetrolle zu ändern, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Troubleshooting > Protokolleinstellungen**.
2. Markieren Sie die gewünschte Rolle.
3. Klicken Sie **Bearbeiten**.
4. Nehmen Sie die gewünschten Einstellungen vor (siehe unten).
5. Klicken Sie **Speichern und schließen**.

Registerkarte **Protokolleinstellungen**

- **Ort der Protokolldatei|** Der Speicherort für die Log-Dateien.
- **Protokollkategorien|** Die Kategorien, für die Sie die Protokollierung aktivieren möchten.

HINWEIS: 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. Wir empfehlen, das Log nur für eine festgelegte Zeitspanne zu erstellen. Klicken Sie dazu auf **Ändern** und nehmen Sie dann die gewünschte Einstellung vor.



Registerkarte **Debugeinstellungen**

Sie können alle E-Mails vor und nach der Bearbeitung durch NoSpamProxy auf der Festplatte speichern.

- **Speicherort**| Der Speicherort für E-Mails als absoluter Pfad auf der Gatewayrolle.

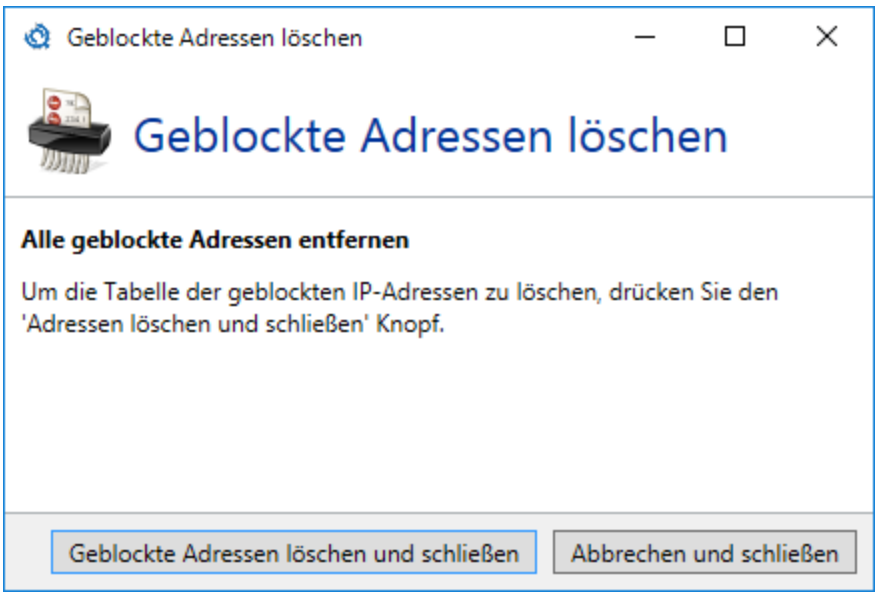
HINWEIS: Die Speicherung aller E-Mails auf der Festplatte hat einen hohen Platzbedarf und kann starke Leistungseinbußen des Servers nach sich ziehen. Nutzen Sie diese Funktion deshalb nur zur Fehlerdiagnose und schalten Sie sie danach wieder ab.

HINWEIS: Dieser Reiter ist nur bei Gatewayrollen vorhanden.

Geblockte IP-Adressen

NoSpamProxy sperrt nach Erhalt einer Spam-E-Mail das einliefernde Gateway standardmäßig für 30 Minuten. Falls irrtümlich eine vertrauenswürdige IP-Adresse in diese Blacklist aufgenommen wird, so können Sie hier die Liste der gesperrten Server löschen.

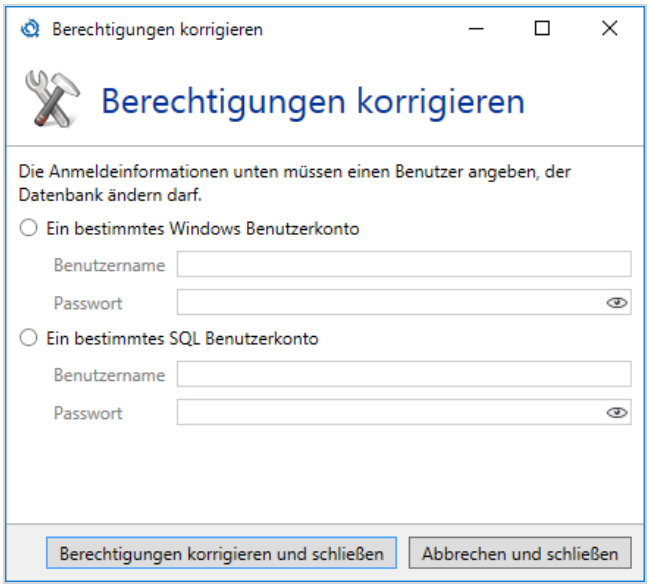
1. Gehen Sie zu **Troubleshooting > Geblockte IP-Adressen**.
2. Klicken Sie **Geblockte Adressen löschen**.
3. Klicken Sie **Geblockte Adressen löschen und schließen**.



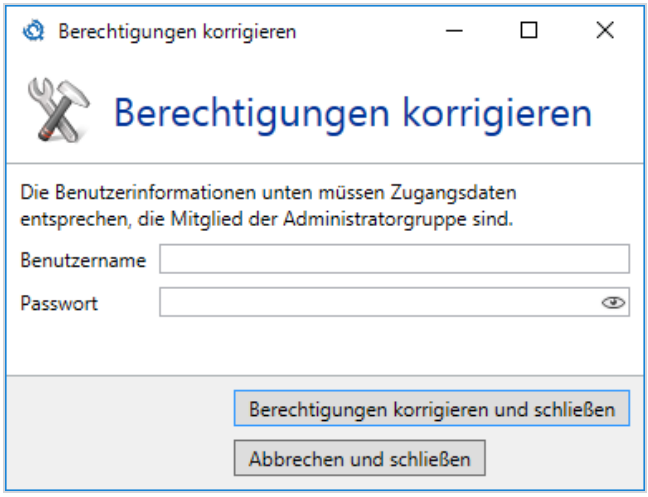
Berechtigungen korrigieren

Falls die Dateisystemberechtigungen von NoSpamProxy beispielsweise durch Drittprogramme so verändert wurden, dass die Funktion eingeschränkt wird, können Sie dies hier korrigieren.

1. Gehen Sie zu **Troubleshooting > Berechtigungen korrigieren**.
2. Markieren Sie die gewünschte Rolle.
3. Klicken Sie entweder **Datenbank berichtigen** oder **Dateisystem berichtigen**.
    - Datenbank berichtigen



- Dateisystem berichtigen



4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie **Berechtigungen korrigieren und schließen**.

Webportal-Sicherheit

Für die Sicherheit aller installierten Webportale müssen bestimmte Informationen synchron gehalten werden. Falls Sie mehrere Webportale einsetzen, müssen diese Informationen nach der Installation des zweiten Webportals synchronisiert werden. Ein solcher Vorfall wird auf der Übersichtsseite angezeigt. Zusätzlich sehen Sie hier, welches Portal dies betrifft.

Um die Sicherheitsschlüssel zu berichtigen, gehen Sie folgendermaßen vor:

- Markieren Sie alle Webportale, die den Text **Der Sicherheitsschlüssel ist falsch** anzeigen, und klicken Sie **Webportal Sicherheitsschlüssel berichtigen**.

HINWEIS: Solange die Schlüssel nicht synchron sind, zeigen die Formulare auf dem Webportal Fehler an und sind in ihrer Funktion beeinträchtigt.

Disclaimer

> Dieses Feature ist verfügbar, wenn Sie eine entsprechende Lizenz erworben haben.

Mit NoSpamProxy Disclaimer können Sie E-Mail-Disclaimer automatisch nach vorher definierten Regeln in Ihre E-Mails einbinden. Damit Sie Disclaimer in Ihre E-Mails einbinden können, müssen Sie NoSpamProxy in drei einfachen Schritten konfigurieren:

Platzhalter für die Verwendung in Disclaimer-Vorlagen vorbereiten

Vorlagen und Regeln einrichten

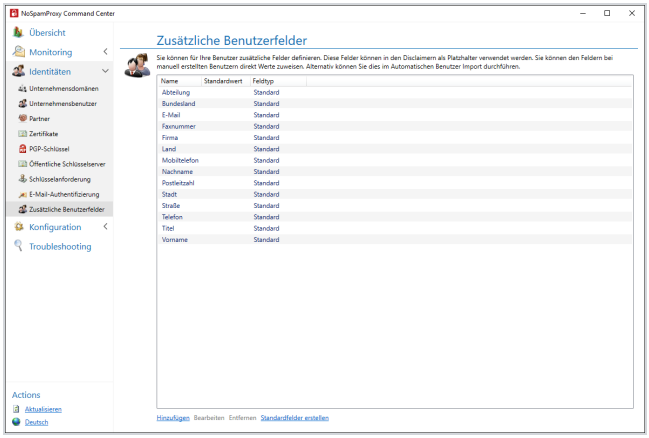
Disclaimer anwenden

Platzhalter für die Verwendung in Disclaimer-Vorlagen vorbereiten

Bevor Sie Platzhalter anlegen können, müssen Sie zusätzliche Benutzerfelder erstellen. Erst dann können Sie Platzhalter in den Disclaimer-Vorlagen verwenden, denn die Platzhalter werden durch die in den Benutzerfeldern gesetzten Werte ersetzt. Siehe **Zusätzliche Benutzerfelder hinzufügen**, **Vorlagen erstellen**.

Zusätzliche Benutzerfelder global erstellen

1. Gehen Sie zu **Identitäten > Zusätzliche Benutzerfelder > Zusätzliche Benutzerfelder**.
2. Klicken Sie **Hinzufügen**.
3. Legen Sie die benötigten Felder an und hinterlegen Sie bei Bedarf Standardwerte für die einzelnen Felder.



TIPP:
Für die meisten Anwendungsfälle ist es empfehlenswert, **Standardfelder erstellen** zu wählen. Dadurch werden häufig genutzte Felder erstellt. Beim Erstellen der Felder wird automatisch die Zuordnung der Benutzerfelder zu Active-Directory-Feldern vorgenommen. Diese Zuordnung können Sie später manuell anpassen.

Standardwerte 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.

Siehe **Benutzerimport automatisieren**.

HINWEIS:

- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden im Vorlagen-Editor mit einem Stern (*) dargestellt, also beispielsweise **[*BenutzerdefiniertesBenutzerfeld]**. Ausgenommen sind Platzhalter in Vorlagen, die mit NoSpamProxy Version 13.2 oder kleiner erstellt wurden.
- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden nicht lokalisiert.

Zusätzliche Benutzerfelder während des Benutzerimports erstellen

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.

1. Gehen Sie zu **Identitäten > Zusätzliche Benutzerfelder > Zusätzliche Benutzerfelder**.
2. Erstellen Sie eigene Felder oder Standard-Benutzerfelder.
3. Legen Sie während des Benutzerimports fest, aus welchem Feld des Verzeichnisses die Daten übernommen werden sollen.

> **HINWEIS:** 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.

Vorlagen und Regeln einrichten

Eine **Vorlage** bestimmt den HTML- und Nur-Text-Inhalt eines Disclaimers, eine **Regel** bestimmt, wann und wie ein Disclaimer einer E-Mail hinzugefügt wird.

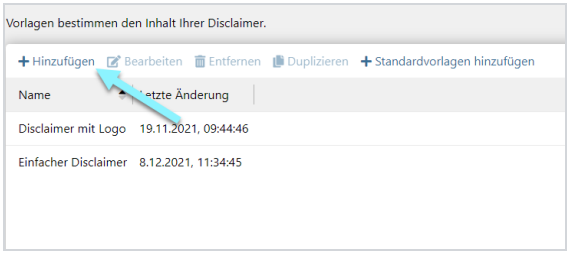
- Klicken Sie auf der Übersichtsseite des NoSpamProxy Command Center auf **Disclaimer-Webseite öffnen**.

Vorlagen erstellen

Vorlagen bestimmen den Inhalt Ihrer Disclaimer.

Eine Vorlage hinzufügen

1. Gehen Sie zu **Disclaimer > Disclaimer-Vorlagen**.
2. Klicken Sie **Hinzufügen**, um eine neue Vorlage hinzuzufügen.



3. Geben Sie unter **Allgemein** einen Namen für die neue Vorlage ein und klicken Sie **Weiter**.
4. Fügen Sie HTML-Inhalt hinzu und klicken Sie Weiter.

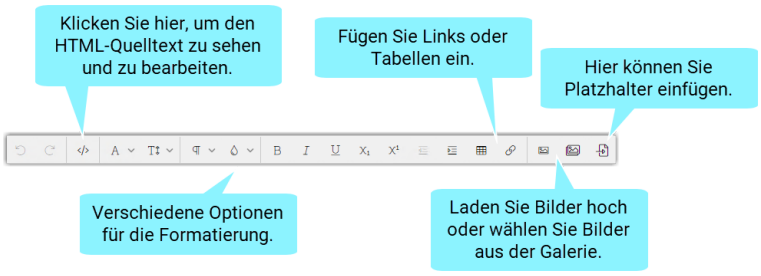
5. Fügen Sie Nur-Text-Inhalt hinzu.
6. Klicken Sie **Beenden**.

In der HTML-Ansicht können Sie die Werkzeugleiste sowie die weiteren Schaltflächen nutzen, um dem Disclaimer Elemente wie Platzhalter oder Grafiken hinzuzufügen. Sie können auch freien Text - wie zum Beispiel eine Grußformel - hinzufügen.

> **HINWEIS:** Die Nur-Text-Ansicht verwenden E-Mail-Clients, wenn die HTML-Anzeige deaktiviert ist. Hier können Sie ausschließlich Platzhalter und freien Text einfügen.

Optionen in der Werkzeugleiste (HTML-Ansicht)

Die Funktionsweise der Werkzeugleiste orientiert sich an vergleichbaren Werkzeugleisten in Office-Produkten.



> **TIPP:** Bevor Sie Platzhalter einfügen können, müssen Sie zusätzliche Benutzerfelder erstellen. Siehe **Zusätzliche Benutzerfelder hinzufügen**, **Platzhalter für die Verwendung in Disclaimer-Vorlagen vorbereiten**.

HINWEIS:

- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden im Vorlagen-Editor mit einem Stern (*) dargestellt, also beispielsweise **[*BenutzerdefiniertesBenutzerfeld]**. Ausgenommen sind Platzhalter in Vorlagen, die mit NoSpamProxy Version 13.2 oder kleiner erstellt wurden.
- Platzhalter, die auf benutzerdefinierten Benutzerfeldern beruhen, werden nicht lokalisiert.

Verfügbare Platzhalter

Platzhalter werden durch die in Ihrem Azure Active Directory zugeordneten Werte des jeweiligen Benutzerprofilattributs ersetzt.

Die folgenden Platzhalter sind verfügbar:

Platzhalter	Benutzerprofilattribut im Azure Active Directory
Abteilung	Department
Bundesland	State
E-Mail	Mail
Faxnummer	FaxNumber
Firma	CompanyName
Land	Country
Mobiltelefon	MobilePhone

Platzhalter	Benutzerprofilattribut im Azure Active Directory
Nachname	Surname
Postleitzahl	PostalCode
Stadt	City
Straße	StreetAddress
Telefon	BusinessPhones
Titel	JobTitle
Vorname	GivenName

Standardvorlagen hinzufügen

Standardvorlagen enthalten bereits eine Auswahl häufig benutzter Platzhalter, können aber ebenso wie neu angelegte Vorlagen frei editiert werden.

- Klicken Sie **Standardvorlagen hinzufügen**, um diese hinzuzufügen.

Regeln hinzufügen

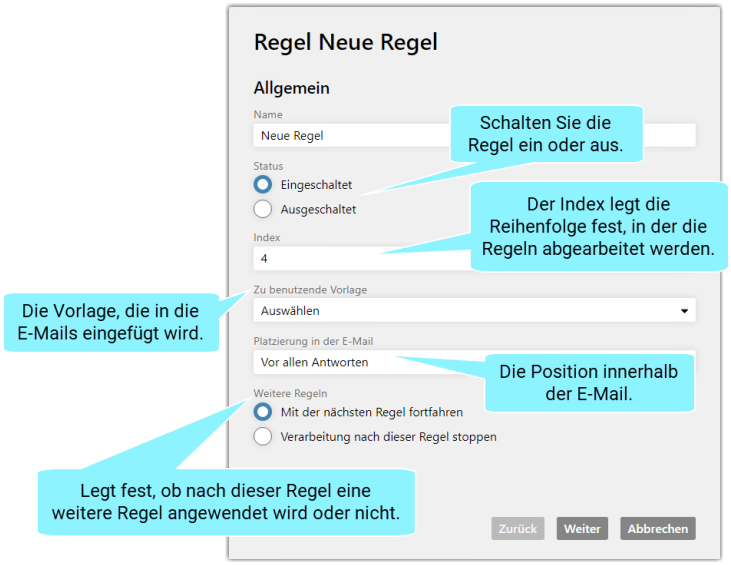
Regeln bestimmen, wann und wie Disclaimer in Ihre E-Mails eingefügt werden.

1. Gehen Sie zu **Disclaimer > Disclaimer-Regeln**, um die Übersichtsseite der Regeln zu öffnen.
2. Klicken Sie **Hinzufügen**, um eine neue Regeln hinzuzufügen.

3. Konfigurieren Sie die gewünschten Optionen (siehe unten).
4. Klicken Sie **Beenden**, um die vorgenommenen Änderungen zu speichern und zur Übersicht der Regeln zurückzukehren.

Allgemein

Hier nehmen Sie grundlegende Einstellungen für die neue Regel vor.



> **TIPP:** Mit einem E-Mail-Disclaimer für eingehende E-Mails können Sie beispielsweise alle E-Mails markieren, die aus dem Internet stammen.

Bedingungen

Eine Regel wird angewendet, wenn **alle** Bedingungen erfüllt sind.

Mit bestimmten Worten (mehrere Optionen)| Die Bedingung ist erfüllt, wenn eines oder mehrere der definierten Worte vorhanden sind.

In einer bestimmten Zeitspanne| Die Bedingung ist in der angegebenen Zeitspanne erfüllt.

Ausnahmen

Eine Regel wird angewendet, wenn **keine** der Ausnahmen zutrifft.

Mit bestimmten Worten (mehrere Optionen)| Die Ausnahme trifft zu, wenn eines oder mehrere der definierten Worte vorhanden sind.

In einer bestimmten Zeitspanne| Die Ausnahme ist in der angegebenen Zeitspanne erfüllt.

Reihenfolge der Regeln ändern

Um die Reihenfolge (den Index) der Regeln zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie die Regel aus, deren Index Sie verändern wollen.
2. Klicken Sie **Reihenfolge ändern**.
3. Bewegen Sie die Regel, indem Sie entweder **Nach oben** oder **Nach unten** klicken.
4. Klicken Sie **Speichern**.

Disclaimer anwenden

Die Aktion **Disclaimer anwenden** fügen Sie als Aktion einer NoSpamProxy-Regel hinzu. Die Aktion fügt ausgehenden Nachrichten einen Disclaimer hinzu. Dazu werden die auf der Disclaimer-Website angelegten Regeln und Vorlagen ausgewertet.

1. Gehen Sie im NoSpamProxy Command Center zu **Konfiguration > Regeln**.
2. Öffnen Sie eine Regel für ausgehende E-Mails.
3. Wechseln Sie zur Registerkarte **Aktionen**.
4. Klicken Sie auf **Hinzufügen**, wählen Sie im Dialogfenster **Aktion hinzufügen** die Aktion **Disclaimer anwenden**.
5. Klicken Sie **Auswählen und schließen** und danach **Speichern und schließen**.

Ihre konfigurierten Disclaimer-Regeln und -Vorlagen werden auf diese NoSpamProxy-Regel angewendet.

Ändern des SSL-Zertifikats

Wenn Sie ein spezielles eigenes SSL-Zertifikat zur Absicherung der Management-Webseite des Disclaimer-Tools nutzen möchten, so ist dies problemlos möglich. Hierzu muss das gewünschte Zertifikat mit dem privaten Schlüssel im Zertifikatsspeicher des Computerkontos auf der Intranetrolle unter **Eigene Zertifikate** hinterlegt sein.

Im **Trainingsvideo** zum Einbinden eines eigenen TLS-Zertifikats wird dies unter anderem für die Gatewayrolle erklärt. Die manuelle Rechteanpassung für die Intranetrolle ist jedoch nicht notwendig, dies wird vom folgenden Powershell-Kommando für Sie erledigt.

Wenn das Zertifikat sich im Zertifikatsspeicher auf der Intranetrolle befindet, führen Sie auf dieser als lokaler Administrator eine mit Admin-Rechten gestartete Powershell aus. In dieser setzen Sie dann folgendes Kommando ab:

```
Set-NspWebApiConfiguration -ShowCertificateSelectorUI
```

Es öffnet sich nun ein Fenster, in der Ihnen die verfügbaren Zertifikate angezeigt werden. Wählen Sie das gewünschte Zertifikat aus und bestätigen Sie die Auswahl. Starten Sie nun noch die Intranetrolle neu und Ihr Zertifikat ist auf der Disclaimer-Tool-Management-Webseite aktiv.

Anhang

Filter in NoSpamProxy

Filter bewerten E-Mails und beeinflussen dadurch das **Spam Confidence Level (SCL)** der E-Mails. Das SCL bestimmt, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis ein bestimmtes SCL übersteigt.

Wie funktionieren Filter?

Die Filter übernehmen bei der Prüfung der E-Mail die eigentliche Arbeit. Sie bewerten, wie stark die E-Mail ein bestimmtes Filterkriterium erfüllt und vergeben dafür Punkte. Sie können Ihr eigenes Regelwerk mit ganz verschiedenen Filterkombinationen aufstellen und die Regeln auf bestimmte Sender und Empfänger einschränken. So können Sie sehr individuell und flexibel auf Spam-Attacken reagieren.

Wenn Sie beispielsweise einen Wortfilter einsetzen, ist der Ausdruck *Viagra* sehr wahrscheinlich auf Ihrer Blockliste. Für ein Pharma-Unternehmen ist dieser Ausdruck jedoch nur sehr bedingt ein Spam-Kriterium. Wenn eine E-Mail ansonsten seriös erscheint oder von einem bekannten E-Mail-Sender kommt, kann das Auftreten des verdächtigen Wortes unter Umständen akzeptabel sein. Für jede E-Mail werden die einzelnen Filter der zutreffenden Regel ausgeführt. Die Filter bewerten und vergeben Malus- und Bonus-Punkte für die zu überprüfende E-Mail. Diese Punkte werden mit dem Multiplikator der Filter gewichtet und dann zu einem Gesamtwert addiert. Überschreitet dieser Wert den eingestellten Schwellenwert (SCL) der Regel, wird die E-Mail abgewiesen. Den Schwellenwert können Sie individuell für jede Regel einstellen.

Beispiel für eine Filterkonfiguration

Sie setzen einen Wortfilter, der E-Mails mit Viagra-Werbung blocken. Für ein Pharma-Unternehmen ist dieser Ausdruck jedoch nur sehr bedingt ein Spam-Kriterium. Mit NoSpamProxy Protection können Sie selbst entscheiden, ob Sie **Viagra** in den Wortfilter aufnehmen, oder ob Sie überhaupt einen Wortfilter einsetzen und wenn ja, wie stark Sie ihn mit dem Multiplikator gewichten. Wenn eine E-Mail ansonsten seriös erscheint oder von einem bekannten E-Mail-Sender kommt, kann das Auftreten des verdächtigen Wortes unter Umständen akzeptabel sein. Sie können auch festlegen, dass die Regel mit dem Wortfilter nur für bestimmte IP-Adressen oder Empfänger gilt; zum Beispiel nur für Absender mit einer bestimmten TLD (Top Level Domain) oder IP-Adressen aus einem bestimmten Subnetz.

Position	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.

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

In NoSpamProxy verfügbare Filter

Core Antispam Engine Filter

> **HINWEIS:** Dieser Filter ist verfügbar, wenn NoSpamProxy Protection lizenziert ist.

> Dieser Filter ist gültig für folgende Absender: Extern. Der Standard SCL-Wert bei einfachem Multiplikator ist 4.

Dieser Filter erstellt anhand festgelegter Kriterien einen Fingerabdruck der zu prüfenden E-Mail und vergleicht ihn mit den bereits bekannten Fingerabdrücken. Ist dieser bekannt, vergibt NoSpamProxy 4 SCL-Punkte. NoSpamProxy wird die E-Mail so bereits mit den Standardeinstellungen abweisen. Der Filter selbst verfügt über

keine weiteren Einstellungsmöglichkeiten. Lediglich über die Gewichtung mit Multiplikatoren kann der Administrator weiteren Einfluss auf das Filterergebnis ausüben.

CSA Certified IP List

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

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

Wenn sich der Absender einer empfangenen E-Mail in der CSA Certified IP List befindet, markiert der Filter CSA Certified IP List die E-Mail als vertrauenswürdig und vergibt negative SCL-Punkte. Siehe **Spam Confidence Level (SCL)**.

CSA Certified IP List aktivieren

1. Öffnen Sie eine Regel für eingehende E-Mails.
2. Wechseln Sie zur Registerkarte **Filter**.
3. Klicken Sie auf **Hinzufügen** und markieren Sie den Filter **CSA Certified IP List**.
4. Klicken Sie **Auswählen und schließen**.

> **HINWEIS:** Die Konfiguration des Filters nehmen Sie unter **Verbundene Systeme** vor.

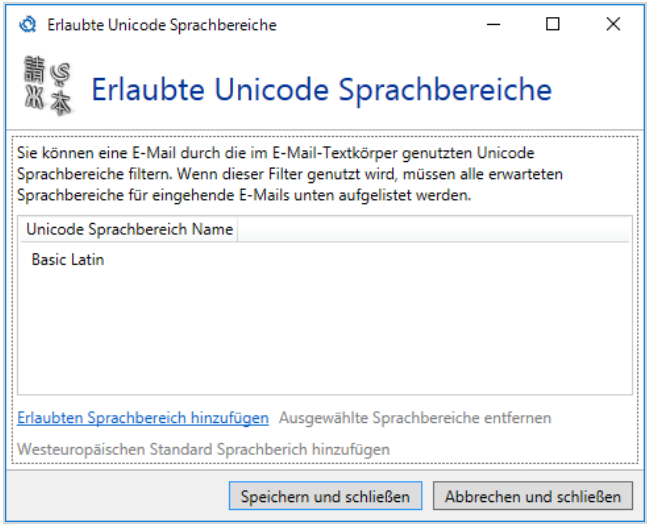
Erlaubte Unicode-Sprachbereiche

> Dieser Filter ist gültig für folgende Absender: Extern und Lokal.
> Standard SCL-Wert bei einfachem Multiplikator ist 4.

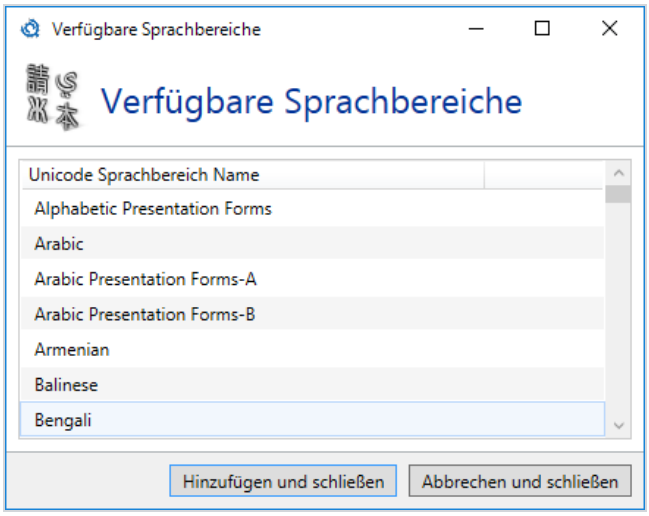
Spam-E-Mails kommen teilweise aus Sprachräumen, mit denen man üblicherweise keine Kommunikation unterhält. So kann zum Beispiel Spam eintreffen, der chinesische Schriftzeichen enthält. Dieser Filter kann E-Mails abblocken, in dem er alle enthaltenen Zeichensätze analysiert und die E-Mail nur passieren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

Anwendung

1. Fügen Sie den Filter Erlaubte Unicode Sprachbereiche an Ihre Regel an.



2. Fügen Sie nun alle Sprachbereiche, die in eintreffenden E-Mails verwendet werden können, zu den erlaubten Sprachbereichen hinzu.



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

32Guards

32Guards ist einerseits ein Filter, der die Bewertung des Spam Confidence Levels beeinflusst, andererseits eine Aktion, die Bedrohungen direkt temporär oder permanent abweisen kann. Siehe **32Guards**.

Realtime Blocklists

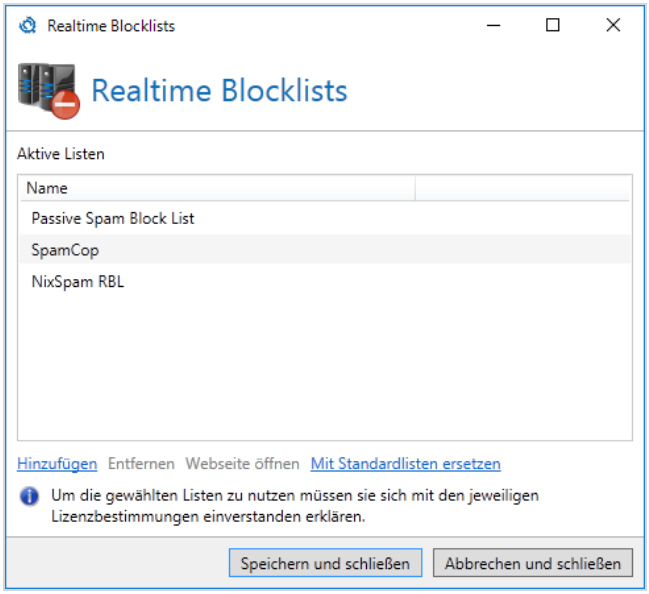
> Dieser Filter ist gültig für folgende Absender: Extern. Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Listen. Pro Treffer werden die in der Liste eingestellten SCL-Punkte vergeben.

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

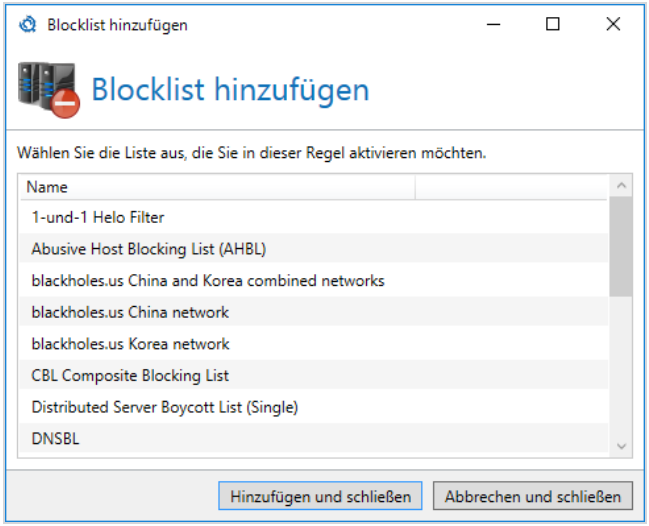
Anwendung

1. Fügen Sie den Filter an Ihre Regel an.
   Es öffnet sich der Dialog für die Konfiguration.

2. Klicken Sie **Hinzufügen**



3. Markieren Sie eine oder mehrere Listen aus, die Sie aktivieren möchten.



4. Klicken Sie **Hinzufügen und schließen**.
5. Klicken Sie **Speichern und schließen**.

> **TIPP:** Klicken Sie **Mit Standardlisten ersetzen**, um die aktuell ausgewählten Listen durch die von Net at Work empfohlenen Listen zu ersetzen.

Listen entfernen

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

> **HINWEIS:** Entfernte Listen werden nur aus der gerade editierten Regel entfernt. In den globalen Regeleinstellungen tauchen die Listen nach wie vor auf.

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

Reputationsfilter

Dieser Filter führt verschiedene Prüfungen auf dem E-Mail-Envelope, dem Inhalt der E-Mail sowie den Kopfzeilen aus. Durch einige der Prüfungen wird auch DKIM (DomainKeys Identified Mail) und SPF (Sender Policy Framework) analysiert. Abhängig von den Ergebnissen der einzelnen Prüfungen können SCL-Punkte vergeben werden, die individuell konfigurierbar sind. So können Sie die Bewertungen an die Anforderungen Ihres Unternehmens anpassen.

Titel	Beschreibung
Ungesicherte Verbindung	Prüft, ob die eingehende Verbindung durch TLS gesichert ist. Eine TLS-Verschlüsselung garantiert, dass sowohl Meta- als auch Inhaltsdaten zwischen E-Mail-Programm und Server beziehungsweise zwischen verschiedenen E-Mail-Servern verschlüsselt ausgetauscht werden. Die Datenschutz-Grundverordnung (DS-GVO) schreibt den Einsatz einer TLS-Verschlüsselung vor. Da Spammer sich häufig nicht an die DS-GVO halten, lässt dieser Test Rückschlüsse auf die Legitimität der E-Mail zu.

Titel	Beschreibung
Fehlender PTR-Eintrag	Prüft, ob sich die IP-Adresse zu einem Hostnamen zurück auflösen lässt. Ist dies nicht der Fall, so ist die Ursache ein fehlender PTR-Eintrag. PTR (Pointer Resource Records) ordnen im DNS einer IP-Adresse einen oder mehrere Hostnamen zu. Ist diese Zuordnung nicht möglich, deutet dies auf einen Missbrauchsversuch hin.
Dynamische Adresse vermutet	Prüft, ob der Hostname, der mit der IP-Adresse verknüpft ist, die IP-Adresse in Textform beinhaltet. NoSpamProxy prüft, ob die IP-Adresse aus einem dynamischen IP-Adressbereich stammt. Dies tritt häufig bei infizierten Rechnern auf, die als Spambot

Titel	Beschreibung
	agieren.
'Reverse lookup' schlug fehl	Prüft, ob der Hostname, der mit der IP-Adresse des E-Mail-Servers verknüpft ist, sich bei einem Gegentest ('Reverse lookup') zu dieser IP-Adresse zurück auflösen lässt. Ist dies nicht möglich, so deutet dies auf Spoofing hin, da mit hoher Wahrscheinlichkeit die tatsächliche Identität des Hosts verschleiert werden soll.
Fehlende IP-Adresse	Prüft, ob sich die 'MAIL FROM'-Domäne zu einer IP-Adresse auflösen lässt. Ist dies nicht möglich, so deutet dies auf einen Missbrauchsversuch hin, da die genannte Domäne höchstwahrscheinlich nicht existiert.

Titel	Beschreibung
SPF schlug fehl	Prüft, ob ein gültiger SPF-Eintrag vorhanden ist. Es wird geprüft, ob die IP-Adresse des E-Mail-Servers im DNS als berechtigter MTA (Mail Transfer Agent) hinterlegt ist, also für diese Domäne E-Mails versenden darf. Dieser Test vergibt nur Punkte, falls keine DMARC-Policy (siehe unten) aktiv ist.

Titel	Beschreibung
DKIM schlug fehl	Führt DKIM-Prüfungen für die jeweilige E-Mail aus. Diese Prüfungen bestehen aus der Überprüfung der Header-Signatur sowie des Hashes, der aus dem Body der E-Mail berechnet wird und ebenfalls signiert ist. Der öffentliche Schlüssel des Absenders ist im DNS hinterlegt. Dieser Test vergibt nur SCL-Punkte, falls keine DMARC-Policy aktiv ist.
DMARC-Ergebnis 'Quarantäne'	In der DMARC-Policy des Absenders ist für den Fall einer gescheiterten Überprüfung der Modus 'quarantine' definiert. Die DMARC-Prüfung beinhaltet zusätzlich die des sogenannten 'alignment' zwischen den von DKIM und SPF geprüften Domänen. Die Höhe der vergebenen Punkte hängt vom

Titel	Beschreibung
	angewandten DMARC-Ergebnis ab.
DMARC-Ergebnis 'Abweisen'	In der DMARC-Policy des Absenders ist für den Fall einer gescheiterten Überprüfung der Modus 'reject' definiert. Die DMARC-Prüfung beinhaltet zusätzlich die des sogenannten 'alignment' zwischen den von DKIM und SPF geprüften Domänen. Die Höhe der vergebenen Punkte hängt vom angewandten DMARC-Ergebnis ab.
Adresse ist nicht übereinstimmend	Prüft, ob die 'MAIL FROM'-Domäne und 'Header-From'-Domäne identisch sind ('alignment'). Dieser Test vergibt nur Punkte, falls keine DMARC-Policy aktiv ist.

HINWEIS: Sollte ein oder mehrere Tests vom Typ DMARC - also SPF, DKIM oder DMARC - fehlschlagen, wird dieses Ergebnis durch eine intakte ARC-Kontrollkette überschrieben. In einem solchen Fall werden keine Strafpunkte vergeben, die das **Spam Confidence Level (SCL)** erhöhen würden. Siehe **Vetrauenswürdige ARC-Unterzeichner**.

Titel	Beschreibung
Ungültige spitze Klammern	Prüft, ob der 'Header-From' eine spitze Klammer mit einer ungültigen E-Mail-Adresse enthält, was nicht RFC-konform ist. Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.
Fehlender Absender	Prüft, ob der 'MAIL FROM' leer ist und der 'Header-From' eine gültige E-Mail-Adresse enthält. Ist dies nicht der Fall, so deutet dies auf NDR Backscatter hin. Mobilgeräte und E-Mail-Programme wie Outlook zeigen nur den Anzeigenamen an, so dass

Titel	Beschreibung
	ein Missbrauch nicht erkannt wird.
Unternehmensdomäne in der E-Mail-Adresse	Prüft, ob die im 'Header-From' angegebene E-Mail-Adresse eine Unternehmensdomäne enthält. Ist dies der Fall, so deutet dies auf Identitätsdiebstahl hin, da dieser Test nur für eingehende E-Mails nutzbar ist und es sich deshalb um eine externe E-Mail handeln muss. Beachten Sie, dass ein solcher Fall auch auftreten kann, wenn ein externes E-Mail-System im Namen der Unternehmensdomäne sendet, aber nicht als **E-Mail-Server des Unternehmens hinzufügen** konfiguriert ist. > **BEISPIEL:** <xyz@netatwork.de>

Titel	Beschreibung
	HINWEIS: Eine gültige DKIM-Signatur für die 'Header-From'-Domäne setzt diesen Filter standardmäßig außer Kraft, so dass keine Maluspunkte vergeben werden. Um dieses Verhalten zu unterbinden, beachten Sie die Informationen unter **Aufheben der DKIM-Signatur im Reputationsfilter**.
Unternehmensdomäne im Anzeigenamen	Prüft, ob der Anzeigename eine E-Mail-Adresse enthält, deren Teil eine Unternehmensdomäne ist. E-Mail-Adressen, deren Teil eine Unternehmensdomäne ist, werden von Spammern als Teil von

Titel	Beschreibung
	Anzeigenamen verwendet, da in vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. Der Absender kann so eine falsche Identität vortäuschen. > **BEISPIEL:** "Uwe Ulbrich uwe.ulbrich@netatwork.de" <spam@spammer.de>
Unterdomäne einer Unternehmensdomäne in der E-Mail-Adresse	Prüft, ob eine Unterdomäne einer Unternehmensdomäne verwendet wird. Ist diese Unterdomäne legitim, wird der Test 'Unternehmensdomäne in der E-Mail-Adresse' angewendet. > **BEISPIEL:** <xyz@hr.netatwork.de>
Unterdomäne einer Unternehmensdomäne im Anzeigenamen	Prüft, ob der Anzeigename eine Subdomäne einer Unternehmensdomäne enthält. Domänen im Anzeigenamen werden von Spammern verwendet, da in

Titel	Beschreibung
	vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. Der Absender kann so eine falsche Identität vortäuschen. > **BEISPIEL:** "hr.netatwork.de" <spam@spammer.de>
Verschleierte Unternehmensdomäne in der E-Mail-Adresse	Wie der Test 'Unternehmensdomäne in der E-Mail-Adresse'. Zusätzlich wird hier geprüft, ob ASCII-Schriftzeichen in der Domäne verwendet wurden, die bestimmten Buchstaben ähnlich sehen. > **BEISPIEL:** <xyz@n3tatw0rk.de>
Verschleierte Unternehmensdomäne im Anzeigenamen	Wie der Test 'Unternehmensdomäne im Anzeigenamen'. Zusätzlich wird hier geprüft, ob ASCII-Schriftzeichen in der Domäne verwendet wurden, die bestimmten Buchstaben ähnlich sehen. Domänen im Anzeigenamen werden von Spammern verwendet,

Titel	Beschreibung
	da in vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. > **BEISPIEL:** "Uwe Ulbrich uwe.ulbrich@n3tatw0rk.de" <spam@spammer.de>
Unterdomäne einer verschleierten Unternehmensdomäne in der E-Mail-Adresse	Wie der Test 'Unterdomäne einer Unternehmensdomäne in der E-Mail-Adresse'. Zusätzlich wird hier geprüft, ob ASCII-Schriftzeichen in der Domäne verwendet wurden, die bestimmten Buchstaben ähnlich sehen. > **BEISPIEL:** <xyz@hr.n3tatw0rk.de>
Unterdomäne einer verschleierten Unternehmensdomäne im Anzeigenamen	Wie der Test 'Unterdomäne einer Unternehmensdomäne im Anzeigenamen'. Zusätzlich wird hier geprüft, ob ASCII-Schriftzeichen in der Domäne verwendet wurden, die bestimmten Buchstaben ähnlich

Titel	Beschreibung
	sehen. Domänen im Anzeigenamen werden von Spammern verwendet, da in vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. > **BEISPIEL:** Uwe Ulbrich uwe.ulbrich@hr.n3tatw0rk.de" <spam@spammer.de>
Mehrere E-Mail-Adressen	Prüft, ob der 'Header-From' mehr als eine E-Mail-Adresse enthält, was nicht RFC-konform ist. Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.
Domäne im Anzeigenamen abweichend von der E-Mail-Adresse	Prüft, ob eine im Anzeigenamen des 'Header-From' angegebene Domäne von der Domäne abweicht, die Teil der 'Header-From'-E-Mail-Adresse ist. Domänen im Anzeigenamen werden von Spammern verwendet, da in

Titel	Beschreibung
	vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. **BEISPIEL:** "service@paypal.com" <spam@spammer.de>

Titel	Beschreibung
Ungültiges '@'	Prüft, ob der 'Header-To' ein '@'-Zeichen enthält, das nicht Teil einer E-Mail-Adresse ist, was nicht konform mit RFC 5322 ist. Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.
Ungültige spitze Klammern	Prüft, ob der 'Header-To' spitze Klammern mit einer ungültigen E-Mail-Adresse enthält, was

Titel	Beschreibung
	nicht konform mit RFC 5322 ist. Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.
Fehlendes 'Header-To'	Prüft, ob der 'Header-To' eine Angabe enthält beziehungsweise vorhanden ist. Ist dies nicht der Fall, ist der Empfänger nicht bestimmbar. Angaben zum Empfänger sind in diesem Fall nur im 'Bcc'-Feld zu finden.
Fehlende Unternehmens-E-Mail-Adresse	Prüft, ob der 'Header-To' oder der 'CC' eine Unternehmens-E-Mail-Adresse enthält. Angaben zum Empfänger sind in diesem Fall nur im 'Bcc'-Feld zu finden.

Spamassassin Konnektor

Dieser Filter ist gültig für folgende Absender: Extern und Lokal. Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig vom Rückgabewert des SpamAssassin Daemon.

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

Er besteht aus Server (SpamD) und Client (SpamC). Der Filter von NoSpamProxy Protection agiert als SpamAssassin Client (SpamC) und funktioniert nur in Verbindung mit einem SpamAssassin Daemon (SpamD). Sie können den SpamAssassin Daemon auf einem System Ihrer Wahl installieren. Dies kann ein UNIX oder Windows-System sein. Auch der Betrieb direkt auf dem gleichen Server wie NoSpamProxy ist möglich.

HINWEIS: Stellen Sie sicher, dass NoSpamProxy das angefragte System auch erreichen kann. Oftmals sind Portfilter, IP-Routing und Firewalls zu konfigurieren.

Spam URI Realtime Blocklists

Dieser Filter ist gültig für folgende Absender: Extern und Lokal.
Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Listen. Pro Treffer einer Liste werden 2 SCL-Punkte vergeben.

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

Der "Spam URI Realtime Blocklists Filter" analysiert Links in E-Mails und PDF-Dokumenten und prüft, ob ein entsprechender Eintrag in diesen Listen vorliegt. Des Weiteren sucht er auch nach Adressen, die mit "www." anfangen und nicht als Links in E-Mails und PDF-Dokumenten auftauchen.

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

Bösartige Links werden dabei einer der folgenden Kategorien zugewiesen:

- Malware
- PhishingAndFraud
- Compromised
- CriminalActivity
- Botnets
- IllegalSoftware
- ChildAbuseImages
- SpamSites
- ParkedDomains

Wortübereinstimmungen

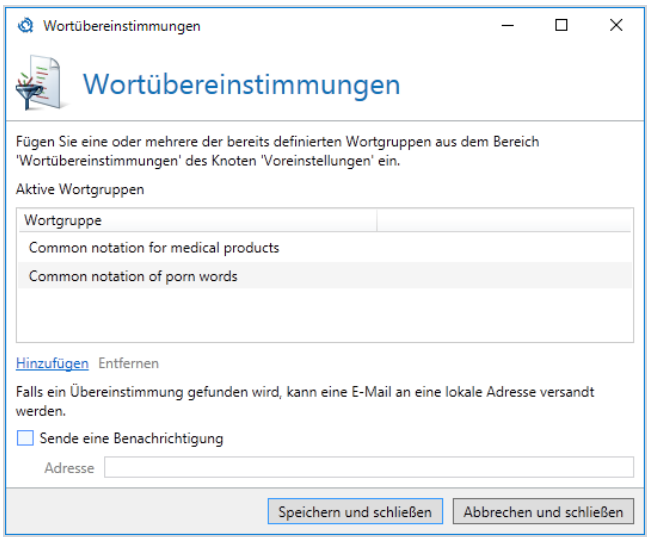
> Dieser Filter ist gültig für folgende Absender: Extern und Lokal. Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Wortgruppen. Pro Treffer werden die in der Wortgruppe eingestellten SCL-Punkte vergeben.

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

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

Anwendung

1. Fügen Sie den Filter an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration.

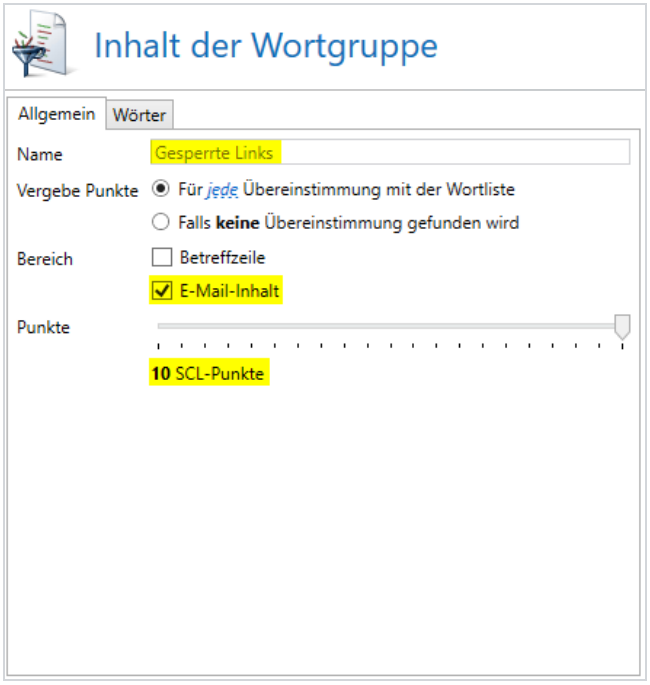


2. Klicken Sie **Hinzufügen**.
3. Wählen Sie die Wortgruppe aus, die Sie hinzufügen möchten und klicken Sie **Hinzufügen und schließen**.
4. **Optional** Geben Sie eine E-Mail-Adresse an, an die Benachrichtigungen gesendet werden sollen.
5. Klicken Sie **Speichern und schließen**.

Neue Wortgruppe hinzufügen

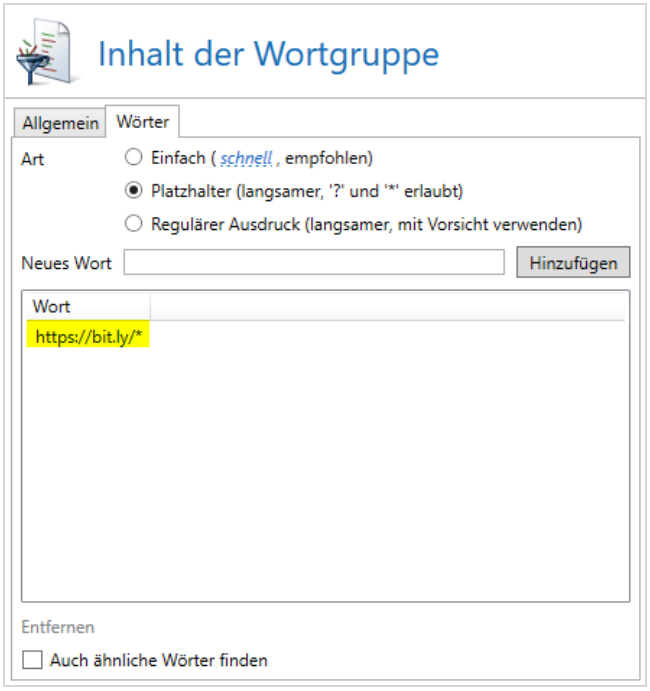
1. Gehen Sie zu **Konfiguration > Voreinstellungen > Wortübereinstimmungen**.
2. Klicken Sie **Hinzufügen**.
3. Bestimmen Sie auf der Registerkarte **Allgemein**
    - den Namen der Wortgruppe,
    - ob für Übereinstimmungen oder für nicht auftretende Übereinstimmungen Punkte vergeben werden,
    - den Bereich, auf den die Wortgruppe angewendet wird sowie

- die vergebenen SCL-Punkte.



4. Bestimmen Sie auf der Registerkarte **Wörter**
    - ob Sie nach exakten Treffern suchen wollen (einfach) oder Platzhalter oder Reguläre Ausdrücke einsetzen wollen,
    - die Wörter, die in der Wortliste enthalten sind und

- ob Sie auch nach ähnlichen Wörtern suchen wollen.



5. Klicken Sie auf **Fertigstellen**.

Aktionen in NoSpamProxy

Aktionen reagieren auf Filterergebnisse und führen die konfigurierten Aufgaben aus. Im Gegensatz zu den Filtern können Aktionen die E-Mails verändern, zum Beispiel Anhänge aussortieren. Zudem können Aktionen Filterergebnisse überstimmen. Beispiele hierfür sind Virenscanner oder die Aktion **Greylisting**.

Aktionen aktivieren

1. Öffnen Sie die Regel, die die Aktion enthalten soll.
2. Wechseln Sie zur Karteikarte **Aktionen**.
3. Klicken Sie **Hinzufügen**.
4. Markieren Sie die Aktion, die sie der Regel hinzufügen wollen.
5. Klicken Sie **Auswählen und schließen**.

Die Aktion wird der Regel hinzugefügt.

> **HINWEIS:** Falls die Regel konfiguriert werden muss, öffnet sich zuerst ein Konfigurationsdialog, nach dessen Beendigung die Aktion zu Ihrer Regel hinzugefügt wird.

Verfügbare Aktionen

Welche Aktionen in NoSpamProxy verfügbar sind, erfahren Sie unter **In NoSpamProxy verfügbare Aktionen**.

In NoSpamProxy verfügbare Aktionen

Die folgenden Aktionen sind in NoSpamProxy verfügbar:

Adressmanipulation

Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

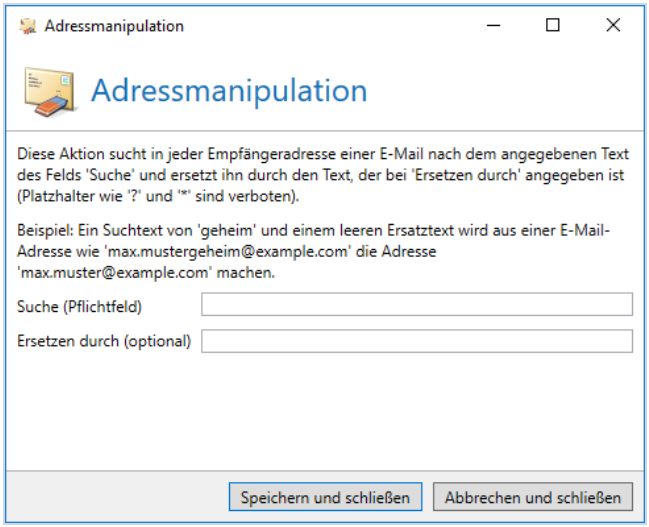
Diese Aktion verändert die Zieladresse beim Empfang einer E-Mail. So können Sie beispielsweise nach einem Namenswechsel der Firma alle E-Mails, die an die alte Adresse adressiert sind, an die neue Adresse umschreiben lassen. Ein zweiter Anwendungsfall ist die Definition einer "Geheimadresse". So können 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:

Position	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.

Anwendung der Aktion Adressmanipulation

1. Aktivieren Sie die Aktion Adressmanipulation in einer Regel (siehe oben).
   Es öffnet sich der Dialog für die Konfiguration.



2. Tragen Sie unter **Suche** den zu ersetzenden String aus der "Geheim"-Adresse ein, für die die Adressmanipulation aktiv werden soll.
3. Tragen Sie unter **Ersetzen** ein, mit welchem Text der Text aus dem Feld **Suche** ersetzt werden soll.
4. Klicken Sie **Speichern und schließen**.

> **TIPP:** Es ist 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

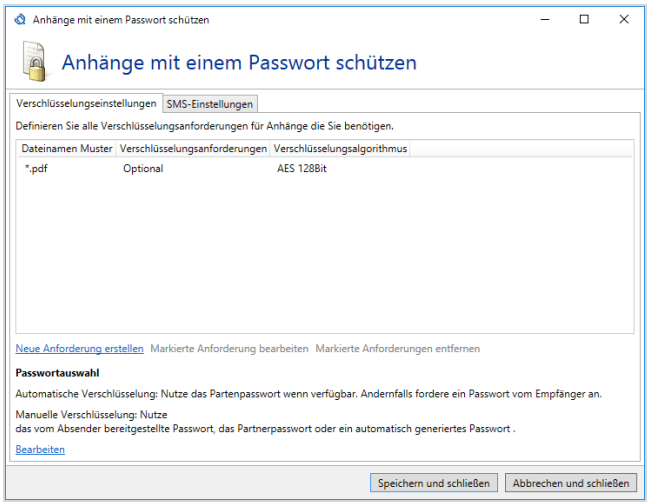
> Diese Aktion ist gültig für folgende Absender: Lokal.

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.

Anwendung der Aktion Anhänge mit einem Passwort schützen

- Fügen Sie die Aktion **Anhänge mit einem Passwort schützen** an Ihre Regel an.

  Es öffnet sich der Dialog für die Konfiguration.



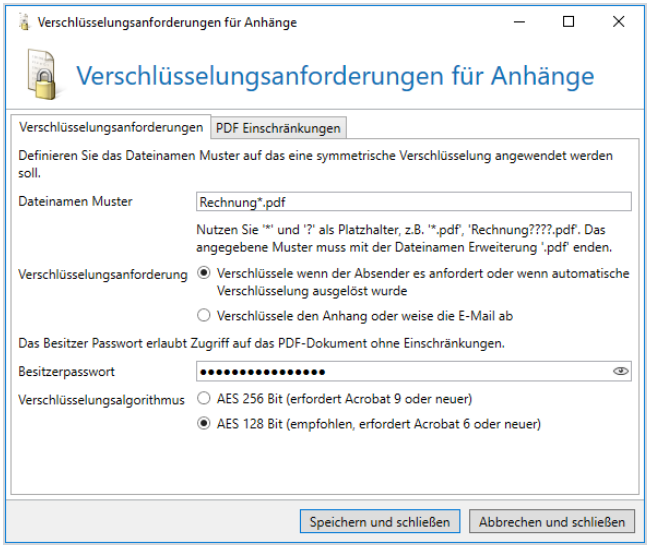
> **HINWEIS:** Beachten Sie die Hinweise zu nicht unterstützten Szenarien im Zusammenhang mit der Verwendung der automatischen Verschlüsselung.

HINWEIS:
Damit ein Passwort gültig ist, muss es mindestens zwei der folgenden Eigenschaften aufweisen:

- Es besteht aus mindestens acht Zeichen.
- Es enthält einen Kleinbuchstaben.
- Es enthält einen Großbuchstaben.
- Es enthält eine Ziffer.
- Es enthält ein Sonderzeichen.

Verschlüsselungsanforderung

1. Klicken Sie auf der Registerkarte **Verschlüsselungseinstellungen** auf **Neue Anforderung erstellen**.
   Der Dialog Verschlüsselungsanforderungen für E-Mail-Anhänge **öffnet sich.**



2. Tragen Sie das Dateinamenmuster für die zu verschlüsselnden PDF-Dateien ein.

> **TIPP:** Sie können an dieser Stelle die Platzhalter '*' und '?' benutzen.

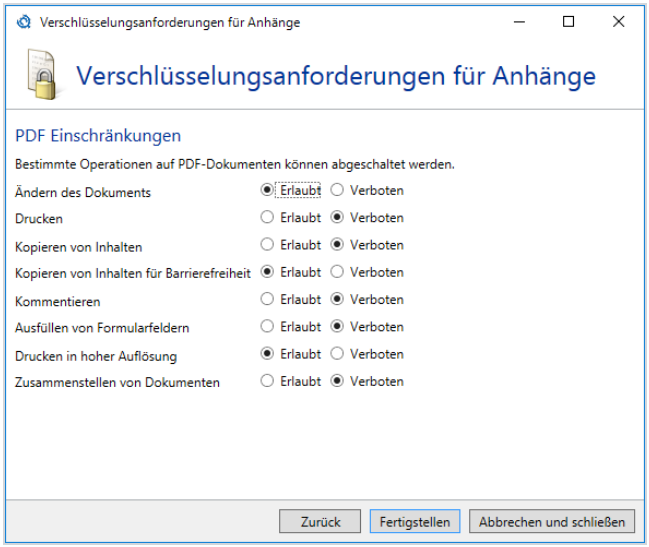
3. Geben Sie an, ob alle PDF-Anhänge, die dem angegebenen Dateinamenmuster entsprechen, verschlüsselt werden müssen oder ob sie unverschlüsselt versendet werden sollen, wenn es weder vom Benutzer noch durch die Regel gefordert ist.
4. Geben Sie ein Besitzerpasswort ein.

> **HINWEIS:** 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.

5. Geben Sie den Verschlüsselungsalgorithmus an.

> **TIPP:** Wir empfehlen AES mit 128 Bit für die optimale Balance aus Sicherheit und Kompatibilität.

6. Wechseln Sie zur Registerkarte **PDF-Einschränkungen**.



7. Konfigurieren Sie hier die unterschiedlichen Operationen auf geschützten PDF-Dokumenten.

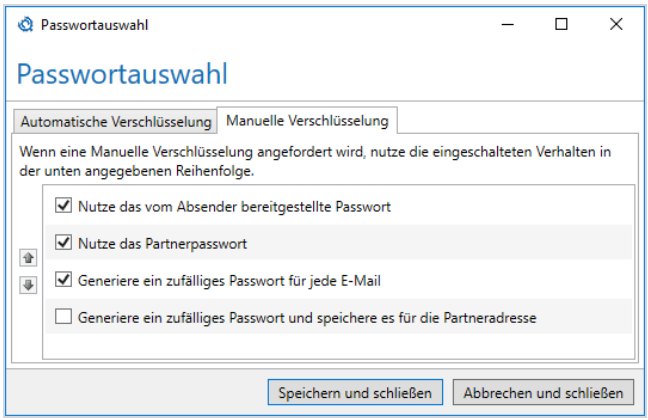
> **HINWEIS:** Hier gewählte Einschränkungen können durch das im ersten Schritt angegebene Besitzerpasswort aufgehoben werden.

8. Klicken Sie auf **Fertigstellen**.

Passwortauswahl

1. Klicken Sie **Bearbeiten**.
2. Definieren Sie, aus welchen Quellen die Passwörter bei der
    - automatischen Verschlüsselung sowie bei der

    - manuellen Verschlüsselung genommen werden.



> **HINWEIS:** 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.

3. Klicken Sie **Speichern und schließen**.
4. Wählen Sie unter **SMS-Einstellungen Sende eine SMS um den Empfänger automatisch zu benachrichtigen**.

> **HINWEIS:** Sie müssen einen SMS-Anbieter im Knoten SMS-Anbieter der Gatewayrolle konfiguriert haben, um diese Funktion zu nutzen.

5. Wählen Sie den Namen in der Liste **SMS Provider Profil** aus.
6. Erstellen Sie eine Textvorlage für die SMS.

> **HINWEIS:** Die maximal erlaubte Länge der Textvorlage beträgt 120 Zeichen.

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.

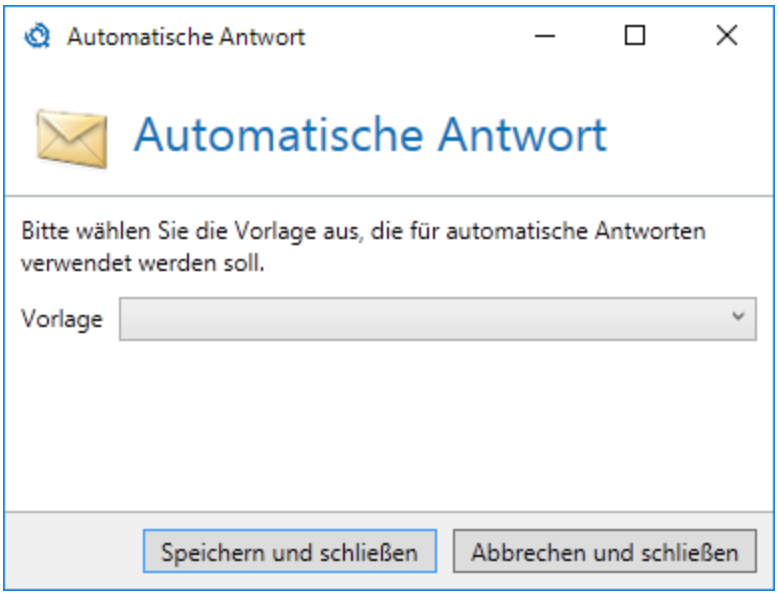
Diese E-Mail-Header können über das NoSpamProxy Outlook Add-In direkt beim Versenden von E-Mails auf dem Computer des Absenders gesetzt werden.

> **TIPP:** Unter Betreffkennzeichnungen erfahren Sie, wie Sie die Schlüsselworte für die PDF-Verschlüsselung in Betreffzeilen nutzen. Im Handbuch zum NoSpamProxy Outlook Add-In erfahren Sie alles über die Benutzung des Add-Ins.

Automatische Antwort

> Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

Diese Aktion sendet eine automatische Antwort an den Absender einer E-Mail. Der Text der E-Mail wird über eine Vorlage aus dem Templates-Ordner der Intranetrolle 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 Intranetrolle zu allen Gatewayrollen repliziert. Die Rollen müssen dafür nicht neu gestartet werden.



HINWEIS: Der Autoresponder antwortet auf jede E-Mail, die von der entsprechenden Regel verarbeitet wird. Somit ist es möglich, dass ein E-Mail-Absender mehrfach automatische Antworten erhält. Dieses Verhalten weicht von der Out-of-Office-Funktion in Microsoft Outlook/Exchange ab, die automatische Antworten nur einmal pro E-Mail-Absender versendet.

Anpassen der Antwort-Vorlagen

1. Wechseln Sie zu dem System, auf dem die Intranetrolle installiert ist.
2. Gehen Sie zu **C:\Program Files\NoSpamProxy\Intranet Role\Templates**.
3. Erstellen Sie eine Kopie der Datei **SampleAutoReply.cshtml** und speichern Sie diese unter einem neuen Namen.

4. Nehmen Sie die gewünschten Änderungen am Textteil der Datei vor.

> **HINWEIS:** Achten Sie darauf, dass Sie die HTML-Struktur nicht verändern. Ansonsten wird die Vorlage nicht erkannt.

5. Legen Sie die Datei im oben genannten Verzeichnis ab.
6. Wechseln Sie zum NoSpamProxy Command Center und starten Sie die Intranetrolle neu.

> Die Vorlagen werden nun neu eingelesen; der E-Mail-Verkehr wird nicht beeinträchtigt.

Anwenden der Aktion

1. Gehen Sie zu **Konfiguration > Regeln**.
2. Öffnen Sie die Regel, auf die der Autoresponder angewendet werden soll.
3. Wechseln Sie zur Registerkarte **Aktionen** und fügen Sie die Aktion **Automatische Antwort** hinzu.
4. Wählen Sie die gewünschte Vorlage über das Dropdown-Menü aus.
5. Speichern Sie die Regel.

Automatisch verschlüsseln

> Diese Aktion ist verfügbar, wenn NoSpamProxy Encryption lizenziert ist.

Diese Aktion ist für ausgehende Regeln verfügbar. Um sie nutzen zu können, werden die folgenden Aktionen benötigt:

- **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 jeweiligen Regel fehlen, klicken Sie **Notwendige Aktionen hinzufügen** und fügen Sie sie der Liste hinzu.

> **HINWEIS:** Die Konfiguration der Aktionen entspricht der Konfiguration der Standardregeln.

CxO-Betrugserkennung

Die CxO-Betrugserkennung dient der Erkennung von Phishing-Angriffen. Sie vergleicht den Absendernamen von eingehenden E-Mails mit den Namen von Unternehmensbenutzern. Gefälschte E-Mails, die im Namen von Vorgesetzten oder Mitarbeitern an Sie gesendet werden, werden so abgefangen.

Bei der Überprüfung werden unterschiedliche Varianten des Absendernamens in den Vergleich einbezogen:

- Erika Mustermann
- Mustermann Erika
- ErikaMustermann
- MustermannErika

Alle Unternehmensbenutzer, die Sie für die CxO-Betrugserkennung verwenden wollen, müssen Sie zuvor für den jeweiligen **Unternehmensbenutzer** aktivieren.

Disclaimer anwenden

Diese Aktion ist 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. Siehe **Disclaimer**.

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

DKIM-Signatur anwenden

Diese Aktion ist 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**.

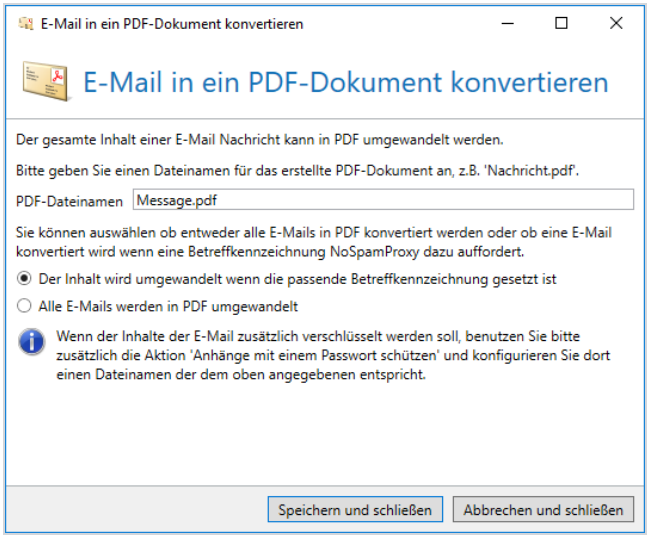
E-Mails in PDF-Dokumente konvertieren

Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

Diese Aktion wandelt den gesamten Inhalt einer E-Mail in ein PDF-Dokument um. 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.

Anwenden der Aktion

1. Öffnen Sie eine Regel für ausgehende E-Mails.
2. Wechseln Sie zur Registerkarte **Aktionen**.
3. Klicken Sie auf **Hinzufügen** und markieren Sie die Aktion **E-Mails in PDF-Dokumente konvertieren**.
4. Klicken Sie **Auswählen und schließen**.



5. Wählen Sie im Feld **PDF-Dateinamen** den Dateinamen des Anhangs aus, in den die E-Mail eingebettet werden soll.
6. Konfigurieren Sie , ob E-Mails in jedem Fall oder nur dann umgewandelt werden, wenn der Benutzer dies über das Setzen der entsprechenden Betreffkennzeichnung oder das Outlook Add- In bestimmt.

HINWEIS:
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.

HINWEIS: 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.

HINWEIS: Beachten Sie die Hinweise zu nicht unterstützten Szenarien im Zusammenhang mit der Verwendung der automatischen Verschlüsselung.

Greylisting

Diese Aktion ist gültig für folgende Absender: Extern.

Das Greylisting ist eine Vorsichtsmaßnahme gegen "verdächtige" E-Mails. Bleibt eine E-Mail knapp unter dem von Ihnen definierten Spam-Schwellwert, würde diese E-Mail ohne Greylisting als ausreichend gut bewertet werden.

Die Greylisting-Aktion lässt nun diese E-Mail nicht gleich durch, sondern lehnt sie temporär ab. Der einliefernde E-Mail-Server erhält eine Fehlermeldung, die ihn anweist, die E-Mail nach einiger Zeit erneut zu senden. Die E-Mail wird dann erneut zugestellt. Dabei kann eingestellt werden, ab wann der einliefernde Server einen zweiten Versuch starten darf.

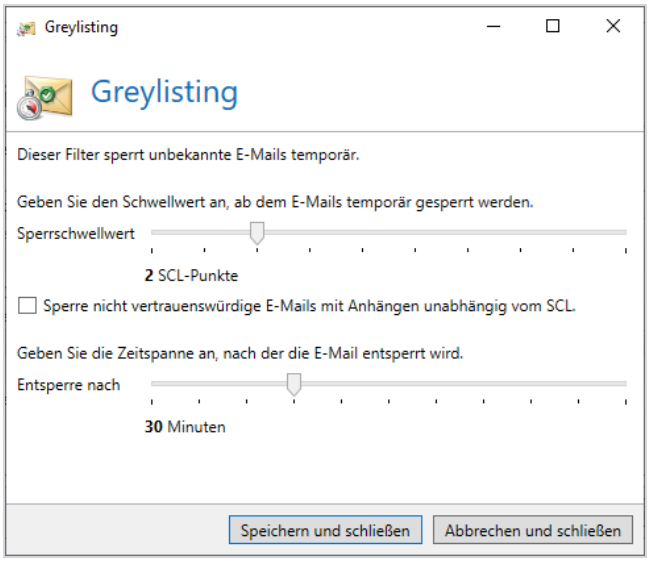
Die Aktion Greylisting basiert auf folgendem Prinzip: Ein Spammer scheut in der Regel die Mühe, eine zweite E-Mail zu senden. Ein normaler Absender hingegen wird nach einiger Zeit erneut die Zustellung versuchen. Beim zweiten Versuch wird nun diese Verbindung besser bewertet, so dass die E-Mail passieren kann. Den Schwellwert für die Anzahl an Malus-Punkten - ab dem eine eigentlich passierende E-Mail als verdächtig eingestuft wird - können Sie individuell einstellen.

Aktivieren der Aktion Greylisting

1. Öffnen Sie eine Regel für eingehende E-Mails.
2. Wechseln Sie zur Registerkarte **Aktionen**.
3. Klicken Sie auf **Hinzufügen** und markieren Sie die Aktion **Greylisting**.

4. Klicken Sie **Auswählen und schließen**.

   Der Konfigurationsdialog öffnet sich.



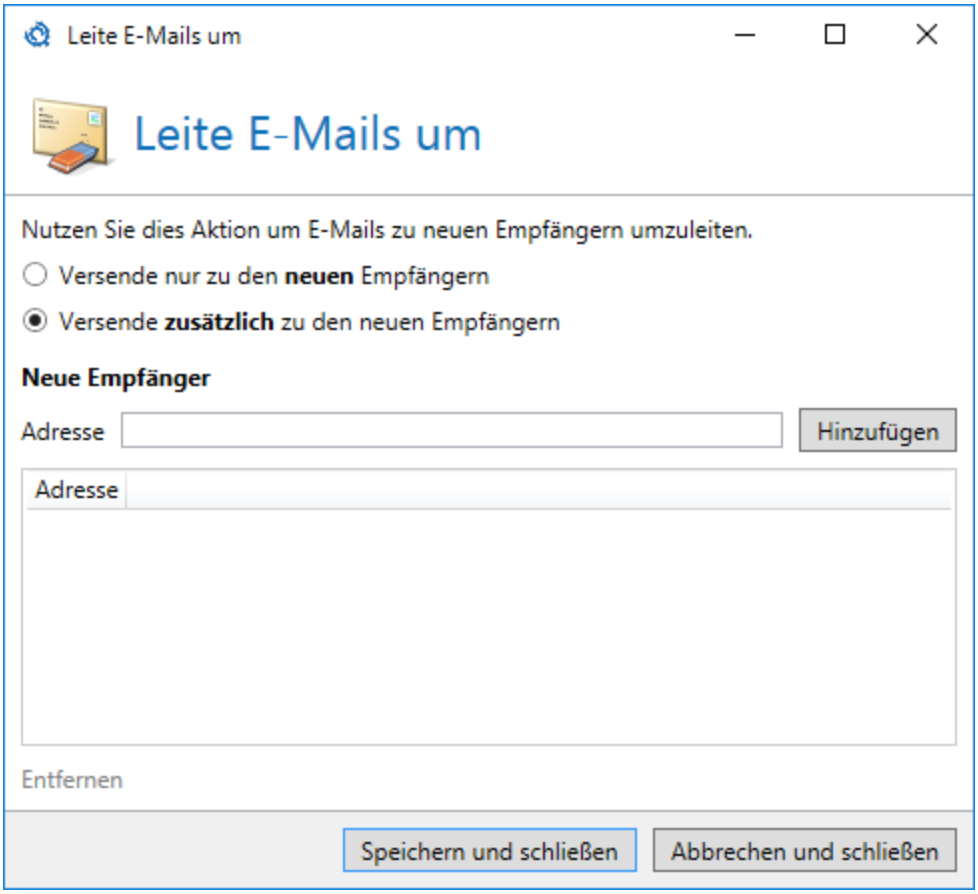
5. Geben Sie an,
   - ab welchem Schwellwert das Greylisting aktiv wird sowie
   - die Zeitspanne, nach der die E-Mail wieder entsperrt wird.
6. **Optional** Setzen Sie das Häkchen in Checkbox, wenn nicht vertrauenswürdige E-Mails mit Anhängen unabhängig vom Spam Confidence Level gesperrt werden sollen.

> **HINWEIS:** Der Greylisting-Schwellwert muss niedriger sein als der Spam-Schwellwert, da sonst das Greylisting nicht greift.

Leite E-Mail um

> Diese Aktion ist 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.

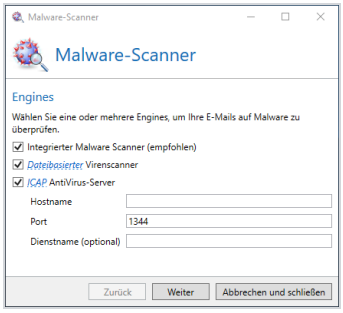


HINWEIS: Es muss mindestens eine Empfängeradresse in der Liste hinterlegt werden, um die Aktion nutzen zu können.

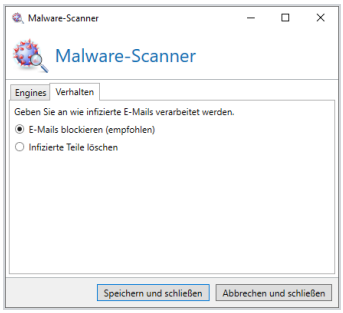
Malware-Scanner

Diese Aktion umfasst drei unterschiedliche Engines, die einzeln oder in Kombination miteinander genutzt werden können. Details zu den einzelnen Engines finden Sie weiter unten.

- Auf der Registerkarte **Engines** wählen Sie die Engine aus.



- Auf der Registerkarte **Verhalten** bestimmen Sie, wie E-Mails verarbeitet werden, falls eine oder mehrere Engines eine Infizierung festgestellt hat.



Integrierter Malware Scanner

Der integrierte Malware Scanner überprüft die Anhänge von ankommenden E-Mails.

> **HINWEIS:** Um Parallelbetrieb mit weiteren lokal installierten Virenscannern auf der Gatewayrolle zu gewährleisten, beachten Sie auch die Hinweise unter **Installierte On-Access-Virenscanner konfigurieren**.

Siehe auch

Melden von False Negatives und False Positives

Dateibasierter Virenscanner

Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

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

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

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

NoSpamProxy unter `\AntiSpam Role\Temporary Files \Netatwork.NospamProxy.Addins.Core.Actions.FileVirusScanAction` liegen.

Um (wiederkehrende) Probleme beim Zusammenspiel von installierten On-Access-Virenscannern zu beheben, konfigurieren Sie Ihren Virenscanner so, dass die **Verzeichnisse**

- C:\ProgramData\Net at Work Mail Gateway\Core Antispam Engine
- C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailQueues
- C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailsOnHold
- C:\Program Files\NoSpamProxy\Core Antispam Engine

auf allen Systemen mit installierter Gatewayrolle oder Web Portal vom Scan ausgeschlossen werden.

> **HINWEIS:** Beachten Sie, dass es sich bei dem Pfad um ein verstecktes Verzeichnis handelt.

Bei Servern mit installiertem Web Portal muss der folgende **Ordner** (Standard-Pfad zum Ablegen der Dateien für das Web Portal) ausgenommen werden:

- C:\Program Files\NoSpamProxy\Web Portal

Ansonsten kann es bei einigen Virenscannern vorkommen, dass der Zugriff auf das Web Portal stark verzögert wird und Kommunikationsprobleme auftreten.

Zusätzlich sollte eine Ausnahme auf die **Prozesse**

- amserver.exe sowie
- NoSpamProxy.CoreAntispamEngine.exe

eingestellt werden, falls der On-Access-Virenscanner dies ermöglicht.

> **TIPP:**
> Falls Sie den oben beschriebenen Pfad nicht finden, handelt es sich sehr wahrscheinlich um eine ältere NoSpamProxy-Installation, die bereits mehrfach aktualisiert worden ist. Prüfen Sie in diesem Fall bitte zunächst die Datei **C:\ProgramData\Net at Work Mail Gateway\Configuration\Gateway Role.config** und suchen Sie dort nach dem Eintrag **<storageLocation path=**.
>
> Dieser Pfad wird derzeit von der Gatewayrolle benutzt.
>
> Falls Sie den dateibasierten Virenscan in den Regeln aktiviert haben, stellen Sie ebenfalls sicher, dass Ihr Scanner so konfiguriert wird, dass infizierte Dateien und Archive komplett gelöscht oder in Quarantäne verschoben werden. Sollte der Scanner auf **Bereinigen** konfiguriert sein, kann NoSpamProxy oftmals nicht erkennen, dass diese vom installierten Scanner verändert wurden. Somit schlägt der “dateibasierte Virenscan” dann trotz erfolgreicher Erkennung durch NoSpamProxy fehl. Dies tritt insbesondere bei Archiven auf.

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

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

HINWEIS: Wie bei allen Virenscannern werden kennwortgeschützte ZIP-Dateien nicht überprüft und ohne weitere Prüfung weitergegeben.

ICAP Antivirus Server

Das Internet Content Adaptation Protocol (ICAP) ist ein Protokoll für das Weiterleiten von Inhalten für HTTP-, HTTPS- und FTP-basierte Dienste. Ein ICAP-Server empfängt Daten, die dann beispielsweise durch einen serverbasierten Virenscanner verarbeitet werden.

Wenn Sie die Aktion ICAP Antivirus Server auswählen, agiert NoSpamProxy als ICAP-Client. Die Daten werden dann von NoSpamProxy an Ihren ICAP-Server gesendet und durch diesen geprüft. Nach Abschluss des Prüfvorgangs sendet der ICAP-Server das Prüfergebnis an NoSpamProxy. In Abhängigkeit dieses Prüfergebnisses wird die konfigurierte Aktion ausgeführt.

HINWEIS: Für die Aktion ICAP Antivirus Server benötigen Sie Zugriff auf einen ICAP-Server.

32Guards

32Guards ist einerseits ein Filter, der die Bewertung des Spam Confidence Levels beeinflusst, andererseits eine Aktion, die Bedrohungen direkt temporär oder permanent abweisen kann. Siehe **32Guards**.

Qualifizierte Dokumentensignatur mit dem digiSeal server

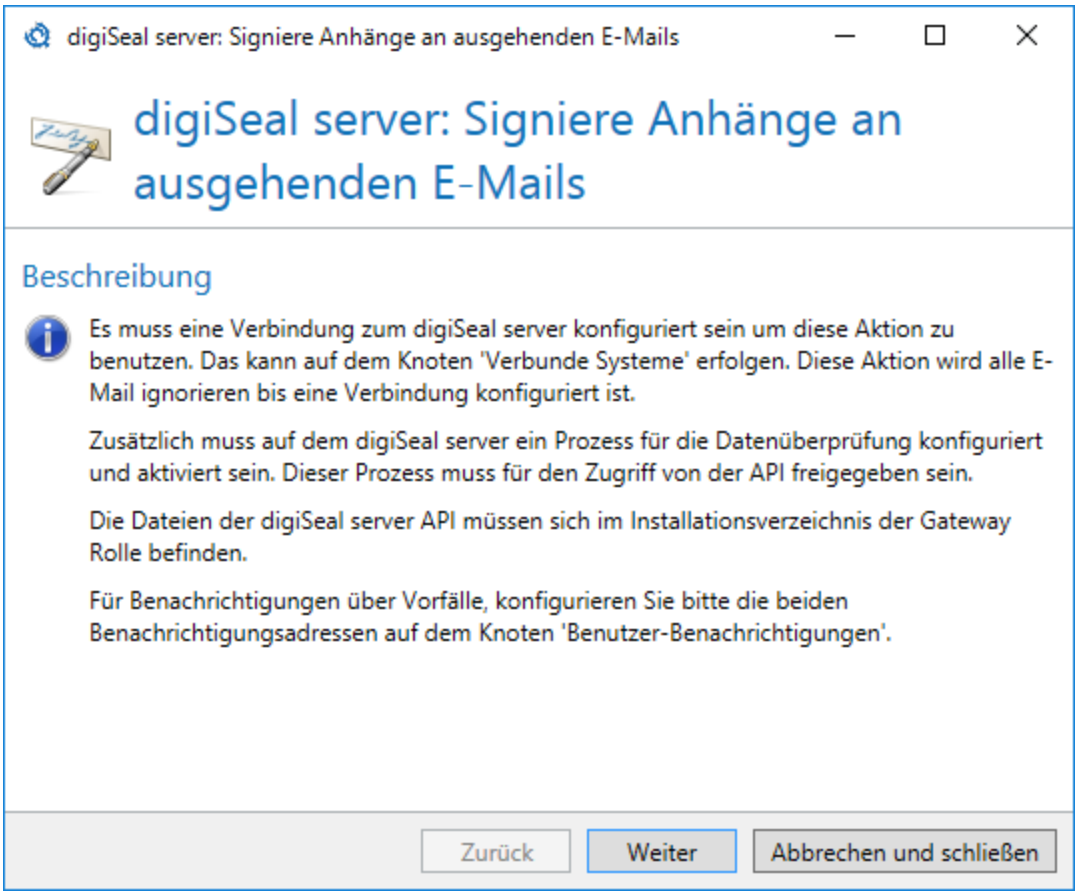
Die Aktionen der qualifizierten Dokumentensignatur werden benutzt, um zum Beispiel Rechnungen zu signieren oder den Empfang von signierten Dokumenten zu überprüfen. NoSpamProxy Encryption bietet diese Funktion im Verbund mit dem digiSeal server der secrypt GmbH an. Das heißt, dass für diese Funktion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

HINWEIS: Die Benutzung der Aktionen für die qualifizierte Signatur erfordert die Installation und Konfiguration eines digiSeal servers der **secrypt GmbH**. Zur Installation eines digiSeal servers kontaktieren Sie uns bitte unter **info@netatwork.de**. Die Verbindung zum digiSeal server richten Sie unter ein. Zusätzlich müssen die Dateien der digiSeal server API im Verzeichnis der Gatewayrolle liegen.

digiSeal server: Signiere Anhänge an ausgehenden E-Mails

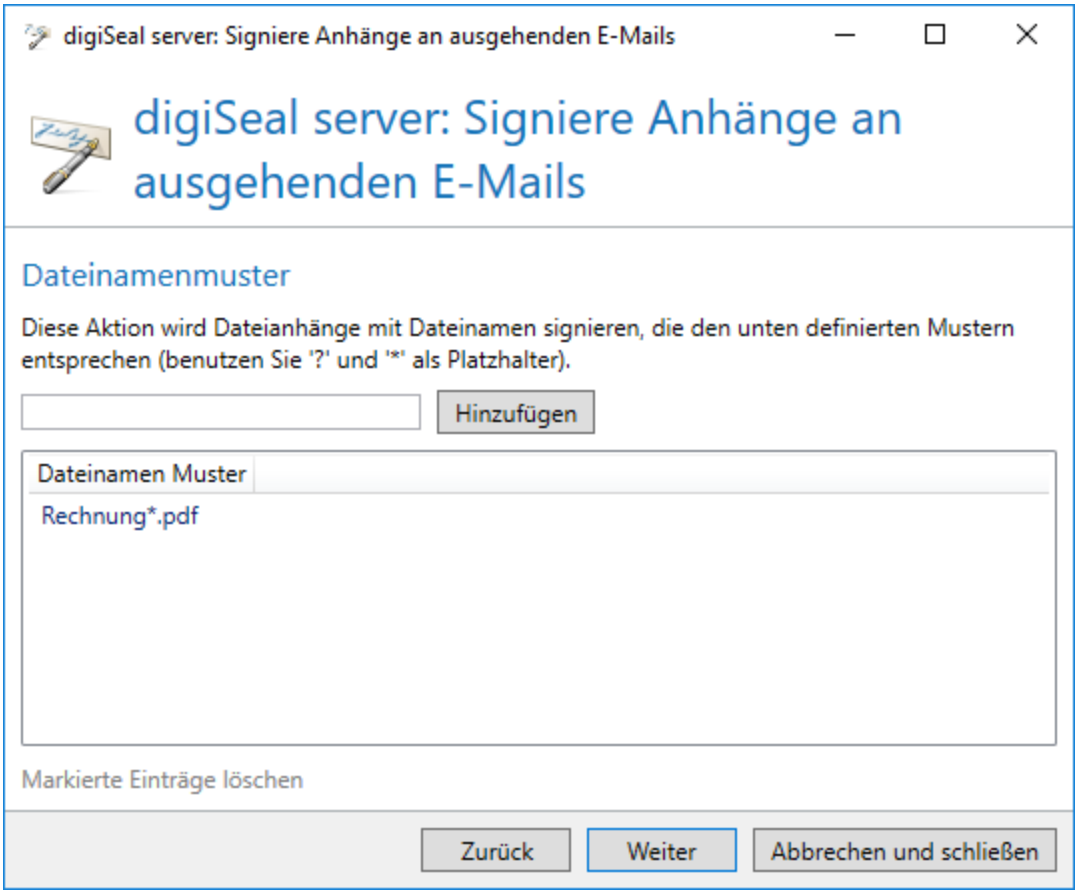
> **HINWEIS:** Diese Aktion ist gültig für folgende Absender: Lokal.

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



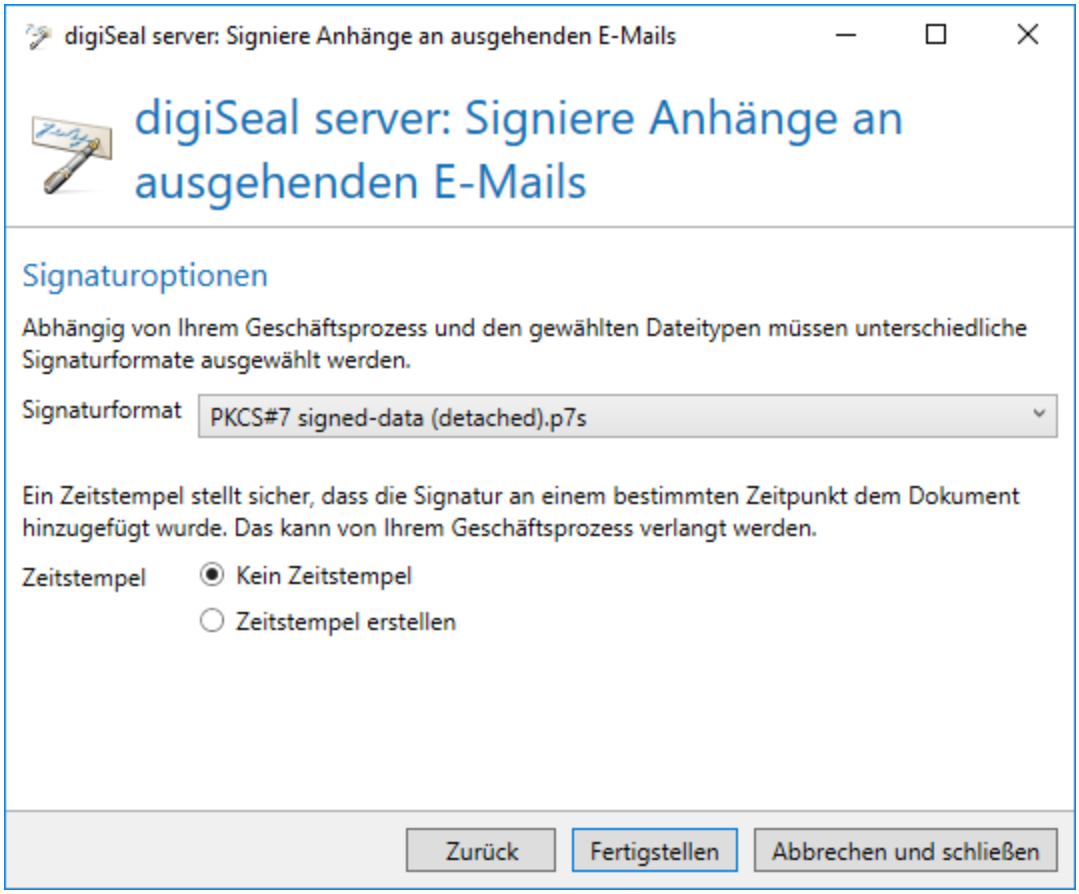
HINWEIS:
Bevor Sie diese Aktion konfigurieren, müssen Sie Folgendes sicherstellen:

- Die Verbindung zum digiSeal server muss konfiguriert sein.
- Es muss ein Prozess für die Datenüberprüfung auf dem digiSeal server definiert und aktiviert sein. Dieser Prozess muss für den Zugriff von der API freigegeben sein.
- Die digiSeal server API-Dateien müssen sich im Installationserzeichnis der Gatewayrolle befinden.



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

> **BEISPIEL:**
> Sie möchten Rechnungen mit Dateinamen (zum Beispiel "Rechnung Mai 2019.pdf" oder "Rechnung März 2018.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.



In Abhängigkeit des Geschäftsprozesses und der zu signierenden Daten müssen Sie nun ein Signaturformat auswählen. 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

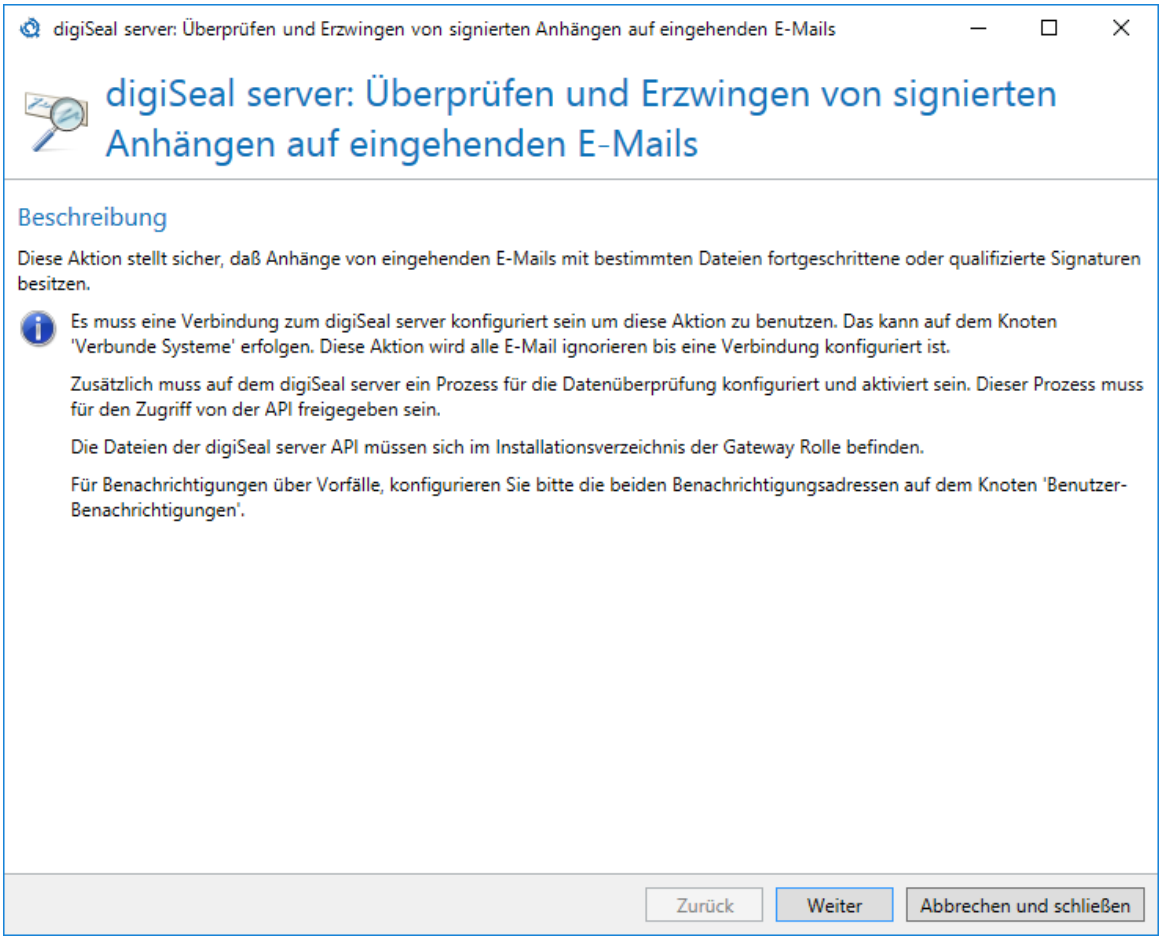
Zusätzlich zum Signaturformat können Sie auch einen optionalen Zeitstempel hinzufügen. Dieser entspricht dem Zeitpunkt, an dem das Dokument signiert wurde.

HINWEIS: 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

> **HINWEIS:** Diese Aktion ist 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.

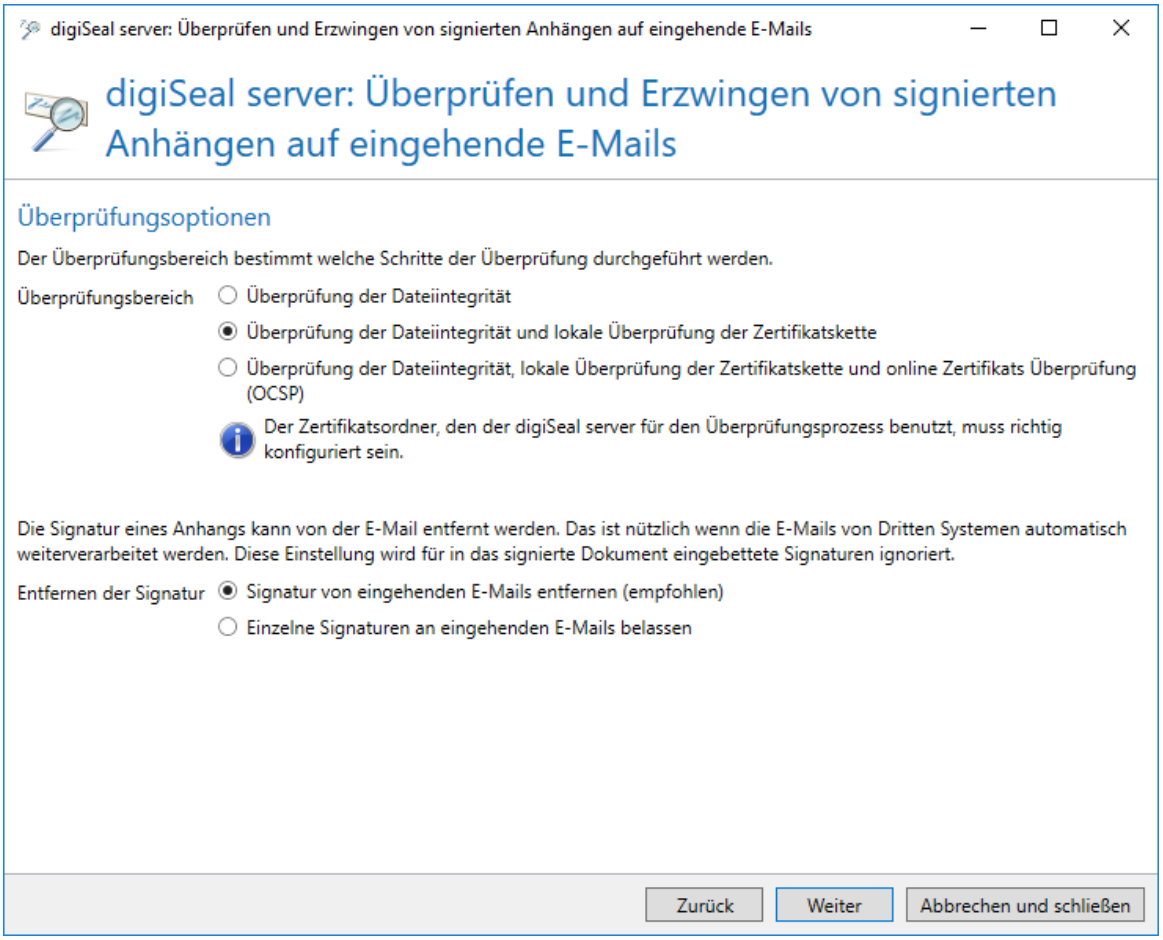

digiSeal server: Überprüfen und Erzwingen von signierten Anhängen auf eingehenden E-Mails
digiSeal server: Überprüfen und Erzwingen von signierten Anhängen auf eingehenden E-Mails
Beschreibung
Diese Aktion stellt sicher, daß Anhänge von eingehenden E-Mails mit bestimmten Dateien fortgeschrittene oder qualifizierte Signaturen besitzen.
Es muss eine Verbindung zum digiSeal server konfiguriert sein um diese Aktion zu benutzen. Das kann auf dem Knoten 'Verbunde Systeme' erfolgen. Diese Aktion wird alle E-Mail ignorieren bis eine Verbindung konfiguriert ist.
Zusätzlich muss auf dem digiSeal server ein Prozess für die Datenüberprüfung konfiguriert und aktiviert sein. Dieser Prozess muss für den Zugriff von der API freigegeben sein.
Die Dateien der digiSeal server API müssen sich im Installationsverzeichnis der Gateway Rolle befinden.
Für Benachrichtigungen über Vorfälle, konfigurieren Sie bitte die beiden Benachrichtigungsadressen auf dem Knoten 'Benutzer-Benachrichtigungen'.
Zurück
Weiter
Abbrechen und schließen

HINWEIS:
Bevor Sie diese Aktion konfigurieren, müssen Sie Folgendes sicherstellen:

- Die Verbindung zum digiSeal server muss unter dem Knoten Erweiterte Einstellungen konfiguriert worden sein.
- Auf dem digiSeal server muss 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 Installationsverzeichnis der Gatewayrolle befinden.

Für die Überprüfung von Dokumenten stehen drei Stufen zur Verfügung. 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).



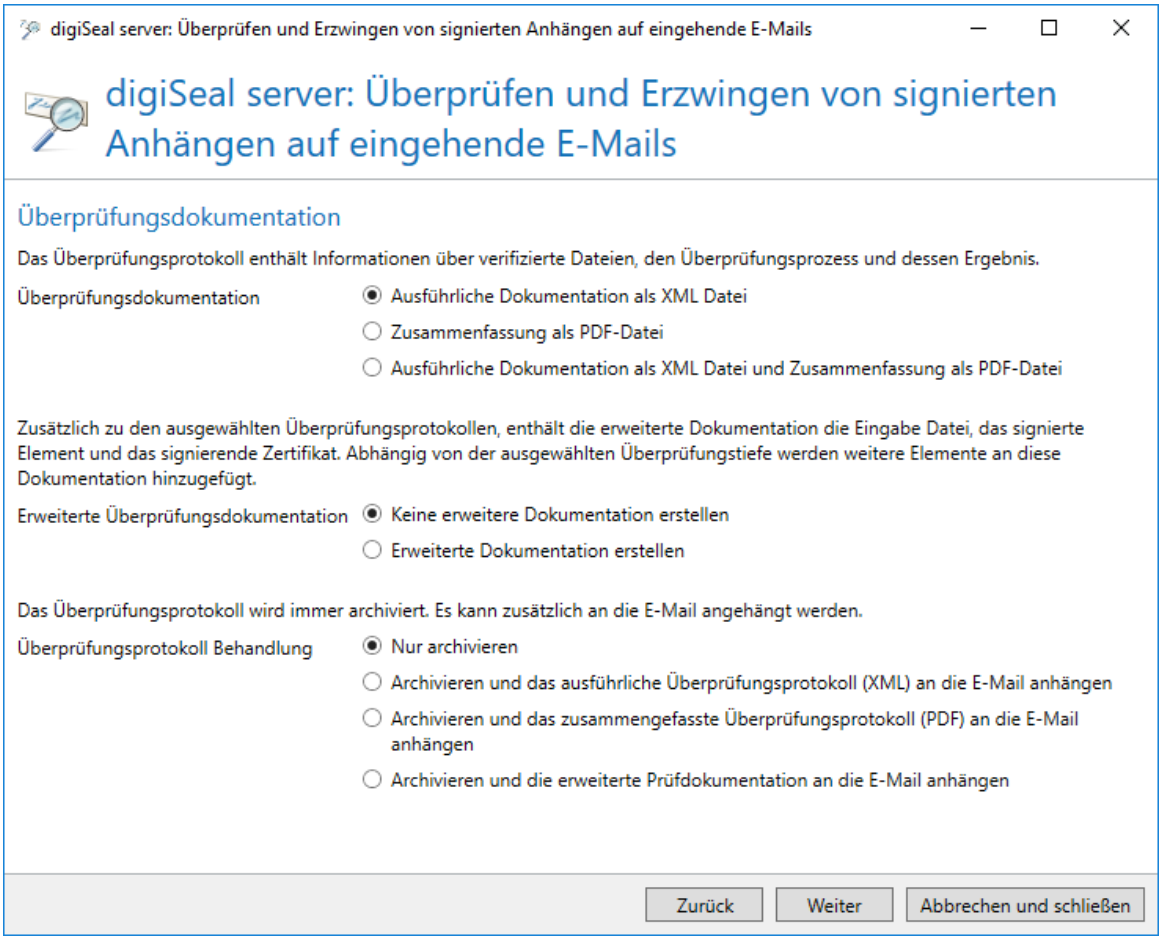
Die zweite und dritte Stufe schließt jeweils die Prüfungen aus den vorhergehenden Stufen mit ein.

> **TIPP:** 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.

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.

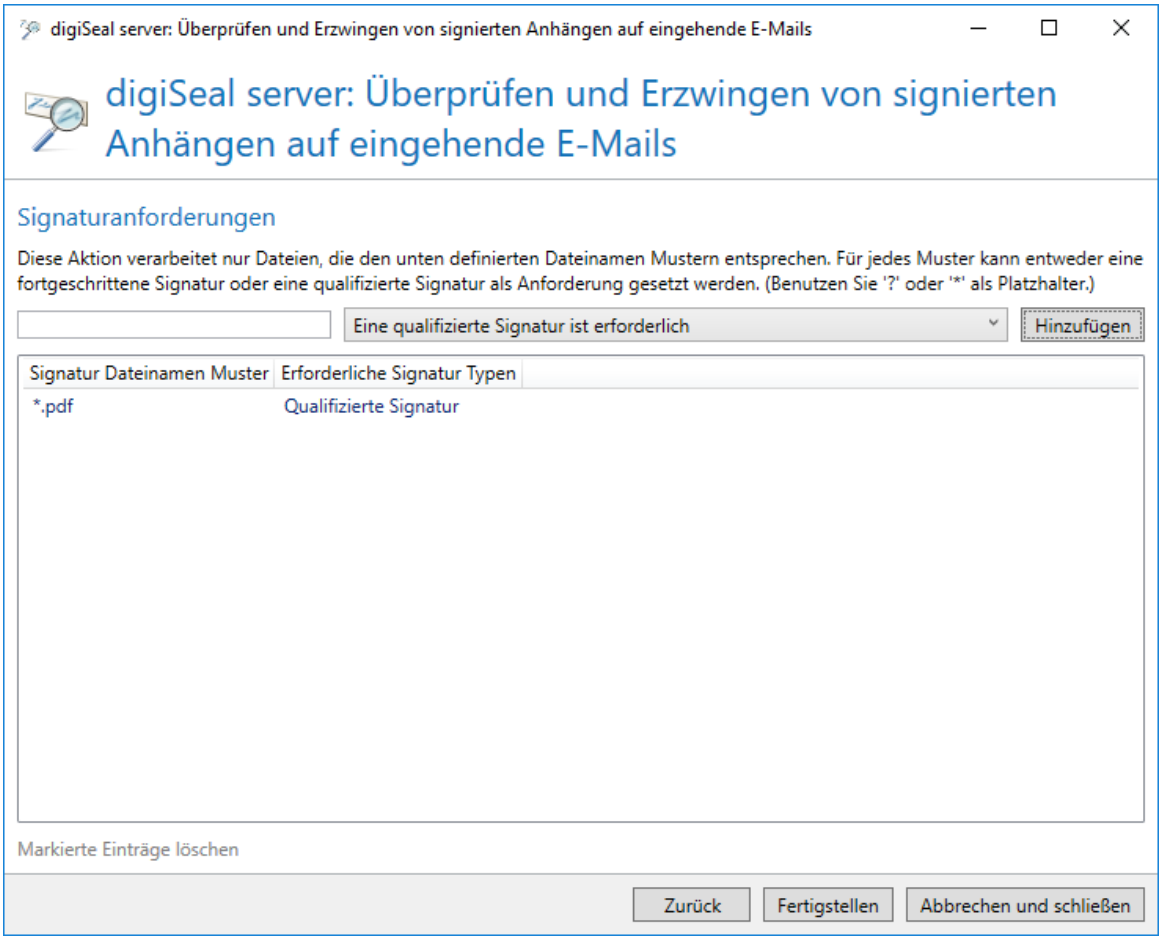
Das Überprüfungsprotokoll kann dabei aus einer ausführlichen XML-Datei bestehen und/oder einer Zusammenfassung der Überprüfung als PDF-Dokument. Zusätzlich zu diesem Protokoll können weitere Details der Überprüfung in der erweiterten Überprüfungsdokumentation festgehalten werden. Sie können zusätzlich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



HINWEIS: 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.

Abhängig vom Dateinamen können Sie für die Ihnen zugesandten, unterschiedlich signierten Dateien festlegen, welchem Signaturtyp die Signatur entsprechen muss:

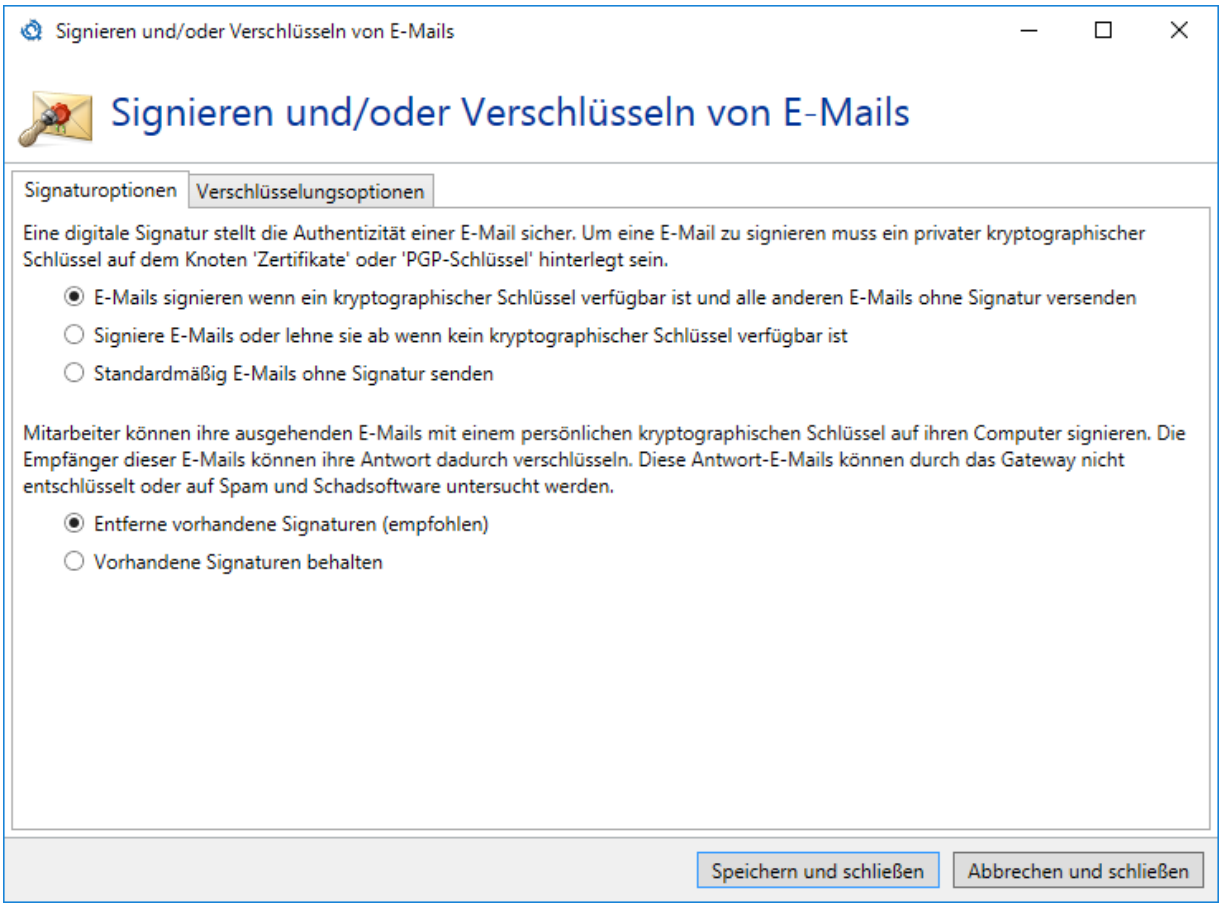
- Dokumente mit dem Dateinamensmuster: "EnergieRechnung*.pdf" müssen eine qualifizierte Signatur besitzen.
- Dokumente mit dem Dateinamensmuster: "TransportRechnung*.pdf" müssen eine fortgeschrittene Signatur besitzen.



Signieren und/oder Verschlüsseln von E-Mails

Diese Aktion ist gültig für folgende Absender: Lokal

Diese Aktion verschlüsselt oder signiert E-Mails mit den unter der Zertifikats- oder PGP-Schlüsselverwaltung vorhandenen kryptographischen Schlüsseln.



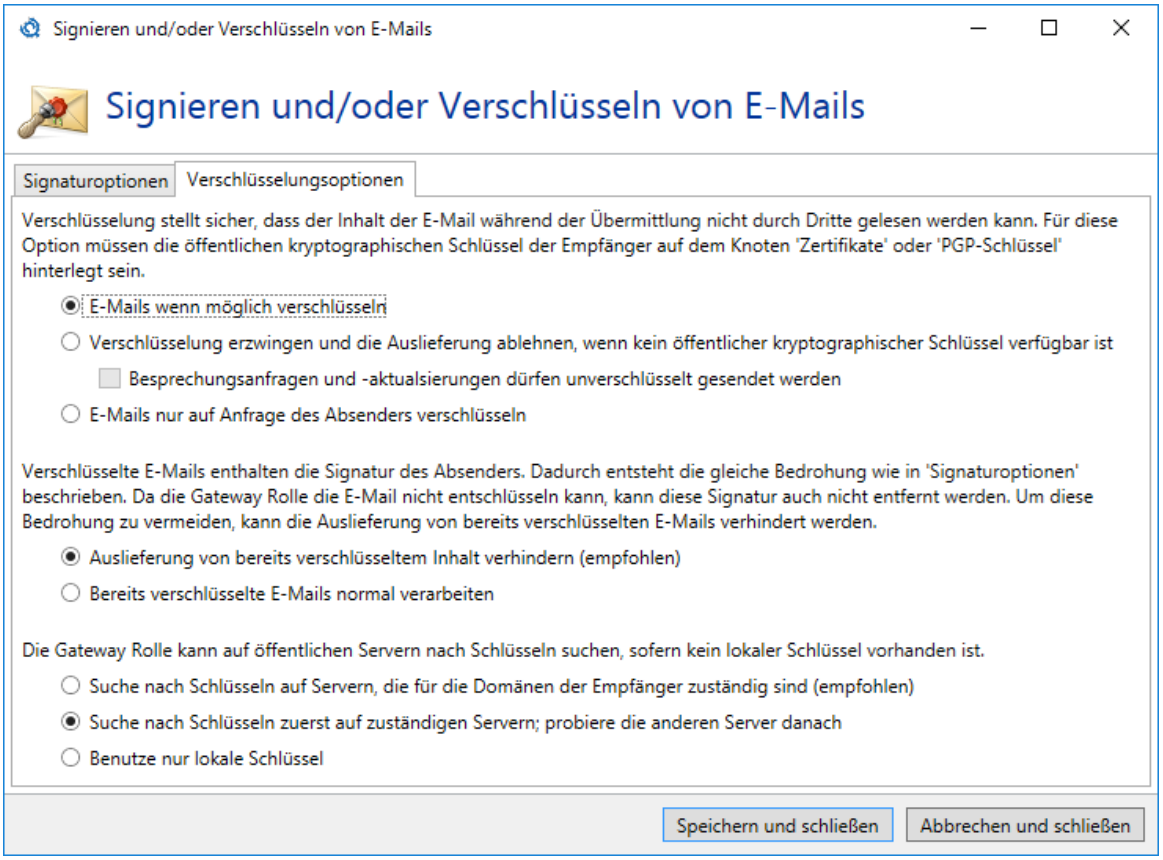
Digitale Signatur

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. 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 EMails verhindern.

HINWEIS: 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.

HINWEIS: Sie können hier auswählen, das auf allen konfigurierten Schlüsselservern gesucht wird. Nutzen Sie diese Einstellung bitte nicht auf der Standardregel für Nachrichten an externe

S/MIME- und PGP-Überprüfung sowie Entschlüsselung

Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

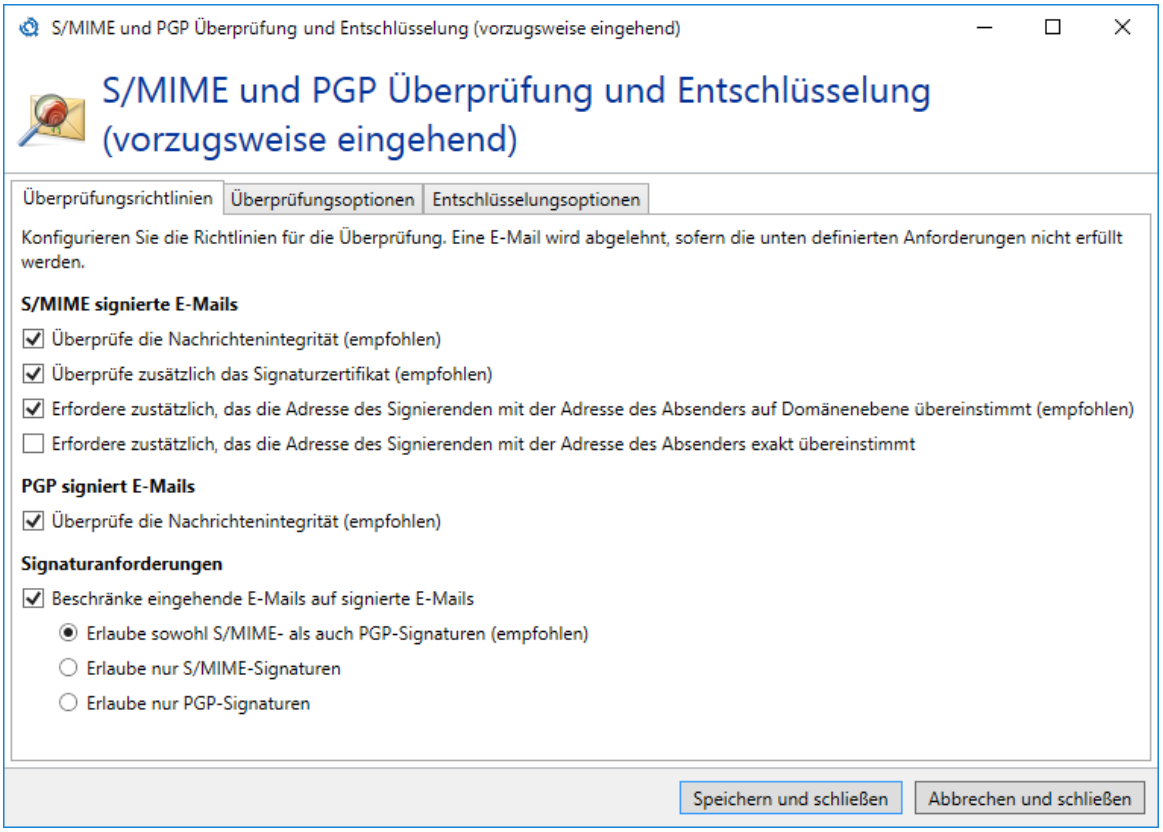
Bei E-Mails an Unternehmensempfänger kann die digitale Signatur automatisch validiert und der Inhalt entschlüsselt werden. Sie können dabei die Optionen für Validierung wie auch Entschlüsselung individuell einstellen.

Überprüfungsrichtlinien

Für die Signatur sind die folgenden Validierungsrichtlinien möglich:

- **S/MIME-signierte E-Mails**| Sie können verschiedene Stufen der Validierung auswählen, die jeweils aufeinander aufbauen.
- **PGP-signierte E-Mails**| Sie können Sie lediglich festlegen, ob die Nachrichtenintegrität überprüft wird.

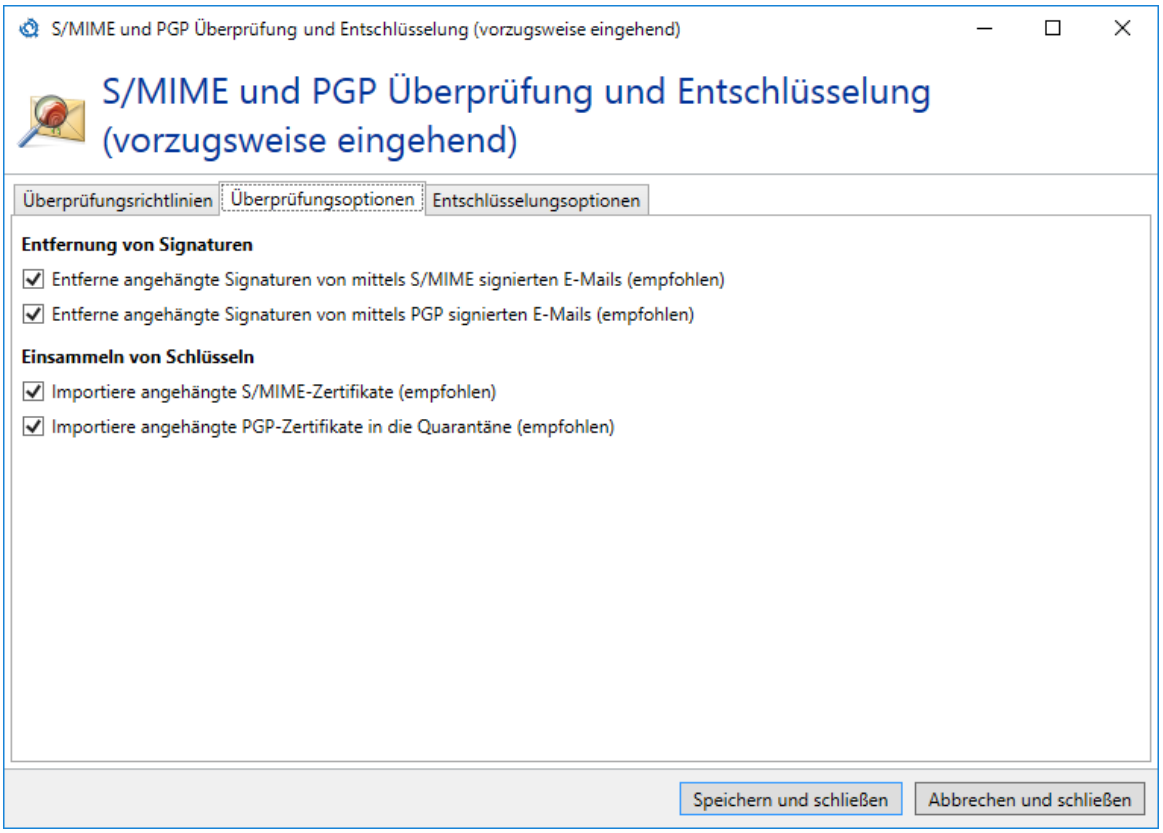
Des Weiteren können Sie festlegen, ob alle E-Mails an lokale Adressen signiert sein müssen. In diesem Fall können Sie zusätzlich die möglichen Signaturverfahren einschränken.



Überprüfungsoptionen

Hier legen Sie - jeweils für S/MIME und PGP - fest, 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 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.

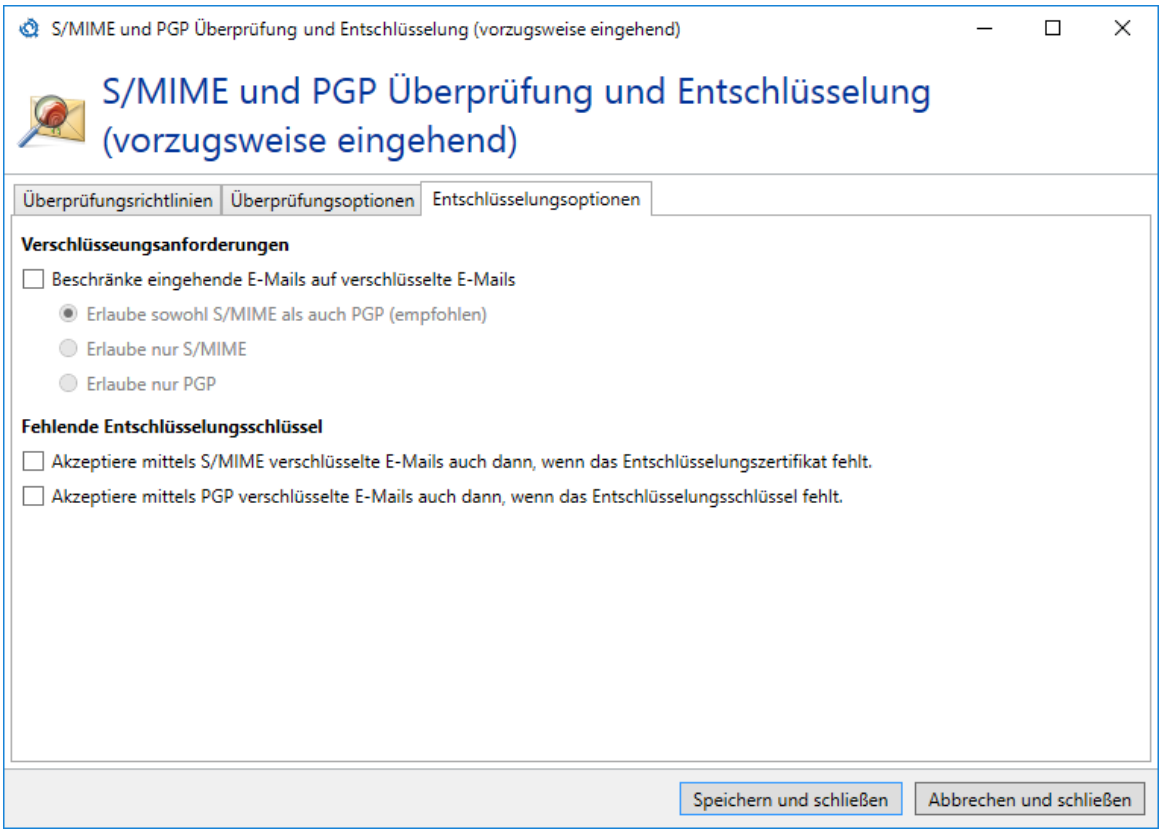


Entschlüsselungsoptionen

Auf der Registerkarte **Entschlüsselungsoptionen** 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.

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



URL Safeguard (Aktion)

Den URL Safeguard aktivieren

Um den URL Safeguard einzusetzen, müssen Sie ihn als Aktion einer Regel hinzufügen. Siehe **Schritt 5: Aktionen konfigurieren**.

Den URL Safeguard konfigurieren

Weitere Einstellungen nehmen Sie in den Standardeinstellungen für Partner oder für einzelne Partnerdomänen vor. Siehe **Standardeinstellungen für Partner** sowie **Partnerdomänen bearbeiten**.

Allowlisten anpassen

NoSpamProxy-Allowlist

1. Gehen Sie zu **Konfiguration > URL Safeguard > Allowlist für Domänen > NoSpamProxy-Allowlist**.
2. Klicken Sie **Bearbeiten**.
3. Setzen oder entfernen Sie das Häkchen bei **Lade die NoSpamProxy-Allowlist automatisch herunter und nutze sie**.
4. Klicken Sie **Speichern und schließen**.

Lokale Allowlist

1. Gehen Sie zu **Konfiguration > URL Safeguard > Allowlist für Domänen > Zusätzliche Domänen**.
2. Klicken Sie **Hinzufügen**.

3. Geben Sie eine oder mehrere Domänen in das Eingabefeld ein und klicken Sie **Hinzufügen**.
4. Klicken Sie **Speichern und schließen**.

Verberge interne Topologie

Diese Aktion ist 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.

Grundlagen

Absenderreputation

NoSpamProxy nutzt für die Bewertung der Absenderreputation ein mehrstufiges System, das insgesamt neun verschiedene Prüfungen umfasst. Zu den wichtigsten gehört die Prüfung von SPF, DKIM und DMARC, mit der sich zweifelsfrei erkennen lässt, ob eine E-Mail vom angegebenen Absender stammt.

- Das Sender Policy Framework (SPF) verhindert das Fälschen der Absenderadresse von E-Mails.
- DomainKeys Identified Mail (DKIM) sichert ausgehende E-Mails mit einer elektronischen Signatur. Siehe **DKIM-Schlüssel**.
- Mit einem DMARC-Eintrag kann die absendende Domain festlegen, welche Qualitätskriterien eine E-Mail von ihr aufweisen muss. NoSpamProxy wertet diese Angaben konsequent aus. Kombiniert werden diese Verfahren mit dem **Level of Trust**.

Einstellungen zur Bewertung der Absenderreputation nehmen Sie im **Reputationsfilter** vor.

TIPP:
In unserer Artikelserie im NoSpamProxy-Blog finden Sie weitere Informationen zu Absenderreputation und E-Mail-Sicherheit:

Absenderreputation und E-Mail-Sicherheit – Teil 1: Authenticated Received Chain (ARC)

Absenderreputation und E-Mail-Sicherheit – Teil 2: Sender Policy Framework (SPF)

Absenderreputation und E-Mail-Sicherheit – Teil 3: DomainKeys Identified Mail (DKIM)

Absenderreputation und E-Mail-Sicherheit – Teil 4: Domain-based Message Authentication, Reporting and Conformance (DMARC)

Absenderreputation und E-Mail-Sicherheit – Teil 5: DNS-based Authentication of Named Entities (DANE)

32Guards

32Guards ist einerseits ein Filter, der die Berechnung des Spam Confidence Levels beeinflusst, andererseits eine Aktion, die Bedrohungen direkt temporär oder permanent abweisen kann.

Die Bewertung von E-Mails durch 32Guards basiert auf der Auswertung einer Reihe von Indikatoren. Diese Auswertung ergibt am Ende eine finale Beurteilung der E-Mail. Beispiele für solche Indikatoren sind verdächtige Dateinamen oder gehäuftes Auftreten neuer beziehungsweise unbekannter URLs in sehr kurzer Zeit.

Diese Aktion/dieser Filter sorgt dafür, dass Metadaten zu E-Mail-Anhängen und URLs gesammelt und in die NoSpamProxy-Cloud hochgeladen werden. Es werden hierbei weder Dateiinhalte gesammelt noch auf diese zugegriffen. Durch 32Guards lassen sich Angriffe durch Spam und Malware schneller und zielsicherer erkennen und abwehren. Auf Basis dieser Metadaten erstellt 32Guards eine Gefahrenbewertung, die wiederum als Grundlage für weitere Aktionen in NoSpamProxy genutzt wird.

Es werden durch NoSpamProxy ausschließlich die folgenden Metadaten gesammelt:

Anhänge

- Dateiname
- Dateigröße
- Details zu den ersten zehn Dateien innerhalb von Archiven/zu maximal 50 Dateien bei verschachtelten Archiven (geordnet nach Dateityp): Dateiname, Hash-Wert, Größe, Anzahl, Größe ohne Komprimierung
- SHA-256-Hashwert
- TLSH-Hashwert
- MIME-Typ (wie durch NoSpamProxy erkannt)
- Informationen darüber, ob Malware im Anhang gefunden wurde

URLs

- Die vollständige URL
- Klassifikation der URL (Spam, Phishing, Malware)

E-Mails

- Quell-IP eingehender E-Mails
- Authentifizierte Domäne und Quelle (DKIM/SPF/S/MIME)
- Salted hash des local part der Header-From-Domäne und 'MAIL FROM'-Domäne eingehender E-Mails
- Salted hash des local part der Rcpt-Domäne und To/CC-Header-Domäne ausgehender E-Mails
- Message ID
- Ob es sich um eine automatisch generierte E-Mail handelt
- Status der Kontrollkette im Rahmen von Authenticated Received Chain (ARC)
- Status bezüglich der Certified IP List der Certified Senders Alliance (CSA)
- TLS-Zertifikat inklusive Gültigkeit, Vertrauensstatus, Thumbprint, Name der Domäne und Herausgeber
- Transaktions-ID
- Informationen darüber, ob die E-Mail eingehend (vertrauenswürdig/nicht vertrauenswürdig) oder ausgehend war
- Version des NoSpamProxy-Clients
- Version des angewendeten 32Guards-Datenmodells

Aus jedem der genannten Bereiche (Anhänge, URLs, E-Mails) fließt nur die jeweils schlechteste Bewertung in die Berechnung ein. Bewertungen aus unterschiedlichen Bereichen werden aufsummiert.

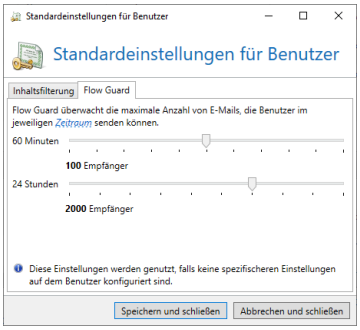
Updates auf NoSpamProxy 14 und höher

Bei Updates von älteren Versionen auf NoSpamProxy 14 und höher wird der **Filter 32Guards** automatisch einer Regel hinzugefügt, wenn vor dem Update die folgenden **beiden** Bedingungen erfüllt sind:

- Die **Aktion 32Guards** ist als Teil einer Regel konfiguriert und
- auf der **Registerkarte Filter** ist die Option **Überprüfen der E-Mail mit den unten angegebenen Filtern** ausgewählt.

Flow Guard

Flow Guard ermöglicht es, die Menge an ausgehenden E-Mails zu kontrollieren. So können ungewollte Massenmails – seien sie nun von unbedarften Benutzern erzeugt oder durch Malware ausgelöst – vor dem Versand erkannt und die Reputation der eigenen Domain geschützt werden. Dazu weist Flow Guard den NoSpamProxy-Benutzern Kontingente für ausgehende E-Mails zu. Wird der festgelegte Schwellwert überschritten, wird jede weitere ausgehende E-Mail abgewiesen.



Es gibt insgesamt zwei Schwellwerte, die pro Benutzer festgelegt werden können:

- Anzahl der E-Mails pro Stunde
- Anzahl der E-Mails insgesamt pro Tag

TIPP: Sie können die Schwellwerte auch auf Basis von AD-Gruppenmitgliedschaften zuweisen.

HINWEIS:
NoSpamProxy erlaubt es, zum Versenden E-Mail-Adressen zu verwenden, die keinem Benutzer zugeordnet sind. In diesen Fällen geht Flow Guard folgendermaßen vor:

- Wenn der E-Mail-Adresse kein Benutzer zugeordnet ist, wird pro E-Mail-Adresse gezählt.
- Wenn einem Benutzer mehrere E-Mail-Adressen zugeordnet sind, werden die E-Mails von allen E-Mail-Adressen zusammengerechnet.

Schwellwerte festlegen

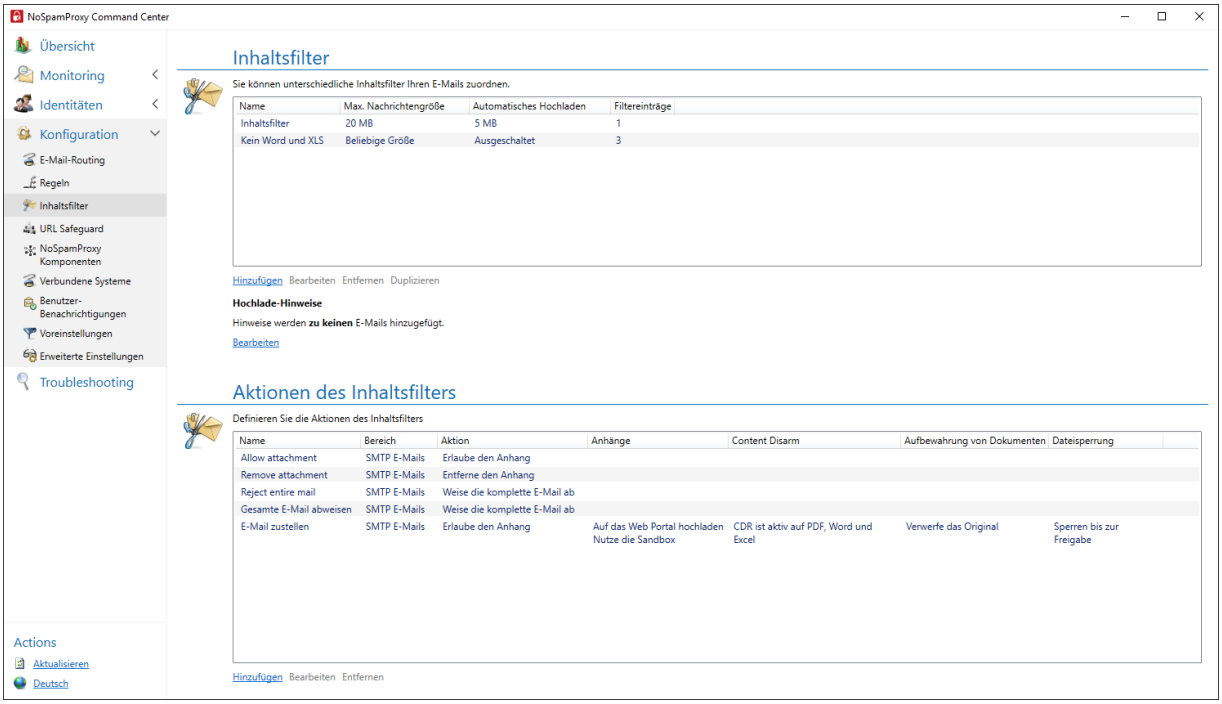
Sie legen die Schwellwerte entweder global für alle Benutzer oder für einzelne Unternehmensbenutzer fest. Dazu müssen Sie

- die **Standardeinstellungen für Benutzer konfigurieren** beziehungsweise
- die Einstellungen unter **Identitäten > Unternehmensbenutzer** für den jeweiligen **Unternehmensbenutzer** konfigurieren.

Inhaltsfilter

Dieser Bereich ist verfügbar, wenn Sie die entsprechende Lizenz erworben haben.

Inhaltsfiltersets ermöglichen das Ausführen von Inhaltsfilteraktionen auf Basis von Bedingungen. Sowohl die Inhaltsfilteraktionen als auch die Bedingungen werden in Inhaltsfilterset-Einträgen konfiguriert. Ein Inhaltsfilterset kann mehrere Inhaltsfilterset-Einträge enthalten.



Wie ein Inhaltsfilter funktioniert

Beim Anlegen von Inhaltsfiltern bestimmen Sie

- die allgemeinen Anweisungen zur Behandlung von Anhängen und den Umgang mit Archiven,
- die Inhaltsfilteraktionen und
- die **Bedingungen definieren**, unter denen die Inhaltsfilteraktionen ausgelöst werden.

Sie konfigurieren sowohl Inhaltsfilteraktionen als auch Bedingungen, indem Sie einem Inhaltsfilter einen oder mehrere Inhaltsfiltereinträge zuweisen. Siehe **Inhaltsfilter erstellen** sowie **Inhaltsfilteraktionen anlegen**.

Verwandte Schritte

Inhaltsfilter zuordnen| Um einen Inhaltsfilter anzuwenden, müssen Sie ihn unter **Partner** oder **Unternehmensbenutzer** zuordnen. Siehe **Inhaltsfilter erstellen**.

Inhaltsfilteraktionen anlegen| Inhaltsfilteraktionen sind Aktionen, die auf Anhängen sowie den sie enthaltenen E-Mails angewendet werden. Sie werden durch die Erfüllung von Bedingungen ausgelöst. Siehe **Inhaltsfilteraktionen anlegen**

Bedingungen definieren| Damit Inhaltsfilteraktionen ausgelöst werden, müssen von Ihnen definierte Bedingungen erfüllt sein. Siehe **Bedingungen definieren**.

Level of Trust

Das Level-of-Trust-System ist ein mehrschichtiges Konzept, das die Vertrauenswürdigkeit einer Kommunikationsbeziehung oder einer Domäne beurteilt.

Den größten Einfluss auf das Vertrauen hat die Qualität der Verbindungshistorie. Eine verlässliche und dauerhafte Kommunikationsbeziehung sorgt dafür, dass der Level-of-Trust-Wert steigt; eine unzuverlässige und fragmentierte Kommunikationsbeziehung sorgt dafür, dass der Level-of-Trust-Wert sinkt.

NoSpamProxy bezieht verschiedene Kriterien in Berechnung des Wertes ein:

Domänenbeziehung| Regelmäßige ausgehende E-Mails an eine bestimmte E-Mail-Domäne werden belohnt. Sogenannte Freemailer sind von dieser Regelung standardmäßig ausgeschlossen. Siehe **Level-of-Trust-Konfiguration**.

Adressbeziehung zwischen Absender und Empfänger| Ausgehende E-Mails an bestimmte externe Adressen werden mit einem hohen Vertrauensbonus belohnt. Siehe **Level-of-Trust-Konfiguration**.

Kombination aus Absender, Betreff und Domäne| Antwort-E-Mails werden belohnt, wenn der Betreff und die Domäne unverändert sind.

Message ID| Die in E-Mail-Headern enthaltenen Message IDs werden – ähnlich wie Antwort-E-Mails – belohnt, wenn Sie unverändert sind.

Zustellbenachrichtigungen| Gültige Benachrichtigungen werden belohnt, ungültige Benachrichtigungen werden bestraft. Siehe **Level-of-Trust-Konfiguration**.

NoSpamProxy bewertet eine E-Mail als vertrauenswürdig, wenn einer der oben beschriebenen Boni mindestens 40 Punkte beträgt. Voraussetzung dafür ist, dass die unter **Level of Trust** genannten Bedingungen erfüllt sind. Wenn Sie sicherstellen wollen, dass E-Mails eines bestimmten Partners zugestellt werden, stellen Sie den Vertrauenswert fest auf 40 oder höher ein. Siehe **Partnerdomänen bearbeiten**. Wir empfehlen Ihnen außerdem, eine Form der Authentifizierung zur Vorbedingung für alle Boni zu machen. Siehe **Authentifizierung als Vorbedingung für alle Boni**.

HINWEIS: Zum Schutz der Daten wird die Beziehung nicht im Klartext gespeichert, sondern nur in Form eines Hashwertes (Prüfsumme) festgehalten.

Video: Level of Trust

Vertrauen muss gepflegt werden

Findet über einen gewissen Zeitraum keine ausgehende Kommunikation mit einem bestimmten Partner statt, verringert sich das Level of Trust automatisch. Diese Abnahme des Wertes geschieht sowohl bei Bonus- als auch bei Malus-Werten.

Automatisches Entfernen von Partnern

Partner werden automatisch entfernt, wenn der Level-of-Trust-Wert der jeweiligen Domäne auf 0 gesunken ist **und** der Partner keine weiteren Eigenschaften besitzt, die dies verhindern, also beispielsweise hinterlegte Benutzer, Passworte oder Zertifikate.

Punktevergabe für Domänen bei Level of Trust

Die Bonuspunkte für Level of Trust werden den jeweiligen Domänen auf zwei unterschiedlichen Wegen zugeordnet:

- Automatisch aufgrund einer ausgehenden E-Mail
- Manuell über die Benutzeroberfläche unter **Partner** oder über das PowerShell-Cmdlet `Set-NspPartnerTrustDetails`.

Damit eine eingehende E-Mail von dieser Domäne die gespeicherten Bonuspunkte erhält, muss mindestens eine der folgenden Bedingungen in Bezug auf die Domäne mit Vertrauenslevel erfüllt sein:

- Die SPF-Prüfung ist erfolgreich.
- Die DKIM-Prüfung ist erfolgreich.
- Die DMARC-Prüfung ist erfolgreich.
- Die E-Mail ist S/MIME- oder PGP-signiert und die Signatur ist gültig (und passt zu der Domäne im E-Mail-Header).

- Die IP-Adresse steht in den Eigenschaften der Domäne. Diese Liste wird nachts automatisch mit den IP-Adressen gefüllt, die NoSpamProxy aus den MX und A Records der jeweiligen Domäne auslesen kann. Die Adressen werden jedoch nur dann gesammelt, wenn kein DMARC Record für die Absenderdomäne vorhanden ist.

Es wird keine Prüfung auf Gültigkeit des SPF-Eintrags durchgeführt, falls die Domäne mit gesetztem Vertrauen nur im Header erscheint. Somit kann auch keine DMARC-Validierung erfolgen. Folglich muss bei der E-Mail bei einer Differenz zwischen MAIL FROM- und Header-From-Domäne entweder

- am Partnereintrag ein vertrautes Subnetz zur einliefernden IP-Adresse passen oder
- eine S/MIME-, PGP- oder DKIM- Signatur angebracht sein, die zur Domäne mit gesetztem Vertrauenslevel gehört.

HINWEIS: Damit das oben beschriebene Szenario funktioniert, muss in jeder Regel, in der Level of Trust aktiv ist, der **Reputationsfilter** mit aktivierten Prüfungen auf DMARC, SPF, DKIM und der absendenden IP-Adresse aktiviert sein.

Authentifizierung als Vorbedingung für alle Boni

Um Angriffe mit gefälschten E-Mail-Adressen zu verhindern, empfehlen wir Ihnen, eine Form der Authentifizierung zur Vorbedingung nicht nur für den Domänenbonus, sondern für alle Boni zu machen. Siehe **Level-of-Trust-Konfiguration**.

Verwandte Schritte

Verwandte Schritte

Level of Trust aktivieren| Das Level-of-Trust-System muss pro Regel aktiviert werden. Siehe **Schritte beim Erstellen**.

Level of Trust konfigurieren| Die Einstellungen für Level of Trust werden unter Level-of-Trust-Konfiguration vorgenommen. Siehe **Level-of-Trust-Konfiguration**.

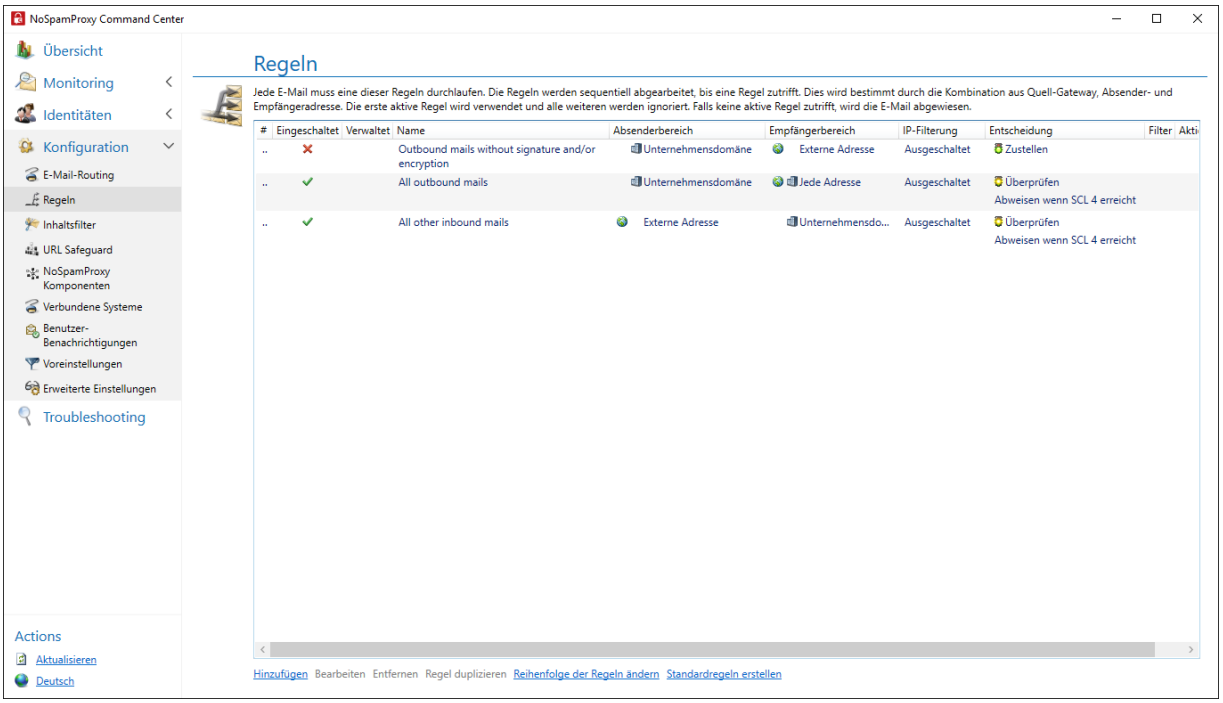
Siehe auch

Level-of-Trust-Konfiguration

Spam Confidence Level (SCL)

Wie NoSpamProxy Protection eine E-Mail als Spam klassifiziert

Regeln



Was sind Regeln?

NoSpamProxy wendet bei der Bearbeitung von E-Mails Regeln an, die Sie individuell konfigurieren können. Diese Regeln 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 konfigurieren.

Sie können auch festlegen, dass Regeln nur für bestimmte IP-Adressen oder Empfänger gilt, zum Beispiel nur für Absender mit einer bestimmten TLD (Top Level Domain) oder IP-Adressen aus einem bestimmten Subnetz.

> **TIPP:** Nach der Neuinstallation von NoSpamProxy können Sie Standardregeln erstellen. Diese ermöglichen es, NoSpamProxy möglichst schnell und mit minimalem Administrationsaufwand die Funktion aufnehmen kann. Trotzdem sollten Sie diese Regeln überprüfen und gegebenenfalls an Ihre Bedürfnisse anpassen.

Die Reihenfolge der Regeln entscheidet

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.

Wie Regeln, Filter und Aktionen zusammenhängen

Um eine E-Mail zu bearbeiten, wendet NoSpamProxy Regeln an, die Sie individuell konfigurieren können. Für jede E-Mail werden die einzelnen Filter der zutreffenden Regel ausgeführt.Filter bewerten, wie stark die E-Mail ein bestimmtes Filterkriterium erfüllt und vergeben entsprechende Malus- und Bonus-Punkte. Die vergebenen Punkte werden mit dem Multiplikator der Filter gewichtet und dann zu einem Gesamtwert addiert. Überschreitet dieser Wert das konfigurierte **Spam Confidence Level (SCL)** der Regel, wird die E-Mail abgewiesen. Das erlaubte SCL können Sie individuell für jede Regel einstellen. Siehe **Schritt 4: Filter konfigurieren** und **Filter in NoSpamProxy**. **Aktionen in NoSpamProxy** werden aufgerufen, nachdem anhand der Filter bestimmt wurde, ob die E-Mail abgewiesen wird oder sie passieren darf. Aktionen können unter anderem die E-Mails verändern, um zum Beispiel eine Fußzeile zu ergänzen oder unerwünschte Anlagen zu entfernen. Aktionen können aber auch E-Mails, die nach der Bewertung durch die Filter eigentlich passieren würden, trotzdem abweisen. Damit kann beispielsweise ein

Virenscanner die E-Mail noch abweisen, obwohl sie nicht als Spam erkannt wurde. Aktionen sind also übergeordnete Einstellungen, mit denen Filter gegebenenfalls überstimmt werden können. Welche Aktionen zur Verfügung stehen und wie sie genau funktionieren, erfahren Sie unter **In NoSpamProxy verfügbare Aktionen**.

Regeln erstellen

Informationen zum Erstellen von Regeln finden Sie unter **Regeln erstellen**.

Spam Confidence Level (SCL)

NoSpamProxy Protection weist alle E-Mails ab, deren Spam Confidence Level (SCL) über einem bestimmten Schwellwert liegt. Diesen Schwellwert legen Sie als Administrator in den einzelnen **Regeln** fest.

Beispiel 1

Diesem Beispiel liegt folgende Filterkonfiguration zu Grunde:

- Es sollen E-Mails überprüft und abgewiesen werden, sobald das SCL größer oder gleich 4 ist.
- Es sind drei Filter aktiviert: Realtime Blocklists, Spam URI Realtime Blocklists und die Wortübereinstimmungen.
- Der Filter Wortübereinstimmungen ist so konfiguriert, dass er nach den Wörtern Sex, Viagra, Cialis usw. suchen und pro Treffer zwei Strafpunkte vergeben soll.

- Die beiden Blocklistenfilter sollen pro Treffer zwei Punkte vergeben.
- **Level of Trust** ist ausgeschaltet.

Nun wird eine Mail verarbeitet, die acht verbotene Wörter und einen verbotenen Link enthält. Der Link ist auf einer Blacklist enthalten. Des Weiteren ist die einliefernde IP-Adresse auf zwei Blacklists vertreten.

Vorläufiges Filterergebnis

Filter	Spam Confidence Level
Realtime Blocklists	4 (Zwei Treffer mal zwei Strafpunkte pro Treffer)
Spam URI Realtime Blocklists	2 (Ein Treffer mal zwei Strafpunkte pro Treffer)
Wortübereinstimmungen	16 (Acht Treffer mal zwei Strafpunkte pro Treffer)

Grundsätzlich ist es bei allen Filtern - auch beim Level of Trust - so, dass der ermittelte Wert immer auf 10 zurückgekürzt wird, wenn er größer als 10 ist. Bei negativen Werten die kleiner als -10 sind, wird der Wert auf -10 angepasst.

"Nettowert" der Filter

Filter	Spam Confidence Level
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)

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

"Nettowert" und Multiplikator

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

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

Beispiel 2

Im diesem Beispiel wird die Filterkonfiguration aus dem ersten Beispiel um das Level of Trust erweitert. Es handelt sich um die gleiche E-Mail wie im vorangegangenen Beispiel. Wir gehen aber davon aus, dass es sich hier um eine gewollte E-Mail handelt und es von der Absender- und Empfänger-Adresse bereits ein Adresspärchen und einen Domänenbonus in der Datenbank gibt.

- Da der letzte Mailkontakt bereits vier Tage zurückliegt, ist der Adresspärchen-Bonus mit 65 Bonuspunkten nicht mehr so hoch. Die Domäne hingegen steht mit statischen 100 Bonuspunkten in den

Vertrauensstellungen.

- Bei den Bonuspunkten des Level of Trust in der Datenbank handelt es sich nicht direkt um den SCL-Wert, sondern um die sogenannten Vertrauenspunkte. Diese werden nur innerhalb der Filter verwendet.

Bewertung durch Level of Trust

In die Berechnung des Level of Trust werden vorhandene negative Werte sowie positive Werte einbezogen. Negative Werte können beispielsweise durch die intelligente DSN-Prüfung oder manuell festgelegte Werte entstehen. Grundsätzlich gilt dann, dass negative Werte Vorrang vor den positiven Werten haben. Hätte also eine E-Mail **+100** Vertrauenspunkte für die Domäne erhalten, wäre aber aus anderen Gründen mit **-5** Vertrauenspunkten belegt worden, so würden diese **-5** Vertrauenspunkte als Basis der Gewichtung verwendet werden.

Zur Berechnung des SCL wird der entstandene Wert dann durch den Wert **-10** dividiert und ergibt in diesem Beispiel einen SCL von **-10** Punkten. Wie bei allen anderen Filtern auch wird der ermittelte Wert auf **10** oder **-10** beschnitten. Die Tabelle mit den Nettowerten aller Filter sieht nun wie folgt aus:

Filter	Spam Confidence Level
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)
Level of Trust	-10

Den Multiplikator der einzelnen Filter können Sie in der jeweiligen Regel festlegen. Das Level of Trust hingegen ermittelt seinen Multiplikator selbstständig. Dazu werden die Multiplikatoren aller anderen Filter addiert und ergeben in diesem Beispiel den Wert **5**.

Ergebnis aus Spam Confidence Level und Level of Trust

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

Die E-Mail wäre in diesem Beispiel zugestellt worden, da der SCL kleiner als 4 ist. Um das Beispiel zu verdeutlichen, wird der Core Antispam Engine Filter mit dem Multiplikator "3" ebenfalls konfiguriert. Dieser Filter vergibt bei einem Treffer immer 4 Punkte und dieser Wert ist auch nicht konfigurierbar.

Der Core Antispam Engine Filter bewertet die E-Mail ebenfalls schlecht.

Endergebnis der SCL-Berechnung

Filter	Spam Confidence Level	Multiplikator	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime	2	2	4

Filter	Spam Confidence Level	Multiplikator	SCL
Blocklists			
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Core Antispam Engine Filter	4	3	12
Level of Trust	-10	8 (=2+2+1+3)	-80
Gesamt			-46

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

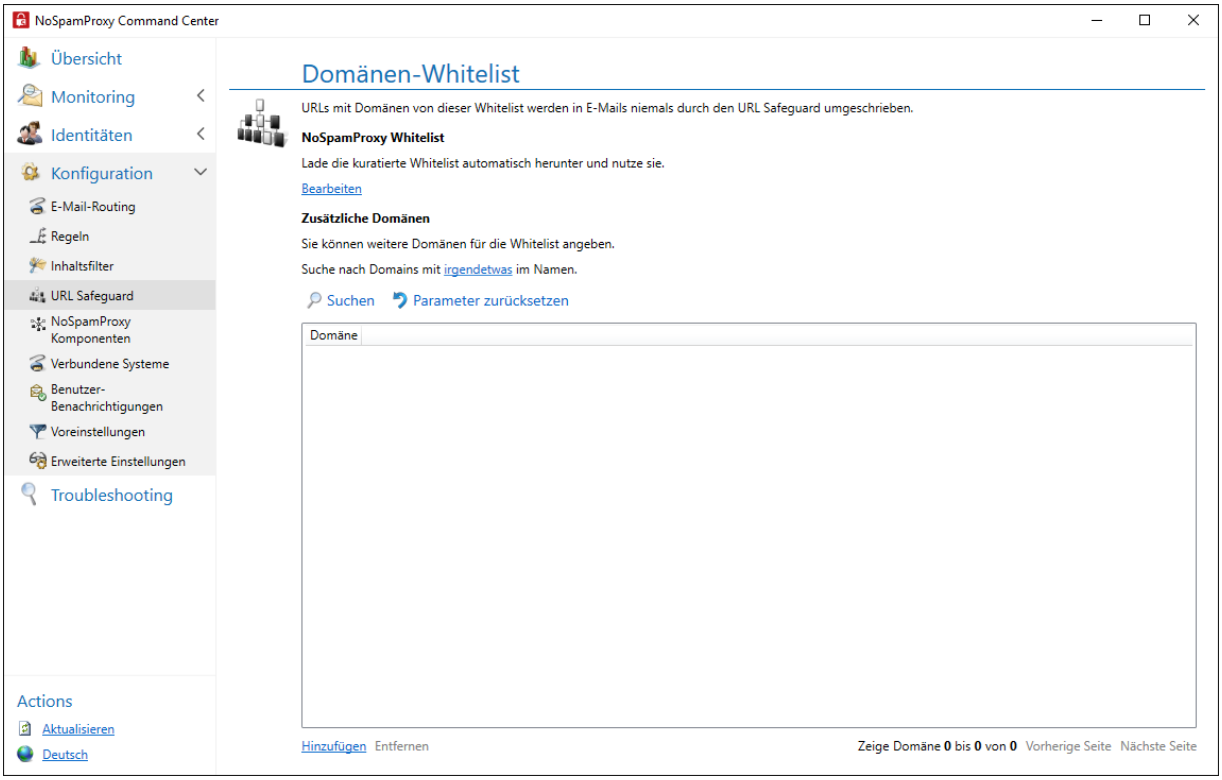
URL Safeguard

Falls entsprechend konfiguriert, prüft der URL Safeguard die Links in eingehenden E-Mails gegen Einträge in den folgenden Listen:

- NoSpamProxy-Allowlist, eine Liste von bekannten Webseiten, die von NoSpamProxy kuratiert wird.
- Die lokale, vom Administrator erstellte Allowlist.

Domänen, die in einer dieser Listen vorhanden sind sowie Unternehmensdomänen werden niemals vom URL Safeguard umgeschrieben.

> **HINWEIS:** Einstellungen für die NoSpamProxy-Allowlist sowie die lokale Allowlist nehmen Sie unter **Konfiguration > URL Safeguard** vor.



Wie arbeitet der URL Safeguard?

Ist die im Link enthaltene Domäne in keiner der Listen vorhanden, führt NoSpamProxy abhängig von der Konfiguration eine der beiden Aktionen aus:

- NoSpamProxy ersetzt den ursprünglichen Link durch einen Link, der auf das Webportal zeigt.
- NoSpamProxy ersetzt den ursprünglichen Link durch einen Link, der auf das Webportal zeigt und sperrt den Zugriff auf den ursprünglichen Link.

In beiden Fällen enthält die an den Empfänger ausgelieferte E-Mail nur den umgeschriebenen Link.

- Wird der Link als ungefährlich eingestuft, wird der Zugriff auf die ursprüngliche URL zugelassen und ausgeführt.
- Wird der Link als gefährlich eingestuft, wird der Zugriff unterbunden. Eine Meldung über den Vorfall wird der Nachrichtenverfolgung hinzugefügt. Je nach Konfiguration erhält der Administrator zudem eine Benachrichtigung.

> **TIPP:** Gesperrte URLs können wieder freigeschaltet werden, indem diese der lokalen Allowlist hinzugefügt werden. Die zur gesperrten URL gehörende Domäne ist vom Empfänger der E-Mail nach dem Klicken auf den umgeschriebenen Link auf dem Web Portal einsehbar. Der zuständige Administrator kann dann die Freischaltung vornehmen. Eine weitere Zustellung der E-Mail durch den Kommunikationspartner ist nicht notwendig.

Häufig gestellte Fragen

Was ist ein Protected Link?

Der Ausdruck **Protected Link** wird anstatt einer URL angezeigt, wenn im Anzeigetext eine URL steht, die sich in den Browser kopieren lässt und zu einer potenziell schadhaften Seite führt.

Lässt sich der Ausdruck Protected Link verändern?

Ja. Siehe **Anpassen des Tags Protected Link im URL Safeguard**.

In welchen Fällen werden URLs umgeschrieben?

Die URL beziehungsweise der Anzeigetext in der E-Mail wird umgeschrieben, wenn die Domäne der URL vom Anzeigetext oder der eigentliche Link nicht auf der NoSpamProxy-Allowlist oder der lokalen Allowlist stehen.

Was kann ich tun, wenn Links zum Webportal auf Grund ihrer Länge nicht geöffnet werden können?

Ein langer Link zum Webportal kann dazu führen, dass er nicht geöffnet werden kann, da er durch die Umschreibung die Längenbegrenzung einiger Browser überschreitet. Die originale URL kann **nicht** im dazugehörigen Message Track nachvollzogen werden, auch wenn die Rückverfolgung aktiviert wurde. Dort wird nur eine verkürzte Version angezeigt. Sie können den Fully Quallified Domain Name (FQDN) im dazugehörigen Message Track, auf der Registerkarte **URL Safeguard** einsehen, sofern die Rückverfolgung aktiviert wurde (siehe **Standardeinstellungen für Partner**). Damit Links von dieser Domäne zukünftig nicht mehr umgeschrieben werden, fügen Sie diese der lokalen Allowlist hinzu. Siehe **URL Safeguard einrichten**.

Siehe auch

URL Safeguard einrichten

Anpassen des Tags Protected Link im URL Safeguard

URL Safeguard (Aktion)

Melden von False Negatives und False Positives

Punktevergabe für Domänen bei Level of Trust

Die Bonuspunkte für Level of Trust werden den jeweiligen Domänen auf zwei unterschiedlichen Wegen zugeordnet:

- Automatisch aufgrund einer ausgehenden E-Mail
- Manuell über die Benutzeroberfläche unter **Partner** oder über das PowerShell-Cmdlet `Set-NspPartnerTrustDetails`.

Damit eine eingehende E-Mail von dieser Domäne die gespeicherten Bonuspunkte erhält, muss mindestens eine der folgenden Bedingungen in Bezug auf die Domäne mit Vertrauenslevel erfüllt sein:

- Die SPF-Prüfung ist erfolgreich.
- Die DKIM-Prüfung ist erfolgreich.
- Die DMARC-Prüfung ist erfolgreich.
- Die E-Mail ist S/MIME- oder PGP-signiert und die Signatur ist gültig (und passt zu der Domäne im E-Mail-Header).
- Die IP-Adresse steht in den Eigenschaften der Domäne. Diese Liste wird nachts automatisch mit den IP-Adressen gefüllt, die NoSpamProxy aus den MX und A Records der jeweiligen Domäne auslesen kann. Die Adressen werden jedoch nur dann gesammelt, wenn kein DMARC Record für die Absenderdomäne vorhanden ist.

Es wird keine Prüfung auf Gültigkeit des SPF-Eintrags durchgeführt, falls die Domäne mit gesetztem Vertrauen nur im Header erscheint. Somit kann auch keine DMARC-Validierung erfolgen. Folglich muss bei der E-Mail bei einer Differenz zwischen MAIL FROM- und Header-From-Domäne entweder

- am Partnereintrag ein vertrautes Subnetz zur einliefernden IP-Adresse passen oder

- eine S/MIME-, PGP- oder DKIM- Signatur angebracht sein, die zur Domäne mit gesetztem Vertrauenslevel gehört.

> **HINWEIS:** Damit das oben beschriebene Szenario funktioniert, muss in jeder Regel, in der Level of Trust aktiv ist, der **Reputationsfilter** mit aktivierten Prüfungen auf DMARC, SPF, DKIM und der absendenden IP-Adresse aktiviert sein.

Hilfe und Unterstützung

Knowledge Base

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter **+49 5251304-636**
- per E-Mail unter **support@nospamproxy.de**.