



Benutzerhandbuch

Protection

Version 15

Rechtliche Hinweise

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

Copyright © 2023 Net at Work GmbH

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

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 11. DEZEMBER 2024 ÜBERARBEITET.

Inhalt

Die Benutzeroberfläche	1
Aktionen auf der Übersichtsseite	1
Weitere Verknüpfungen	3
Monitoring	8
Nachrichtenverfolgung	10
Nachrichtenverfolgung aktivieren	10
Suchergebnisse filtern	11
Details zur Verarbeitung einer E-Mail anzeigen	12
Datensätze exportieren oder importieren	17
Fehlklassifizierung melden	18
Hinweise	18
Nachrichtenverfolgung (Web App)	20
Übersicht	20
E-Mails filtern	21
Details zu einer E-Mail anzeigen	22
E-Mail-Warteschlangen	30
Nach bestimmten Warteschlangen suchen	30
Zustellung über ausgewählte Domains starten oder pausieren	31
Eine ausgeschaltete Warteschlange erstellen	31
Angehaltene E-Mails	33
Nach bestimmten angehaltenen E-Mails suchen	33
In welchen Fällen werden E-Mails angehalten?	34
Verwandte Schritte	34
Gesperzte Anhänge	35

Status-Typen	36
Large Files	41
Verwandte Schritte	41
Filteroptionen bei der Suche	42
Reports	44
Reports	44
De-Mail	46
Ereignisanzeige	48
Einträge filtern	48
Identitäten	50
Unternehmensdomänen	51
Unternehmensdomänen verwalten	52
Kryptographische Schlüssel bearbeiten	53
Administrative Adressen einrichten	55
Unternehmensbenutzer	60
Unternehmensbenutzer hinzufügen	62
Benutzerimport automatisieren	64
Adressumschreibung einrichten	74
Standardeinstellungen für Benutzer konfigurieren	75
Zusätzliche Benutzerfelder hinzufügen	76
Partner	80
Standardeinstellungen für Partner	81
Partnerdomänen hinzufügen	84
Partnerdomänen bearbeiten	85
Benutzereinträge zu Partnerdomänen hinzufügen	87

E-Mail-Authentifizierung	89
DomainKeys Identified Mail (DKIM)	89
Konfiguration	100
E-Mail-Routing einrichten	102
E-Mail-Server des Unternehmens hinzufügen	102
Eingehende Sendekonnektoren anlegen	109
Ausgehende Sendekonnektoren anlegen	111
Empfangskonnektoren anlegen	119
Ungültige Anfragen bei SMTP-Empfangskonnektoren	120
Zustellung über Warteschlangen	122
Headerbasiertes Routing einrichten	124
Regeln erstellen	125
Allgemeine Informationen	125
Schritte beim Erstellen	127
Verwandte Themen	133
NoSpamProxy-Komponenten	137
Intranetrolle	138
Gatewayrolle	139
Web Portal	149
Datenbanken	160
Ändern des Web Ports	182
Verbundene Systeme	184
DNS-Server	184
Archivkonnektoren	186
De-Mail über Mentana-Claimsoft	190

CSA Certified IP List	191
Benutzerbenachrichtigungen	193
Prüfbericht	193
E-Mail-Benachrichtigungen	196
Benutzerbenachrichtigungen anpassen	197
Vorgehen nach Updates	198
Unterschiedliche Designs bei Absenderdomänen verwenden	205
Voreinstellungen	215
Branding	216
Wortübereinstimmungen	217
Realtime Blocklists	219
Erweiterte Einstellungen	221
Schutz sensibler Daten	222
Monitoring	224
Betreffkennzeichnungen	227
Level-of-Trust-Konfiguration	233
SMTP-Protokolleinstellungen	240
SSL-/TLS-Konfiguration	248
Troubleshooting	251
Protokolleinstellungen	254
Geblockte IP-Adressen	257
Berechtigungen korrigieren	258
Marktkommunikation mit AS4	260
Schritt 1: Aktivieren des AS4-Moduls	261
Schritt 3: Erstellen der erforderlichen Windows-Gruppe	263

Schritt 4: Key-Management-Dienst konfigurieren	265
Dienstadresse hinterlegen	265
(Optional) HSM hinzufügen	266
(Optional) Token konfigurieren	268
Häufige Fragen	268
Schritt 5: Ihr Marktpartner-Konto konfigurieren	270
Ihr Marktpartner-Konto hinzufügen	270
Zertifikatsanfrage für die AS4-Kommunikation erstellen	272
Zertifikate importieren	273
Einstellungen ändern	274
Schritt 6: Marktpartner-Kommunikation aktivieren	275
Ausgehendes AS4 anfragen	275
Eingehendes AS4 bestätigen	276
Testen der AS4-Konnektivität	277
AS4-Nachrichtenverfolgung	279
Marktpartner manuell hinzufügen	283
Schlüsselspeicher ändern	285
Speicherort für EDIFACT-Dokumente konfigurieren	286
Anhang	287
Filter in NoSpamProxy	288
In NoSpamProxy verfügbare Filter	291
Aktionen in NoSpamProxy	317
In NoSpamProxy verfügbare Aktionen	318
Grundlagen	340

Absenderreputation	340
32Guards	341
Flow Guard	344
Inhaltsfilter	345
Level of Trust	347
Regeln	352
Spam Confidence Level (SCL)	354
URL Safeguard	359
Hilfe und Unterstützung	365

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.

I 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.

Serverleistung

Datenverkehr System

E-Mails

	Angenommen		Abgewiesen	
	Letzte Minute	Letzte Stunde	Letzte Minute	Letzte Stunde
GWRole01	0	0	0	0
Gesamt	0	0	0	0

Verbindungen

	Angenommen		Abgewiesen	
	Letzte Minute	Letzte Stunde	Letzte Minute	Letzte Stunde
GWRole01	0	0	0	0
Gesamt	0	0	0	0

Schließen

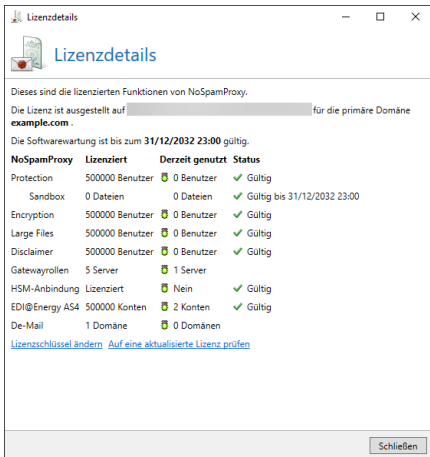
System| Diese Registerkarte zeigt für jedes System mit Intranet- oder Gatewayrollen die installierten Dienste, deren Status und die verwendeten Ressourcen.

Festplatten		Genutzter Speicher		
📁	C:\	41,98 GB (32,89%)		
Dienst	Speicherauslastung	Prozessorauslastung	Betriebszeit	
▶	CYREN Service	39,43 MB	0,00%	1 Stunde, 18 Minuten
▶	Gateway Role	299,75 MB	0,16%	1 Stunde, 18 Minuten
▶	Intranet Role	147,14 MB	1,41%	1 Stunde, 18 Minuten
▶	Management Service	68,90 MB	0,31%	1 Stunde, 18 Minuten
▶	Privileged Service	41,04 MB	0,00%	1 Stunde, 18 Minuten
🖥️	System	2,54 GB (42,36%)	7,95%	1 Stunde, 18 Minuten

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.

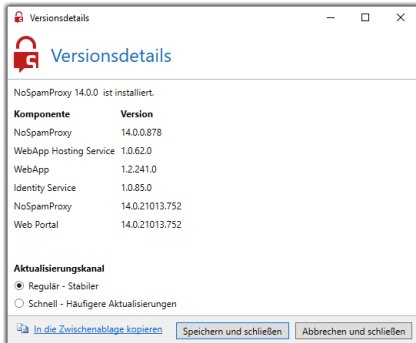
Auswahl des Aktualisierungskanals

- 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.

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.

Nachrichtenverfolgung	10
Nachrichtenverfolgung aktivieren	10
Suchergebnisse filtern	11
Details zur Verarbeitung einer E-Mail anzeigen	12
Datensätze exportieren oder importieren	17
Fehlklassifizierung melden	18
Hinweise	18
Nachrichtenverfolgung (Web App)	20
Übersicht	20
E-Mails filtern	21
Details zu einer E-Mail anzeigen	22
E-Mail-Warteschlangen	30
Nach bestimmten Warteschlangen suchen	30
Zustellung über ausgewählte Domains starten oder pausieren	31
Eine ausgeschaltete Warteschlange erstellen	31
Angehaltene E-Mails	33

Nach bestimmten angehaltenen E-Mails suchen	33
In welchen Fällen werden E-Mails angehalten?	34
Verwandte Schritte	34
Gesperrte Anhänge	35
Status-Typen	36
Large Files	41
Verwandte Schritte	41
Filteroptionen bei der Suche	42
Reports	44
Reports	44
De-Mail	46
Ereignisanzeige	48
Einträge filtern	48

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.



TIP: 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.
- **Zustellerggebnisse**| Der Status der Zustellung.
- **SCL-Wert**| Das errechnete Spam Confidence Level.
- **Regel**| Der Name der Regel, von der die Nachricht verarbeitet wurde.



TIP: 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**.

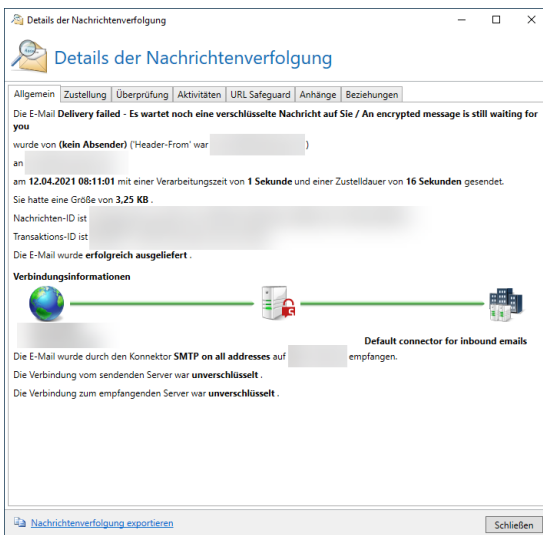
oder

- 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.

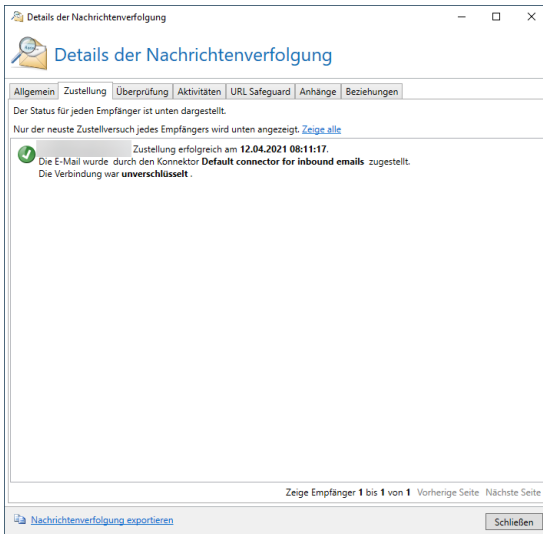
Allgemein

Die Registerkarte **Allgemein** enthält beispielsweise Informationen zur Verbindung, zum Auslieferungsstatus und zu den verwendeten Konnektoren.



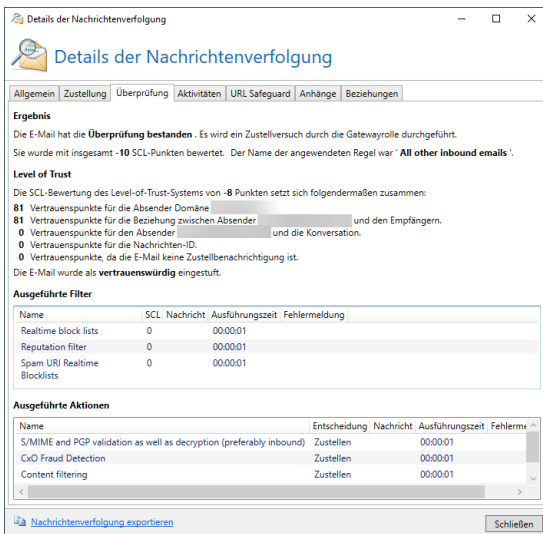
Zustellung

Die Registerkarte **Zustellung** enthält eine Liste der Zustellversuche sowie Informationen zu Konnektoren und Verschlüsselung.



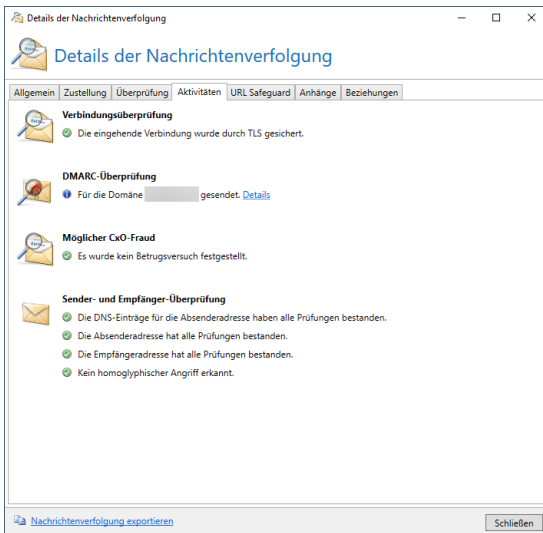
Überprüfung

Die Registerkarte **Überprüfung** zeigt unter anderem Informationen 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 Filtern und Aktionen.



Aktivitäten

Die Registerkarte **Aktivitäten** enthält Informationen zu Aktivitäten, die auf der jeweiligen E-Mail ausgeführt wurden.

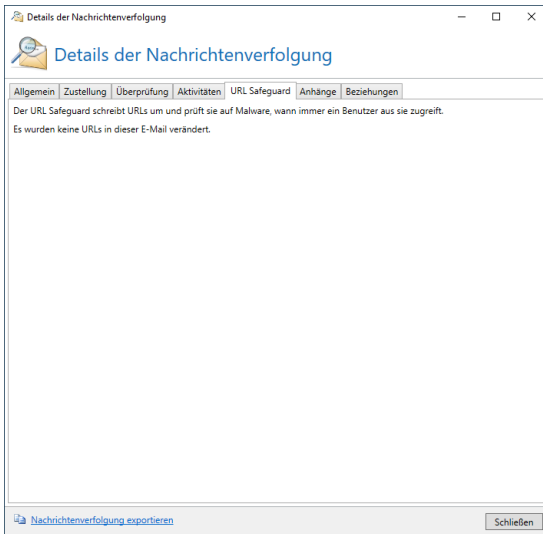


Zudem bietet sie Informationen zu empfangenen oder versendeten E-Rechnungen.



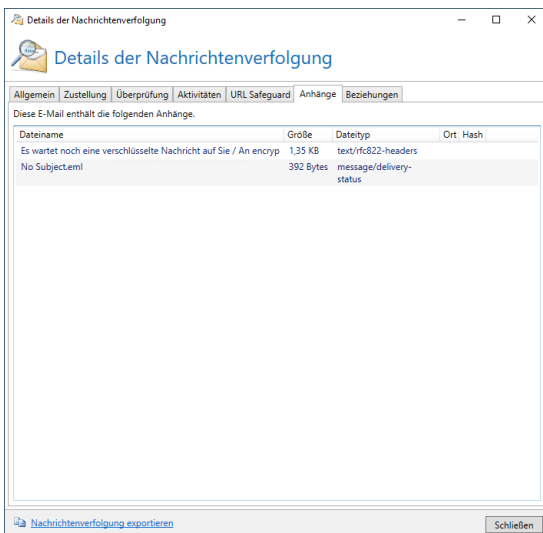
URL Safeguard

Die Registerkarte **URL Safeguard** enthält Informationen zu URLs, die durch den URL Safeguard umgeschrieben wurden.



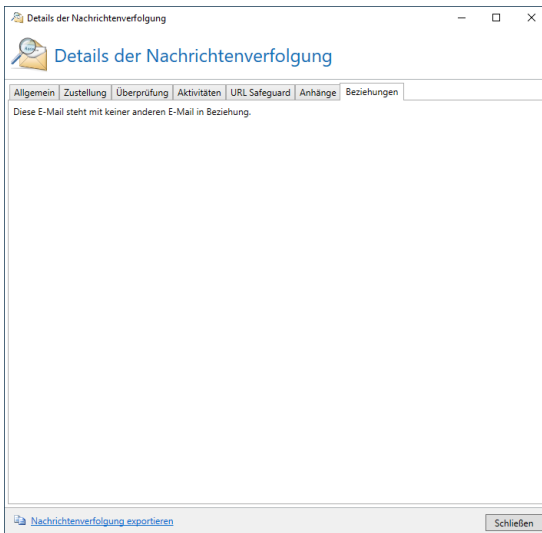
Anhänge

Die Registerkarte **Anhänge** enthält Informationen zu den E-Mail-Anhängen, beispielsweise Größe, Dateityp und Hashes.



Beziehungen

Die Registerkarte **Beziehungen** zeigt E-Mails, die zu der jeweiligen E-Mail in Beziehung stehen.



■ 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 Dialogs.
- Zum Anzeigen klicken Sie **Nachrichtenverfolgungsdatei laden** in der Liste aller gefundenen Datensätze.

I Fehlklassifizierung melden

Für Informationen bezüglich des Meldens von Fehlklassifizierungen, siehe [Melden von False Negatives und False Positives](#).

I 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.

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.



TIP: 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.

👤 Addresses	🌐 Connection	✉ Message	🔍 Validation	🔒 Security
Beliebige Adresse	Richtung	Betreff	Regel	Signiert
'MAIL FROM'-Adresse	Absender-IP-Adresse	Anhang	Status	Verschlüsselt
'Header-From'-Adresse	Gateway Rolle	URL	SCL	
Empfängeradressen	Transaktions-ID	Nachrichten-ID		
	Zustelldauer	Angehalten		
	Verarbeitungsdauer			

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.



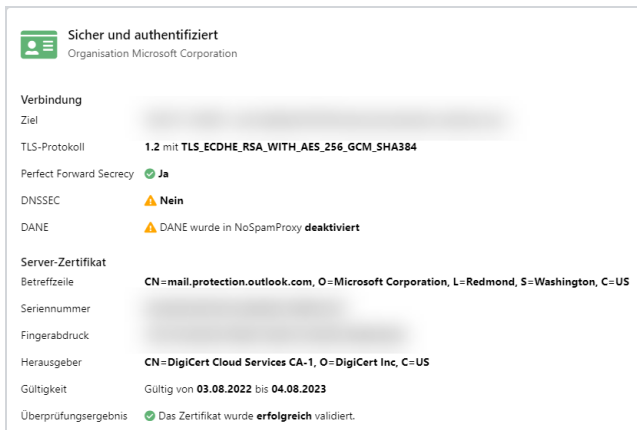
The screenshot shows the 'Allgemein' tab of an email client's message tracking interface. The main content area displays a delivery path diagram with the following callouts:

- Status der E-Mail:** Points to the 'Zustellung erfolgreich' (Delivery successful) status indicator.
- Absenderadresse:** Points to the sender's email address, 'smtp.msn.com'.
- IP-Adresse und Servername des Absenders:** Points to the sender's IP address and server name, 'Microsoft Corporation'.
- Informationen zur Verbindungsverschlüsselung:** Points to the encryption status icons (lock and padlock) in the delivery path.
- Empfängeradresse:** Points to the recipient's email address.
- IP-Adresse und Servername des Empfängers:** Points to the recipient's IP address and server name.
- Beginn der Verbindung zwischen dem einliefernden Server und NoSpamProxy:** Points to the start of the delivery path.
- Dauer der Verarbeitung durch die Gatewayrolle:** Points to the '20 Sekunden' duration for the gateway role.
- Empfangskonnektor sowie Name des Servers, auf dem die Gatewayrolle installiert:** Points to the 'SMTP on all addresses' connector and server name.
- Dauer der Zustellung an alle Empfänger:** Points to the '28 Sekunden' total delivery duration.

Additional details visible in the screenshot include the message subject 'Major update from Message center', message size '12.31 KB', and a 'Herunterladen' (Download) button at the bottom left.

- 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](#).

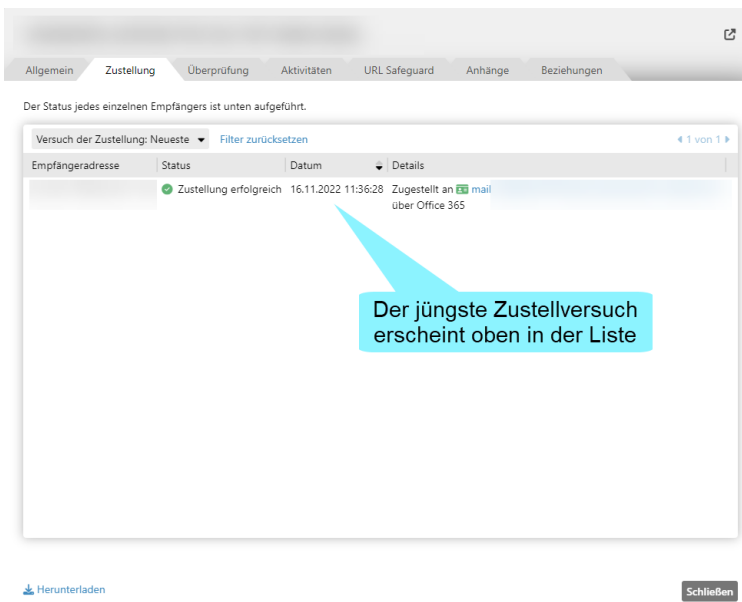
Gesperre Anhänge | Mindestens ein Anhang erfordert eine Freigabe durch den Administrator.



TIP: 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.

Major update from Message center ↗

Allgemein | **Zustellung** | Überprüfung | Aktivitäten | URL Safeguard | Anhänge | Beziehungen

Ergebnis
Die E-Mail hat die **Validierung bestanden**. Es wird ein Zustellversuch der Gateway Rolle durchgeführt.
Sie wurde mit insgesamt **0** SCL-Punkten bewertet. Der Name der angewandten Regel lautete **All other inbound emails**.

Level of Trust
Das Level-of-Trust-System änderte die Bewertung um **0** SCL-Punkte. [Details](#)

Ausgeführte Filter

Name	SCL	Nachricht	Ausführungszeit	Fehlermeldung
32Guards	0		00:00:01	
CSA Certified IP List	0		00:00:01	
Cyren AntiSpam	0		00:00:01	
Cyren IP Reputation	0		00:00:01	
Echtzeit-Blocklisten	0		00:00:01	
Reputationsfilter	0		00:00:06	
Spam URI Realtime Blocklists	0		00:00:01	

Ausgeführte Aktionen

Name	Entscheidung	Nachricht	Ausführungszeit	Fehlermeldung
Inhaltsfilterung	Zustellen		00:00:01	
32Guards	Zustellen		00:00:01	
CxO-Fraud-Detection	Zustellen		00:00:01	
Greylisting	Zustellen		00:00:01	
Malware-Scanner	Zustellen		00:00:01	
URL Safeguard	Zustellen		00:00:01	
S/MIME- und PGP-Überprüfung sowie Entschlüsselung (vorzugsweise eingehend)	Zustellen		00:00:01	

[Herunterladen](#) Schließen

Ergebnisse der Validierung sowie Informationen zu Level of Trust

Filter, die auf diese E-Mail angewendet wurden

Aktionen, die auf Basis der Filterergebnisse ausgeführt wurden

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.

Allgemein Zustellung Überprüfung Aktivitäten URL Safeguard Anhänge Beziehungen

S/MIME Entschlüsselung
Die Nachricht wurde mit dem Zertifikat `nsp-dev-1@nsp-dev-1.de` unter Nutzung von **RSA** (2048 Bit) und **AES-128-CBC** entschlüsselt. Das Padding **PKCS 1.5** wurde verwendet.

DMARC-Überprüfung
✔ Die Domäne `nsp-preview-1.de` besitzt keine DMARC-Richtlinie, aber die Nachricht hätte die Validierung bestanden. [Details](#)

Authenticated-Received-Chain-Überprüfung (ARC)
✘ Die ARC-Kette konnte nicht validiert werden. Die ARC-Nachrichtensignatur ist ungültig

Verbindungsüberprüfung
✔ Die eingehende Verbindung wurde durch TLS gesichert.

Cyren IP-Adress-Reputation
✔ Es gibt keine bekannten Risiken bezüglich der Absenderadresse `3.65.217.116`. [Cyren-Referenz-ID kopieren](#)

Möglicher CxO-Fraud
✔ Es wurde kein Betrugsversuch festgestellt.

DNS-Überprüfung
✔ Die IP-Adresse `3.65.217.116` wurde zu dem Hostnamen `ec2-3-65-217-116.eu-central-1.compute.amazonaws.com` aufgelöst.
✔ Der Hostname `3.65.217.116` zugeordnet zu der IP-Adresse `ec2-3-65-217-116.eu-central-1.compute.amazonaws.com` ist gültig.
✔ Der Hostname `3.65.217.116` zugeordnet zu der IP-Adresse `ec2-3-65-217-116.eu-central-1.compute.amazonaws.com` lässt sich zu der IP-Adresse auflösen.
✔ Die 'MAIL FROM' Domäne löst zu der IP-Adresse `ec2-3-65-217-116.eu-central-1.compute.amazonaws.com` auf.

Sender- und Empfänger-Überprüfung
✔ Die DNS-Einträge für die Absenderadresse haben alle Prüfungen bestanden.
✔ Kein homographischer Angriff erkannt.

Malware Überprüfung
✔ Keine Malware gefunden.
Die E-Mail wurde durch Cyren AntiVirus, den dateibasierten Virens scanner und Cyren Zero Hour Virus Protection überprüft.

Heimralf

[Nachrichtenverfolgungsdatensatz herunterladen](#) Schließen

Zudem bietet sie Informationen zu empfangenen oder versendeten E-Rechnungen.

Allgemein Zustellung Überprüfung Aktivitäten URL Safeguard Anhänge Beziehungen

Möglicher CxO-Fraud
✔ Es wurde kein Betrugsversuch festgestellt.

E-Rechnung
Die Datei `EXTENDED_Kostenrechnung.pdf` wurde als elektronische Rechnung erkannt.
Rechnungsnummer **KR87654321012**
Rechnungsdatum **06.10.2018**
Verkäufer **MUSTERLIEFERANT GMBH**
Käufer **MUSTER-KUNDE GMBH**
Profil **EXTENDED**
Type Code **380 - Handelsrechnung**

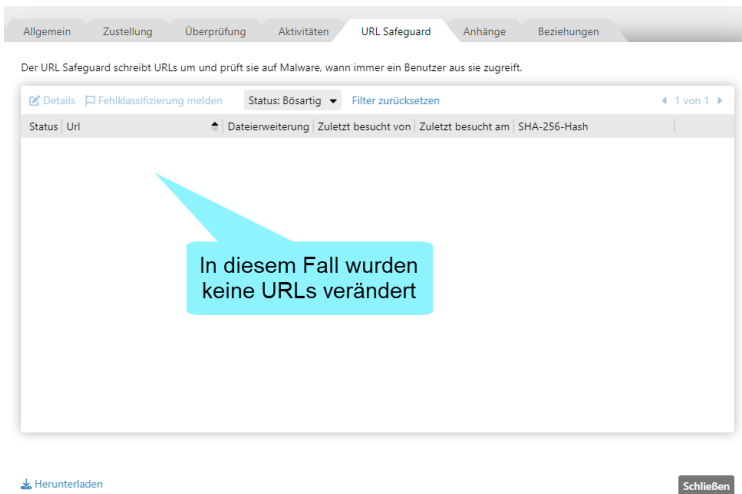
E-Rechnung
Die Datei `XRECHNUNG_Elektron.pdf` wurde als elektronische Rechnung erkannt.
Rechnungsnummer **181301674**
Rechnungsdatum **25.04.2018**
Verkäufer **ELEKTRON Industrieservice GmbH**
Käufer **ConsultingService GmbH**
Profil **XRECHNUNG**
Type Code **877 - Ungültig**

E-Rechnung
Die Datei `BASIC-WL_Einfach.pdf` wurde als elektronische Rechnung erkannt.

[Herunterladen](#) Schließen

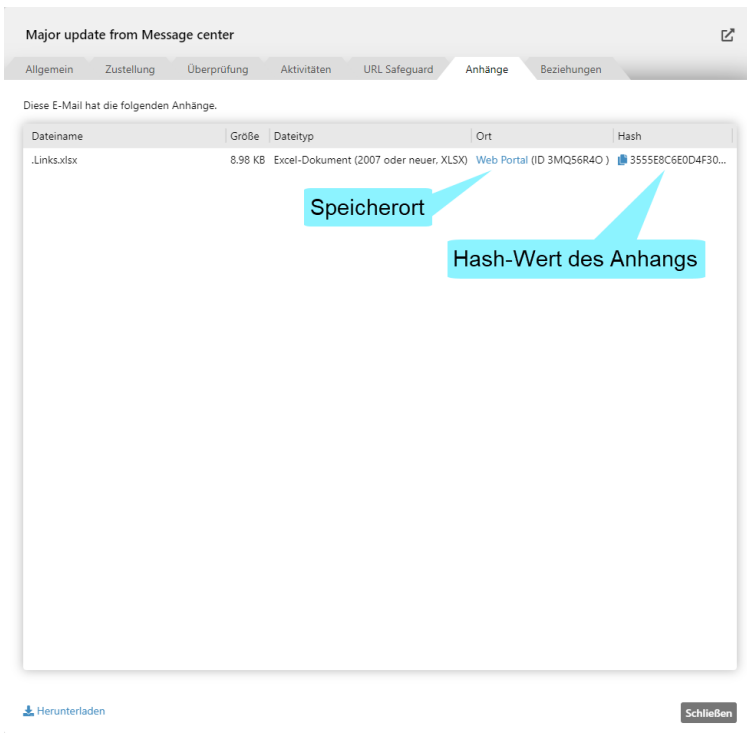
Registerkarte URL Safeguard

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.



Der Status von Anhängen, die auf dem Webportal gespeichert wurden, wird durch folgende Icons angezeigt:

- ⚠ |Die Freigabe dieses Anhangs wurde angefordert.
- ▲ |Der Malware-Scan für diesen Anhang ist fehlgeschlagen.
- ⦿ |Für diesen Anhang ist eine automatische Freigabe eingerichtet.
- 🗑 |Dieser Anhang wurde bereits gelöscht.
- 🔒 |Dieser Anhang ist gesperrt.

Weitere 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.

Major update from Message center

Allgemein Zustellung Überprüfung Aktivitäten URL Safeguard Anhänge **Beziehungen**

Diese E-Mail bezieht sich auf folgende E-Mails.

Typ	Status	Empfangsdatum	MAIL FROM	Empfänger	Betreff
Verursacher	Angehalten	19.05.2022 14:38:35	admin@netspam.email	nsp-preview-1@nsp-preview-1.de	test

Typ der Beziehung

Klicken Sie auf den Betreff der E-Mail, um die entsprechende Detailansicht in einem neuen Tab zu öffnen

Herunterladen Schließen

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.

The screenshot shows the 'E-Mail-Warteschlangen' (E-Mail Queues) page in the NoSpamProxy Command Center. The page title is 'E-Mail-Warteschlangen'. Below the title, there is a search bar with the text 'Suche nach E-Mail-Warteschlangen mit einer Zieldomäne ähnlich einer beliebigen Domäne'. There are two buttons: 'Suchen' and 'Parameter zurücksetzen'. Below the search bar is a table with the following columns: 'Eingeschaltet', 'Domänenname', 'Aufträge in Warteschlange', 'Aktive Aufträge', 'Größe', 'Alter', 'Gateway Rolle', and 'Letzter Fehler'. The table is currently empty. At the bottom of the page, there are several action buttons: 'Einschalten', 'Ausschalten', 'Entfernen', and 'Ausgeschaltete Warteschlange erstellen'. There is also a status indicator that says 'Zeige Warteschlange 0 bis 0' and 'Vorherige Seite Nächste Seite'. The sidebar on the left contains various navigation options: 'Übersicht', 'Monitoring', 'Nachrichtenverfolgung', 'E-Mail-Warteschlangen', 'Angehaltene E-Mails', 'Large Files', 'Reports', 'Ereignisanzeige', 'Identitäten', 'Konfiguration', and 'Troubleshooting'. There is also an 'Actions' section with 'Aktualisieren' and 'Deutsch' buttons.

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.

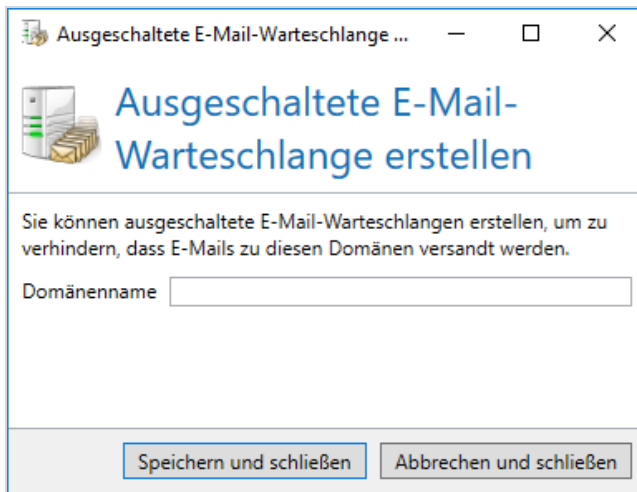
| Zustellung über ausgewählte Domains starten oder pausieren

- 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**.



Ausgeschaltete E-Mail-Warteschlange erstellen

Sie können ausgeschaltete E-Mail-Warteschlangen erstellen, um zu verhindern, dass E-Mails zu diesen Domänen versandt werden.

Domänenname

Speichern und schließen Abbrechen und schließen

2. Geben Sie unter **Domänenname für Warteschlange** den Domännennamen 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.



TIP: 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.

The screenshot shows the 'NoSpamProxy Command Center' interface. On the left is a sidebar with navigation items: 'Übersicht', 'Monitoring' (expanded), 'Nachrichtenverfolgung', 'E-Mail-Warteschlangen', 'Angehaltene E-Mails' (selected), 'Large Files', 'Reports', 'Ereignisanzeige', 'Identitäten', 'Konfiguration', and 'Troubleshooting'. Below the sidebar are 'Actions' like 'Aktualisieren' and 'Deutsch'. The main area is titled 'Angehaltene E-Mails' and contains a search filter: 'Suche nach Nachrichten die gesandt wurden von einem beliebigen Absender an einen beliebigen Empfänger mit allem in der Betreffzeile und einem Typ von jedem Typ'. Below the filter is a search bar and a 'Parameter zurücksetzen' button. A table with the following columns is shown: 'Typ', 'Absender', 'Empfänger', 'Erstellt', 'Status', 'Betreffzeile', 'Fehlerursache', 'Gateway', 'Rolle'. The table is currently empty. At the bottom of the main area, there are controls: 'Erneut versuchen', 'Herunterladen', 'Entfernen', 'Zeige E-Mail in Warteschleife 0 bis 0', 'Vorherige Seite', and 'Nächste Seite'.

■ 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.



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

| In welchen Fällen werden E-Mails angehalten?

- 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, indem 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.

I 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:

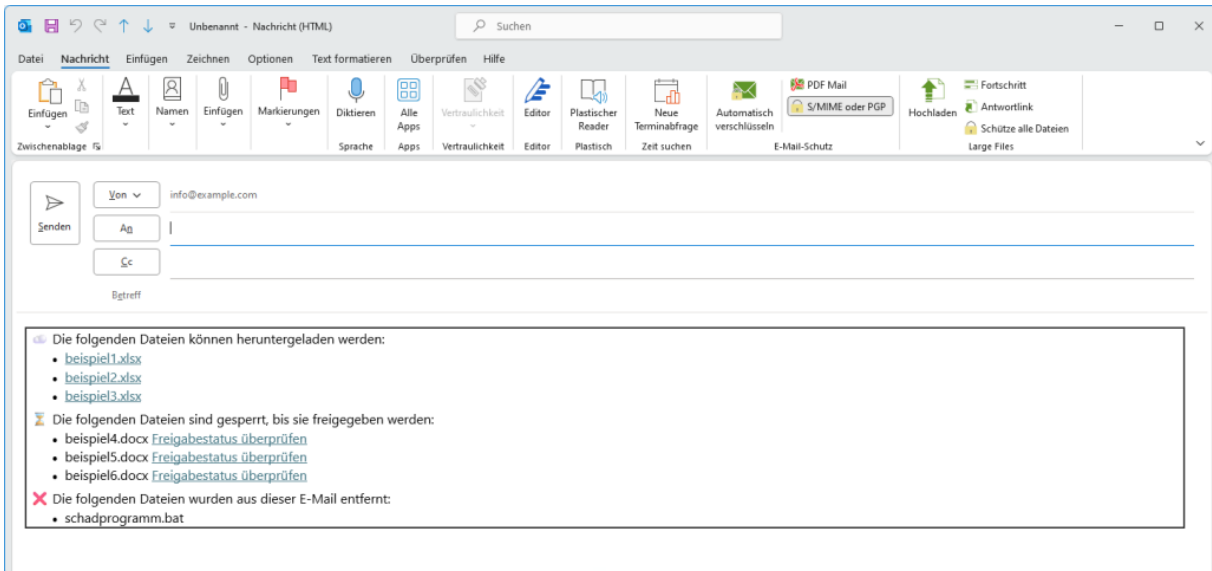
- Klicken Sie **Large Files**, um weitere Informationen zum Anhang zu erhalten, den Anhang herunterzuladen oder eine Malwareprüfung auszuführen.
- Klicken Sie **Anhänge freigeben**, um die jeweiligen Anhänge zu freizugeben.
- Klicken Sie **Anhänge verwerfen**, um die jeweiligen Anhänge zu löschen.



TIP: 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.

E-Mail-Hinweise

Links zu Webportal-Dateien werden als Hinweise in den jeweiligen E-Mails hinzugefügt.



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-Mandanten 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

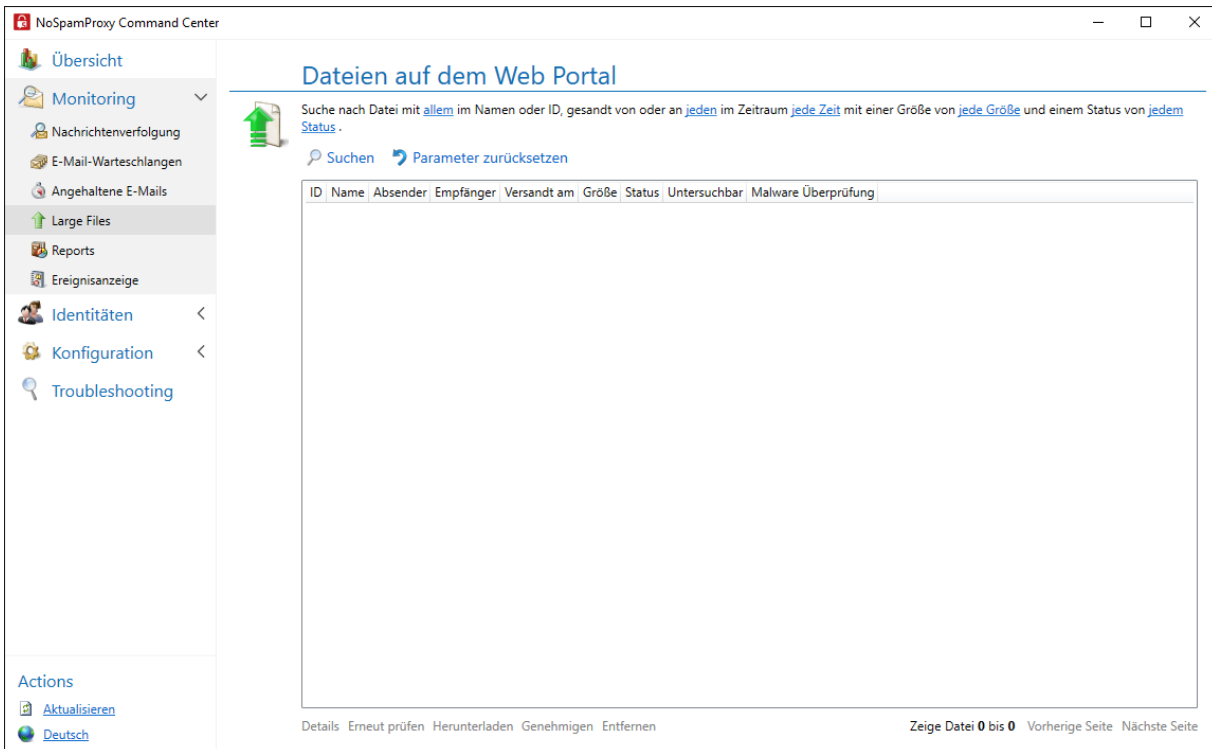


(Partnerorganisation an Office 365) oder durch Umstellung auf unterschiedliche TLS-Identitäten bei ein- und ausgehenden Sendekonnektoren in NoSpamProxy erreichen. Wir empfehlen hier, im ausgehenden Sendekonnektor keine TLS-Identität zu übermitteln.

- **Angehalten**| Es sind weitere Aktionen notwendig, damit die E-Mail erfolgreich zugestellt wird.
 - **Inhaltfilter**| 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.



The screenshot shows the NoSpamProxy Command Center interface. The left sidebar contains navigation options: Übersicht, Monitoring, Nachrichtenverfolgung, E-Mail-Warteschlangen, Angehaltene E-Mails, Large Files (highlighted), Reports, Ereignisanzeige, Identitäten, Konfiguration, and Troubleshooting. The main content area is titled 'Dateien auf dem Web Portal' and includes a search bar with a magnifying glass icon and a 'Suchen' button. Below the search bar is a table with the following columns: ID, Name, Absender, Empfänger, Versand am, Größe, Status, Untersuchbar, Malware, and Überprüfung. The table is currently empty. At the bottom of the interface, there are 'Actions' including 'Aktualisieren' and 'Deutsch', and a footer with 'Details', 'Erneut prüfen', 'Herunterladen', 'Genehmigen', 'Entfernen', and 'Zeige Datei 0 bis 0 Vorherige Seite Nächste Seite'.

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).

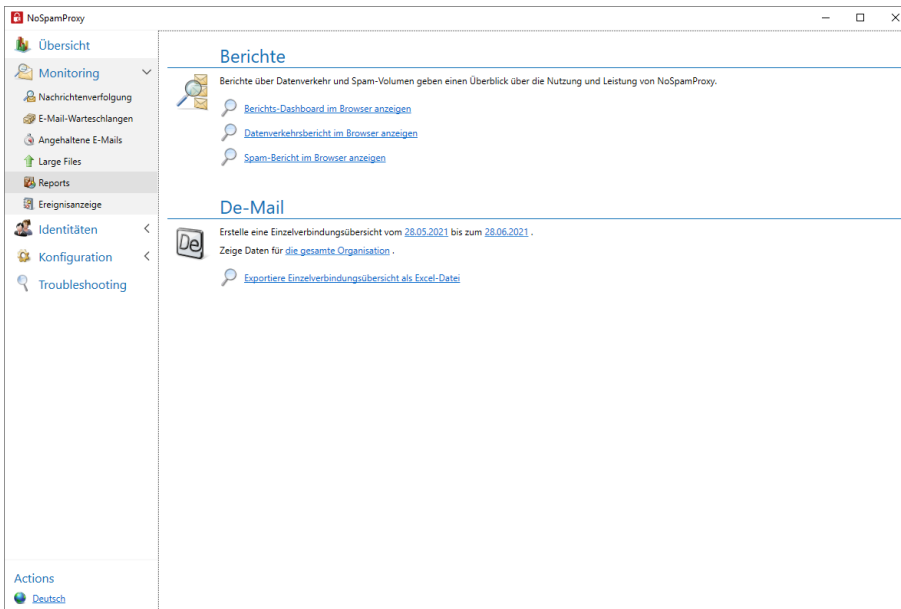
- Untersuchbare Dateien über **Erneut prüfen** auf Malware untersuchen. Wird Malware gefunden, wird die Datei gelöscht und der Empfänger über das Ergebnis informiert. Die Spalte **Malware Überprüfung** zeigt den Zeitpunkt der letzten Überprüfung an.

I Filteroptionen bei der Suche

- **Dateiname**| Geben sie den Dateinamen oder Teile davon an.
- **ID**| Die E-Mail-ID der jeweiligen E-Mail.
- **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.



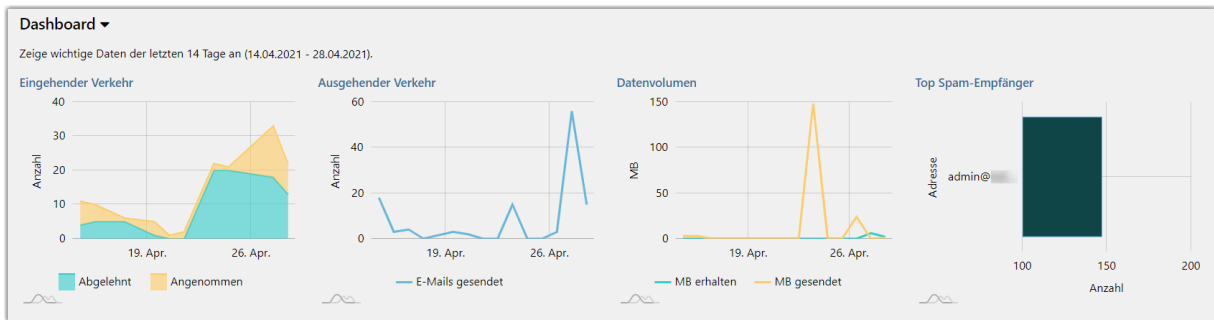
Reports

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



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

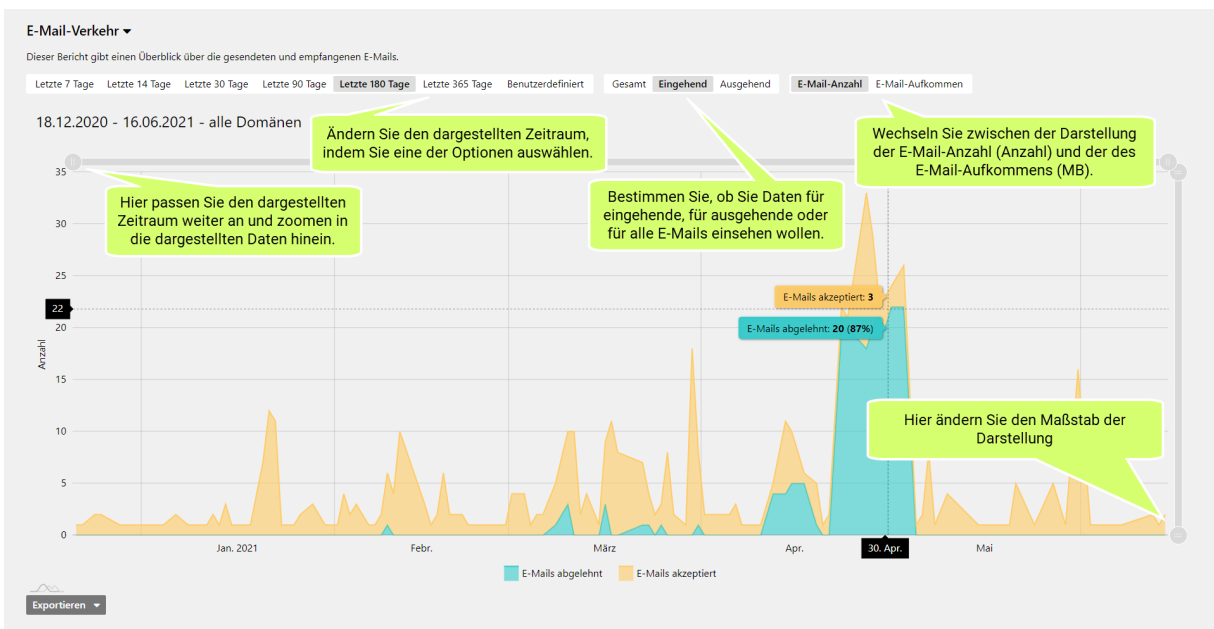
Dashboard



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.

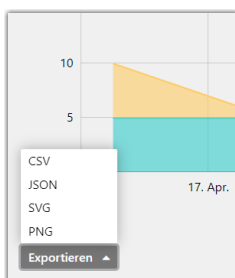
Top-Spam-Empfänger

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.

Schwere	Ereigniskennung	Datum und Uhrzeit	Rolle oder Dienst	Servername
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION
Warnung	2811	22.07.2021 16:33:13	enQsig Web Portal	INSTALLATION

Einträge filtern

Die folgenden Eigenschaften können zur Einschränkung der Ergebnisse verwendet werden:

- Rollen und Dienste

- Intranet Role
- Gateway Role
- Web Portal
- Management service
- Privileged service
- Message tracking service
- Identity service
- Web app

[Alle auswählen](#) [Alle löschen](#)

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

<input checked="" type="checkbox"/>	Fehler
<input checked="" type="checkbox"/>	Warnungen
<input checked="" type="checkbox"/>	Informationen
Alle auswählen Alle löschen	



TIP: 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

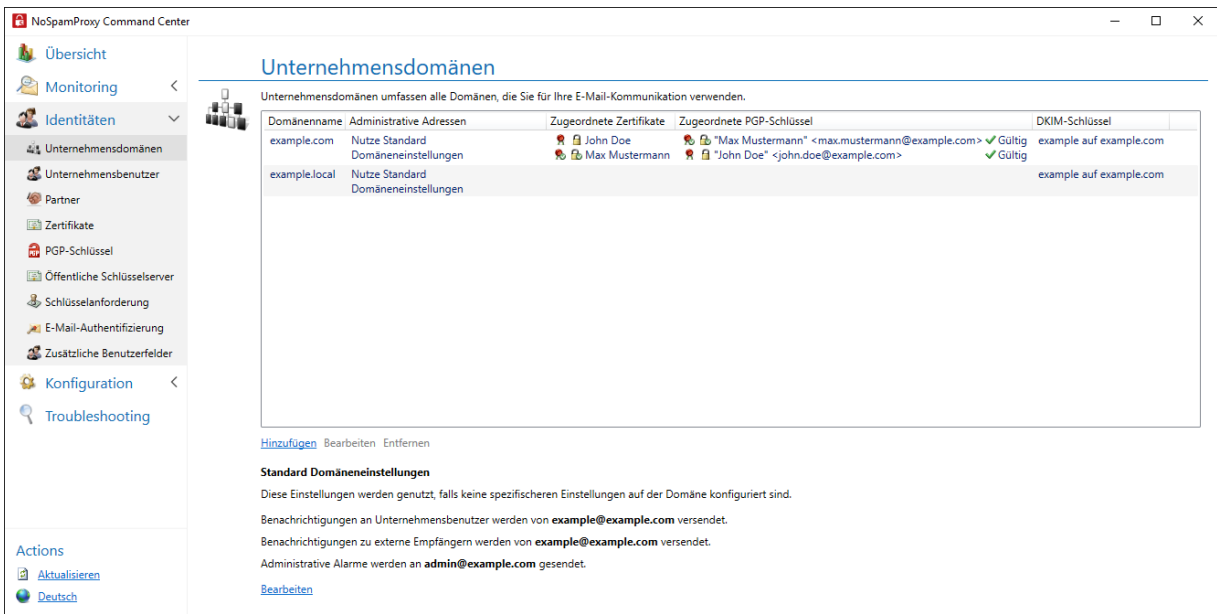
Dieser Bereich bietet Ihnen Zugriff auf alle externen und internen Firmen und Personen sowie auf deren E-Mail-Adressen.

Unternehmensdomänen	51
Unternehmensdomänen verwalten	52
Kryptographische Schlüssel bearbeiten	53
Administrative Adressen einrichten	55
Unternehmensbenutzer	60
Unternehmensbenutzer hinzufügen	62
Benutzerimport automatisieren	64
Adressumschreibung einrichten	74
Standardeinstellungen für Benutzer konfigurieren	75
Zusätzliche Benutzerfelder hinzufügen	76
Partner	80
Standardeinstellungen für Partner	81
Partnerdomänen hinzufügen	84
Partnerdomänen bearbeiten	85
Benutzereinträge zu Partnerdomänen hinzufügen	87
E-Mail-Authentifizierung	89
DomainKeys Identified Mail (DKIM)	89

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

Unternehmensdomänen umfassen alle Domänen, die Sie für Ihre E-Mail-Kommunikation verwenden.

Domänenname	Administrative Adressen	Zugeordnete Zertifikate	Zugeordnete PGP-Schlüssel	DKIM-Schlüssel
example.com	Nutze Standard Domäneneinstellungen	John Doe	"Max Mustermann" <max.mustermann@example.com> Gültig	example auf example.com
example.local	Nutze Standard Domäneneinstellungen	Max Mustermann	"John Doe" <john.doe@example.com> Gültig	example auf example.com

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

Standard Domäneneinstellungen

Diese Einstellungen werden genutzt, falls keine spezifischeren Einstellungen auf der Domäne konfiguriert sind.

Benachrichtigungen an Unternehmensbenutzer werden von **example@example.com** versendet.

Benachrichtigungen zu externe Empfängern werden von **example@example.com** versendet.

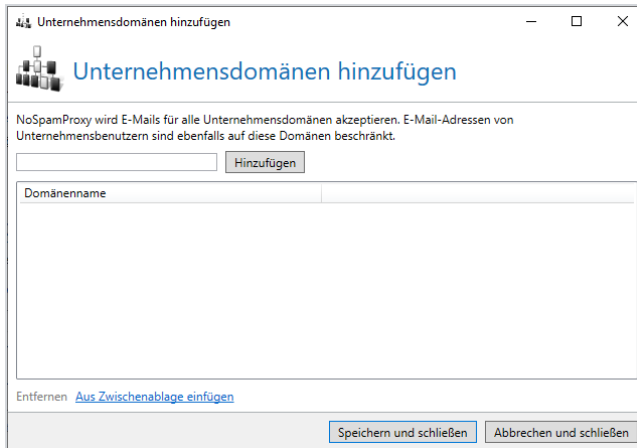
Administrative Alarme werden an **admin@example.com** gesendet.

[Bearbeiten](#)

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.

Einstellungen für Domäne example.com

Einstellungen für Domäne example.com

Administrative Adressen | Zertifikate | PGP-Schlüssel | DomainKeys Identified Mail

Wählen Sie den Domänen-PGP-Schlüssel, um ausgehende E-Mails zu signieren. Zusätzlich wählen Sie den Domänen-PGP-Schlüssel für die Verschlüsselung von eingehenden E-Mails. Diese PGP-Schlüssel werden genutzt, wenn keine Benutzer PGP-Schlüssel vorhanden sind.

Name	Schlüsseltyp	Signieren	Verschlüsseln	Status	Gültig von	Läuft ab	Fingerabdruck
"Max Mustermann" <max.mustermann@example.com>	Geheimer Schlüssel			✓ Gültig	16.12.2019 10:25:47	16.12.2025 10:25:47	008D0391E9A10A6407480A74CC51EC2545B90A87
"John Doe" <john.doe@example.com>	Geheimer Schlüssel			✓ Gültig	16.12.2019 10:20:59	15.12.2025 10:20:59	9290675057E07D1755F70AC88FBC97D2CB229A8E

Details anzeigen Entfernen

Legende

- Signieren/verschlüsseln nicht unterstützt
- Signieren/verschlüsseln unterstützt
- Signieren/verschlüsseln unterstützt und ausgewählt

Speichern und schließen Abbrechen und schließen

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.

Kryptographische Schlüssel löschen

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

Administrative Adressen einrichten

Domänenspezifische Adressen

Einstellungen für Domäne example.local

Einstellungen für Domäne example.local

Administrative Adressen | Zertifikate | PGP-Schlüssel | DomainKeys Identified Mail

Überschreibe Standard Domäneneinstellungen

Geben Sie E-Mail-Adressen für administrative Benachrichtigungen an.

Benachrichtigungen an Unternehmensbenutzer

Absenderadresse: @

Absender Anzeigename:

Benachrichtigungen an externe Empfänger

Absenderadresse: @

Absender Anzeigename:

Empfänger für administrative Benachrichtigungen

Empfängeradresse:

Speichern und schließen | Abbrechen und schließen

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:

Standard Domäneneinstellungen

Standard Domäneneinstellungen

Geben Sie E-Mail-Adressen für administrative Adressen an. Diese Einstellungen werden benutzt wenn keine domänenspezifischen Einstellungen konfiguriert sind.

Benachrichtigungen an Unternehmensbenutzer

Absenderadresse @

Absender Anzeigename

Benachrichtigungen an externe Empfänger

Absenderadresse @

Absender Anzeigename

Empfänger für administrative Benachrichtigungen

Empfängeradresse

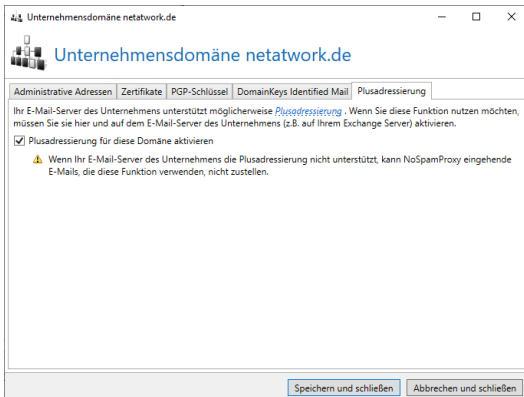
1. Gehen Sie zu **Identitäten > Unternehmensdomänen > Unternehmensdomänen**.
2. Klicken Sie **Standard-Domäneneinstellungen**.
3. Geben Sie die jeweiligen E-Mail-Adressen ein.
4. Klicken Sie **Speichern und schließen**.



TIP: 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, verworfene 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.



WARNING: 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**.



TIP: 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.

Unternehmensbenutzer

Unternehmensbenutzer repräsentieren die Mitglieder Ihrer Organisation.
 Suche nach Benutzern mit irgendwas im Namen, ihren Details oder E-Mail-Adressen und einem Status von jedem Status.

Suchen Parameter zurücksetzen

Eingeschaltet	Typ	Anzeigename	E-Mail-Adressen	Eingehende Inhaltsfilterung	Ausgehende Inhaltsfilterung	Flow Guard
✓	Manueller Benutzer	John Doe	john.doe@example.com	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Benutzer
✓	Manueller Benutzer	Max Mustermann	max.mustermann@example.com	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Benutzer

Hinzufügen Bearbeiten Entfernen Kryptographische Schlüssel für die markierten Benutzer beantragen [Automatischer Benutzerimport](#) Zeige Adresse 1 bis 2 Vorherige Seite Nächste Seite

Standardinstellungen für Benutzer
 Diese Einstellungen werden genutzt, falls keine spezifischeren Einstellungen auf dem Benutzer konfiguriert sind.
 Erlaube **jeden** Anhang an eingehenden E-Mails.
 Erlaube **jeden** Anhang an ausgehenden E-Mails.
 Benutzer können E-Mails an **beliebig viele** Empfänger pro 60 Minuten und an **beliebig viele** Empfänger pro 24 Stunden senden.
[Bearbeiten](#)

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.

I 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](#).
- **Bestimmte Inhaltsfilter als Standard festlegen**| Siehe [Standardeinstellungen für Benutzer konfigurieren](#).

I 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.



HINWEIS: Weitere Informationen zum Bearbeiten von Zertifikaten einer Benutzer E-Mail-Adresse finden Sie unter [Kryptographische Schlüssel für Domänen verwenden](#).

4. (Optional) Richten Sie Adressumschreibungen für die E-Mail-Adresse ein.
5. Wählen Sie den Inhaltsfilter, der dem Benutzer zugeordnet werden soll oder verwenden Sie die [Standardeinstellungen für Benutzer konfigurieren](#). Beachten Sie, dass Inhaltsfilter, die für Partner konfiguriert sind, ebenfalls angewendet werden. Für E-Mails, die vom Internet empfangen werden, werden die Inhaltsfilter des Partners sowie jedes einzelnen lokalen Empfängers kombiniert. Es werden dann die restriktivsten Einstellungen angewandt. Ausgehende Einstellungen werden unter Verwendung der Richtlinie für ausgehende E-Mails verarbeitet.
6. Bestimmen Sie über die Flow-Guard-Einstellungen, wie viele E-Mails der Benutzer senden kann.
7. Bestimmen Sie, ob der Name dieses Benutzers für die [CxO-Betrugserkennung](#) verwendet werden soll.
8. Wählen Sie die Sprachen für E-Mail-Benachrichtigungen und E-Mail-Hinweise.

9. (Optional) Bearbeiten Sie die für diesen Nutzer vorhandenen zusätzlichen Benutzerfelder.
10. Bestimmen Sie, welche De-Mail-Funktionen für diesen Benutzer verfügbar sein sollen.
11. 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.



HINWEIS: Nicht alle Active-Directory-Attribute werden in allen Szenarien mit NoSpamProxy synchronisiert. Das gleiche Verhalten tritt bei den zusätzlichen Benutzerfeldern auf. Ist der automatische Benutzerimport so konfiguriert, dass er den „Globalen Katalog“ verwendet, werden nur einige wenige Attribute vom Active Directory bereitgestellt. Um auf fehlende Attribute zuzugreifen, müssen Sie den Import auf die Verwendung des Standard Domain Controllers oder eines bestimmten Servers umstellen. Weitere Informationen finden Sie in der [Microsoft-Dokumentation](#).

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.



TIP: 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. Wählen Sie, ob Sie die Verbindung per TLS verschlüsseln wollen.
8. Wählen Sie die Art der Authentisierung und geben Sie die Anmeldedaten ein.
9. Wählen Sie den Bereich und welche Adressen importiert werden sollen (alle oder nur primäre Adressen).
10. Geben Sie unter **Gruppen** an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.

11. 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. Stellen Sie ein Zertifikat für die AAD-App-Registrierung bereit, indem Sie folgendes in PowerShell eingeben:

```
$newCertificate = New-SelfSignedCertificate -Subject "nospamproxy-userimport.example.com" -HashAlgorithm "SHA256" -KeyLength 4096 -KeySpec KeyExchange -NotAfter $((Get-Date).AddYears(30)) -KeyExportPolicy NonExportable
```
6. Geben Sie der Intranetrolle Leserechte für den privaten Schlüssel.
7. Legen Sie mit Hilfe des Zertifikats im AAD eine neue App-Registrierung an und weisen Sie folgende Rechte zu: **Microsoft Graph permission: Group.Read.All, User.Read, User.Read.All**
8. Wechseln Sie in das NCC und geben Sie Ihren Mandantennamen, die Client ID und das Zertifikat an.
9. Geben Sie unter **Gruppen** an, welche Funktionen jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.
10. (Optional) Weisen Sie unter **Zusätzliche Benutzerfelder** Werte aus dem Verzeichnis den zusätzlichen Benutzerfeldern zu.
11. 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.



TIP: 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**.



TIP: 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. 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.

6. (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.

7. (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.
8. Klicken Sie **Beenden**.



WARNING: 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 '%' 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**.

| Standardeinstellungen für Benutzer konfigurieren

Hier legen Sie fest, welche globalen Einstellungen für Benutzer angewendet werden, falls keine Einstellungen für individuelle 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).



HINWEIS: Beachten Sie, dass Inhaltsfilter, die für Partner konfiguriert sind, ebenfalls angewendet werden. Für E-Mails, die vom Internet empfangen werden, werden die Inhaltsfilter des Partners sowie jedes einzelnen lokalen Empfängers kombiniert. Es werden dann die restriktivsten Einstellungen angewandt. Ausgehende Einstellungen werden unter Verwendung der Richtlinie für ausgehende E-Mails verarbeitet.

4. Wählen Sie das gewünschte Verhalten des Flow Guard.
5. Wählen Sie die Sprachen für E-Mail-Benachrichtigungen und E-Mail-Hinweise.



HINWEIS: E-Mail-Benachrichtigungen werden in allen Sprachen angezeigt.

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

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.

Zusätzliche Benutzerfelder

Sie können für Ihre Benutzer zusätzliche Felder definieren. Diese Felder können in den Disclaimern als Platzhalter verwendet werden. Sie können den Feldern bei manuell erstellten Benutzern direkt Werte zuweisen. Alternativ können Sie dies im Automatischen Benutzer Import durchführen.

Name	Standardwert	Feldtyp
Abteilung		Standard
Bundesland		Standard
E-Mail		Standard
Faxnummer		Standard
Firma		Standard
Land		Standard
Mobiltelefon		Standard
Nachname		Standard
Postleitzahl		Standard
Stadt		Standard
Straße		Standard
Telefon		Standard
Titel		Standard
Vorname		Standard

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

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.

**TIP:**

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.

Partner

Suche nach Partnern mit [allem](#) im Domänennamen und einem [festen und abnehmenden](#) Vertrauensniveau.

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

Domänenname	Benutzereinträge	Eingehende Inhaltsfilterung	Ausgehende Inhaltsfilterung	URL Safeguard	Standardverschlüsselung
company.uno	20	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Partner
mx-ipaddress.test	0	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Partner
naw-mg.test	0	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Partner
spf.invalid.test	0	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Partner
spf.test	0	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Nutze übergeordnete Einstellungen	Standardeinstellungen für Partner

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#) Zeige Domäne 1 bis 5 [Vorherige Seite](#) [Nächste Seite](#)

Standardeinstellungen für Partner

Diese Einstellungen werden genutzt, falls kein Partnereintrag für eine spezifische Domäne oder E-Mail-Adresse vorhanden sind.

Erlaube **jeden** Anhang an eingehenden E-Mails.
Erlaube **jeden** Anhang an ausgehenden E-Mails.

URLs in vertrauenswürdigen E-Mails werden **beibehalten**.
URLs in nicht vertrauenswürdigen E-Mails werden **beibehalten**.
URL-Rückverfolgung ist **ausgeschaltet**.

Automatisch zwischen S/MIME und PGP wählen.
TLS-Zertifikate werden durch **DANE** überprüft falls das möglich ist.

[Bearbeiten](#)



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](#).

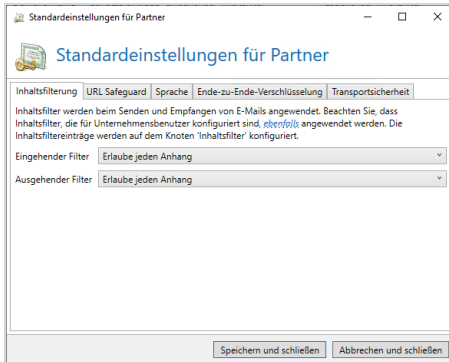
Benutzer hinzufügen| Neue Benutzer einer Domäne fügen Sie der entsprechenden Domäne als Benutzereintrag hinzu. Siehe [Benutzereinträge zu Partnerdomänen hinzufügen](#).

Standardeinstellungen für Partner

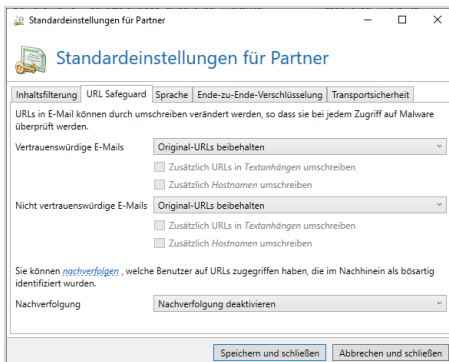
Unter **Identitäten > Partner > Standardeinstellungen für Partner** nehmen Sie Einstellungen vor, die angewendet werden, wenn keine Partnereinträge für eine Domäne oder E-Mail-Adresse vorhanden sind.

- 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.

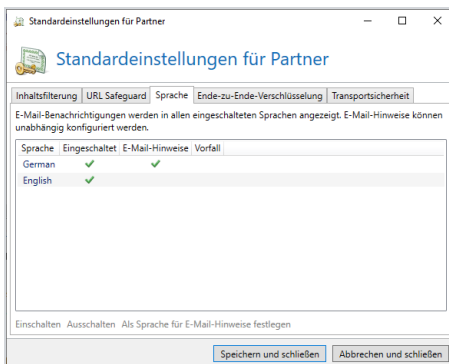


URL Safeguard | Konfigurieren Sie das grundlegende Verhalten des URL Safeguards für vertrauenswürdige und nicht vertrauenswürdige E-Mails. Bestimmen Sie außerdem, ob die Rückverfolgung ein- oder ausgeschaltet sein soll.



TIP: 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**.

Sprache| Wählen Sie die Sprachen für E-Mail-Benachrichtigungen und E-Mail-Hinweise



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.

I Partnerdomänen hinzufügen

Jede Partnerdomäne beinhaltet Einstellungen für Inhaltsfilter, 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](#).

5. Wählen Sie die Sprachen für E-Mail-Benachrichtigungen und E-Mail-Hinweise.
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.

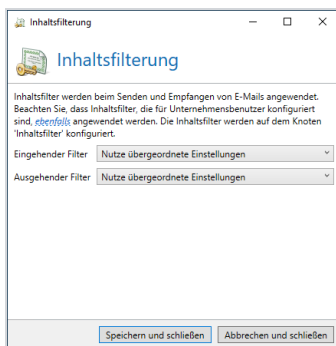


HINWEIS: Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielservers eingesetzt werden können. Zum Deaktivieren der Transportsicherheit entfernen Sie die Häkchen aus allen Kontrollkästchen.

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 **Fertigstellen**.

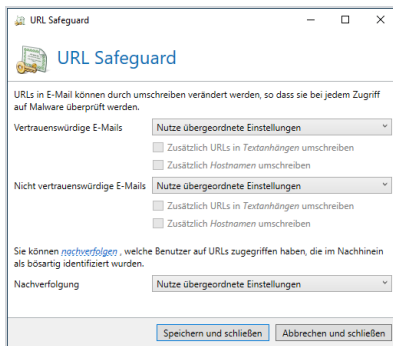
Partnerdomänen bearbeiten

1. Gehen Sie zu **Identitäten > Partner > Partner**.
2. Doppelklicken 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 unter URL Safeguard 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.



TIP: 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. Wählen Sie die Sprachen für E-Mail-Benachrichtigungen und E-Mail-Hinweise.
6. 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](#).
7. Klicken Sie **Dialog schließen**.

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

I 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](#).

7. 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.

E-Mail-Authentifizierung

The screenshot shows the NoSpamProxy Command Center interface. On the left is a navigation menu with categories: Übersicht, Monitoring, Identitäten, Konfiguration, and Troubleshooting. The 'Identitäten' section is expanded, showing options like Unternehmensdomänen, Unternehmensbenutzer, Partner, Zertifikate, PGP-Schlüssel, Öffentliche Schlüsselserver, Schlüsselanforderung, E-Mail-Authentifizierung, and Zusätzliche Benutzerfelder. The main content area is divided into two sections: 'DKIM-Schlüssel' and 'Vertrauenswürdige ARC-Unterzeichner'. The 'DKIM-Schlüssel' section includes a table with columns 'Domäne', 'Name', 'Zugeordnete Domänen', and 'Status'. The table contains two entries: 'example.com' with 'example' and '2' associated domains, and 'example.local' with 'exampletwo'. Below the table are links for 'Hinzufügen', 'Details', 'Entfernen', 'Schlüssel importieren', and 'Schlüssel exportieren'. The 'Vertrauenswürdige ARC-Unterzeichner' section includes a description of ARC, a 'Kuratiertes Liste von Unterzeichnern' section with a 'Bearbeiten' link, and a 'Zusätzliche ARC-Unterzeichner' section with a search input field and 'Suchen' and 'Parameter zurücksetzen' buttons.

Domäne	Name	Zugeordnete Domänen	Status
example.com	example	2	
example.local	exampletwo		

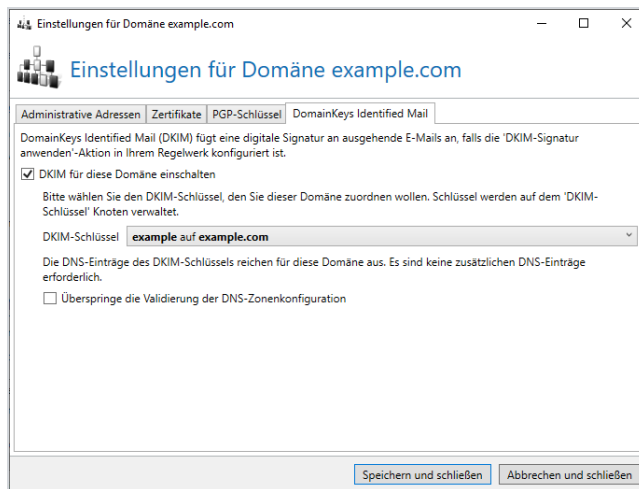
DomainKeys Identified Mail (DKIM)

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.

**WARNING:**

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

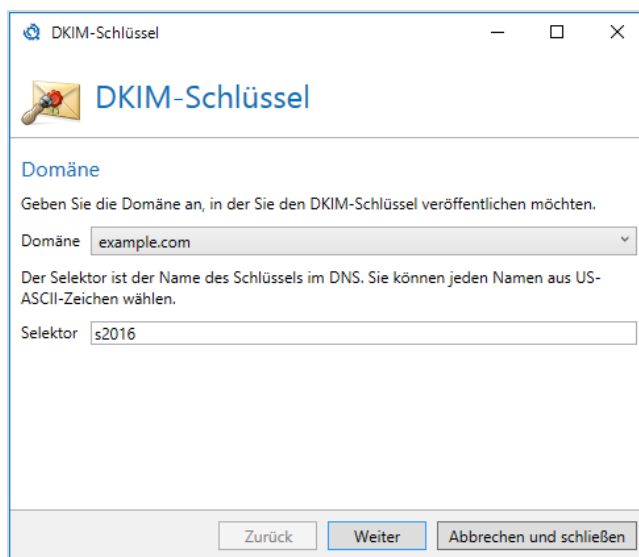
DomainKeys Identified Mail (DKIM) sichert ausgehende E-Mails mit einer elektronischen Signatur. Durch die Auswertung dieser Signatur kann der Empfänger erkennen, ob die E-Mail von der richtigen Domäne versandt wurde (Sicherstellen der Authentizität) und ob sie während des Transports verändert wurde (Sicherstellen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



DKIM-Schlüssel

DKIM-Schlüssel

Domäne

Geben Sie die Domäne an, in der Sie den DKIM-Schlüssel veröffentlichen möchten.

Domäne

Der Selektor ist der Name des Schlüssels im DNS. Sie können jeden Namen aus US-ASCII-Zeichen wählen.

Selektor

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.



TIP: 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



TIP: 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>.

DKIM-Schlüssel

DKIM-Schlüssel

Bitte veröffentlichen Sie diesen Eintrag in der DNS-Zone für `example.com`.

```
key2018r. domainkey IN TXT "v=DKIM1; k=rsa;  
p=  
key2018e. domainkey IN TXT "v=DKIM1; k=ed25519;  
p="
```

[In die Zwischenablage kopieren](#)

Sobald Sie den oben stehenden DNS-Eintrag veröffentlicht haben, können Sie Ihre Konfiguration validieren.

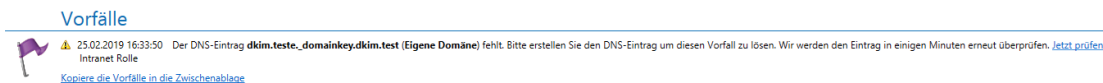
[Eintrag validieren](#)

Schließen

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-Schlüssel im EdDSA-Format benutzt wird aber noch nicht veröffentlicht 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=MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ

EAzvf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstllgGY

XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw

P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy

J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH6kQ+SEc

a0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6FpneHXCfAY6m

OI6vykkmVfb/MAR9CZFKrWY+17dPHDhKJDEwsQymCGUu

GwzLwIPcjLVbMSQGXRtdWy8cJbeOa+iO2Gwp4yS2urmT

/k8aK4256GhSQbBH3HOCxRgNL3Yb4G1mo92QIDAQAB"
```

Zu verwendender Schlüssel im DNS (mit Umbruch)

```
"v=DKIM1; k=rsa;

p=MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ

EAzvf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstllgGY

XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw

P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy

J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH"

"6kQ+SEca0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6Fpne

HXCfAY6mOI6vykkmVfb/MAR9CZFKrWY+17dPHDhKJDEw
```

```
sQymCGUuGwzLwIPcjLVbMSQGXRtdWy8cJbeOa+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](#)

Konfiguration

Dieser Bereich bietet Ihnen Zugriff auf Einstellungen für die Verbindung zu anderen Rollen, Einstellungen der Datenbank sowie Benachrichtigungsadressen.

E-Mail-Routing einrichten	102
E-Mail-Server des Unternehmens hinzufügen	102
Eingehende Sendekonnektoren anlegen	109
Ausgehende Sendekonnektoren anlegen	111
Empfangskonnektoren anlegen	119
Ungültige Anfragen bei SMTP-Empfangskonnektoren	120
Zustellung über Warteschlangen	122
Headerbasiertes Routing einrichten	124
Regeln erstellen	125
Allgemeine Informationen	125
Schritte beim Erstellen	127
Verwandte Themen	133
NoSpamProxy-Komponenten	137
Intranetrolle	138
Gatewayrolle	139
Web Portal	149
Datenbanken	160
Ändern des Web Ports	182
Verbundene Systeme	184
DNS-Server	184
Archivkonnektoren	186
De-Mail über Mentana-Claimsoft	190
CSA Certified IP List	191

Benutzerbenachrichtigungen	193
Prüfbericht	193
E-Mail-Benachrichtigungen	196
Benutzerbenachrichtigungen anpassen	197
Vorgehen nach Updates	198
Unterschiedliche Designs bei Absenderdomänen verwenden	205
Voreinstellungen	215
Branding	216
Wortübereinstimmungen	217
Realtime Blocklists	219
Erweiterte Einstellungen	221
Schutz sensibler Daten	222
Monitoring	224
Betreffkennzeichnungen	227
Level-of-Trust-Konfiguration	233
SMTP-Protokolleinstellungen	240
SSL-/TLS-Konfiguration	248

E-Mail-Routing einrichten

The screenshot shows the NoSpamProxy Command Center interface. The left sidebar contains navigation options: Übersicht, Monitoring, Identitäten, Konfiguration, E-Mail-Routing, Regeln, Inhaltsfilter, URL Safeguard, NoSpamProxy Komponenten, Verbundene Systeme, Benutzer-Benachrichtigungen, Voreinstellungen, Erweiterte Einstellungen, and Troubleshooting. The main content area is titled 'E-Mail-Server des Unternehmens' and contains four sections: 'E-Mail-Server des Unternehmens', 'Eingehende Sendekonnektoren', 'Ausgehende Sendekonnektoren', and 'Empfangskonnektoren'. Each section includes a table of configured connectors and their properties.

E-Mail-Server des Unternehmens
Die unten aufgeführten Server dürfen ausgehende E-Mails unter Verwendung von Unternehmensdomänen in der Absenderadresse versenden.

Typ	Details	Erlaubte Domänen	Kommentar
DNS-Name	localhost	Alle	

Eingehende Sendekonnektoren
Eingehende E-Mails werden durch die unten definierten Konnektoren geleitet. Falls mehrere Konnektoren für das Routing einer E-Mail geeignet sind, wird der kostengünstigste gewählt.

Typ	Name	Zuordnung	Kosten	DNS-Routingbeschränkungen
SM...	Default inbound connector	✓ INSTALLATION	100	Von * an *

Ausgehende Sendekonnektoren
E-Mails in das Internet werden durch die unten definierten Konnektoren geleitet. Falls mehrere Konnektoren für das Routing einer E-Mail geeignet sind, wird der kostengünstigste gewählt.

Typ	Name	Zuordnung	Zustellmethode	Kosten	DNS-Routingbeschränkungen
SM...	Default connector for outbound mails	✓ INSTALLATION	Direkte Zustellung über DNS	100	Von * an *

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

Typ	Name	Zuordnung	Bindung	Zusätzliche Einstellungen	Verbindungssicherheit
SM...	SMTP on all addresses	✓ INSTALLATION	Alle : 25	Blockierung ist 30 Minuten Tarppingniveau ist mittel	⚠ Ausgeschaltet

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 DNS-Hostname

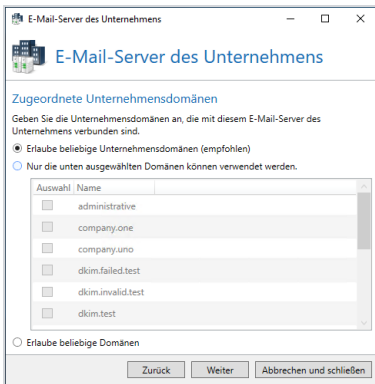
Ein Server gilt hier als E-Mail-Server des Unternehmens, sofern er

- 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**.



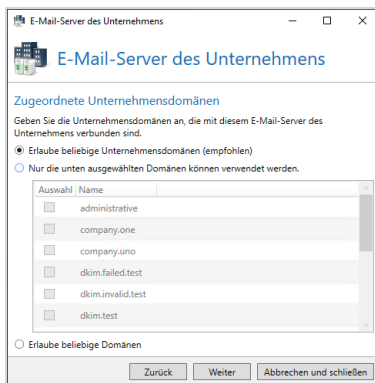
6. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie **Fertigstellen**.

Hinzufügen als TLS-authentifizierter Host

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**.

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



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

Hinzufügen als Office-365-Mandant

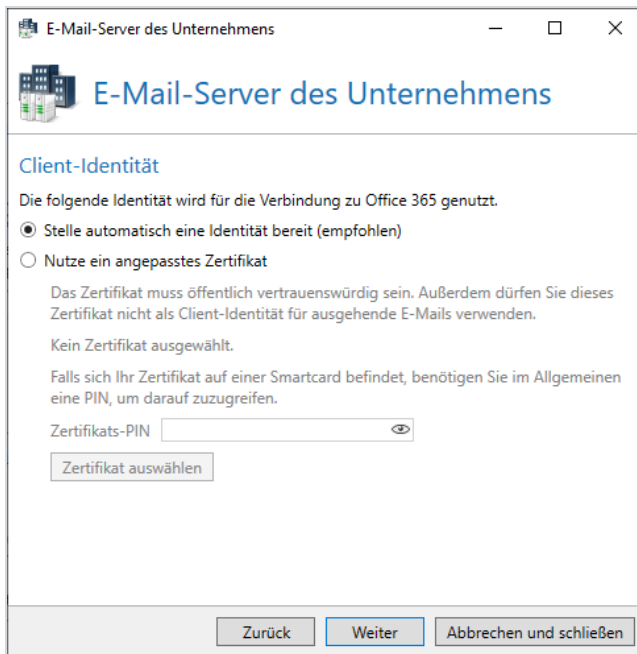
Ein Server gilt hier als E-Mail-Server des Unternehmens, wenn es sich um einen offiziellen Office-365-Server handelt.



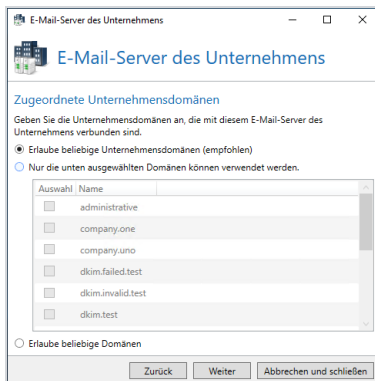
HINWEIS: Wenn Sie Office 365 als E-Mail-Server des Unternehmens konfigurieren, wird ein Sendekonnektor für Office 365 konfiguriert.

- Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
- Klicken Sie **Hinzufügen**.
- Wählen Sie den **Als Office-365-Mandant** aus und klicken Sie **Weiter**.
- 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**.



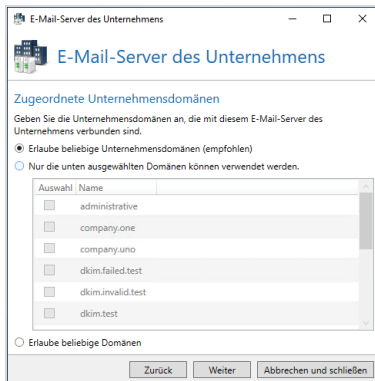
HINWEIS: Durch das Hinzufügen Ihres Office-365-Mandanten wird das erforderliche E-Mail-Routing in NoSpamProxy Server bereits angelegt. Sie müssen nun den Nachrichtenfluss in Microsoft Exchange Online einrichten, indem Sie das bereitgestellte PowerShell-Skript ausführen oder die Einrichtung manuell vornehmen. 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 Benutzername und Passwort (SMTP AUTH)

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 **Benutzername und Passwort (SMTP AUTH)** 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**.



HINWEIS:

- Für das Einbinden von Servern mit SMTP-Authentifizierung ist eine TLS-gesicherte Verbindung erforderlich.
- NoSpamProxy unterstützt die Authentifizierungs-Verfahren **AUTH** und **LOGIN**.

Hinzufügen über eine bestimmte Absenderadresse

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



WARNING: 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.

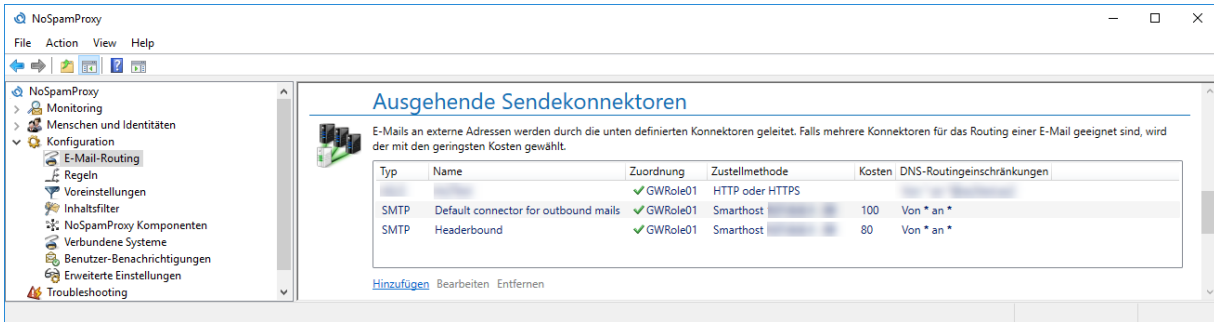
Werden eine oder mehrere weitere Gatewayrollen hinzugefügt, tritt das folgende (erwünschte) Verhalten auf:

- 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 Mentana-Claimsoft GmbH anlegen



HINWEIS: Für die Anbindung an Mentana-Claimsoft De-Mail müssen Sie unter Verbundene Systeme einen 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 Kosten gesendet werden. Des Weiteren können Sie auf dieser Seite festlegen, wie E-Mails zugestellt werden. Einerseits können die E-Mails direkt zugestellt werden, andererseits, und das ist die empfohlene Möglichkeit, kann ein Smarthost verwendet werden. Ein solcher Smarthost wird vom DOI-Netz zur Verfügung gestellt.

Ausgehender Sendekonnektor

DOI Zustellung

Ungültige Sender für DOI

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

Ersatzverhalten Abweisen der E-Mail Senden durch den Standard Konnektor

Routing-Methode

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

Methode Direkte Zustellung Zustellung über einen dedizierten Server

Dedizierter Server (Smarthost)

Zurück Weiter Abbrechen und schließen

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.

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.



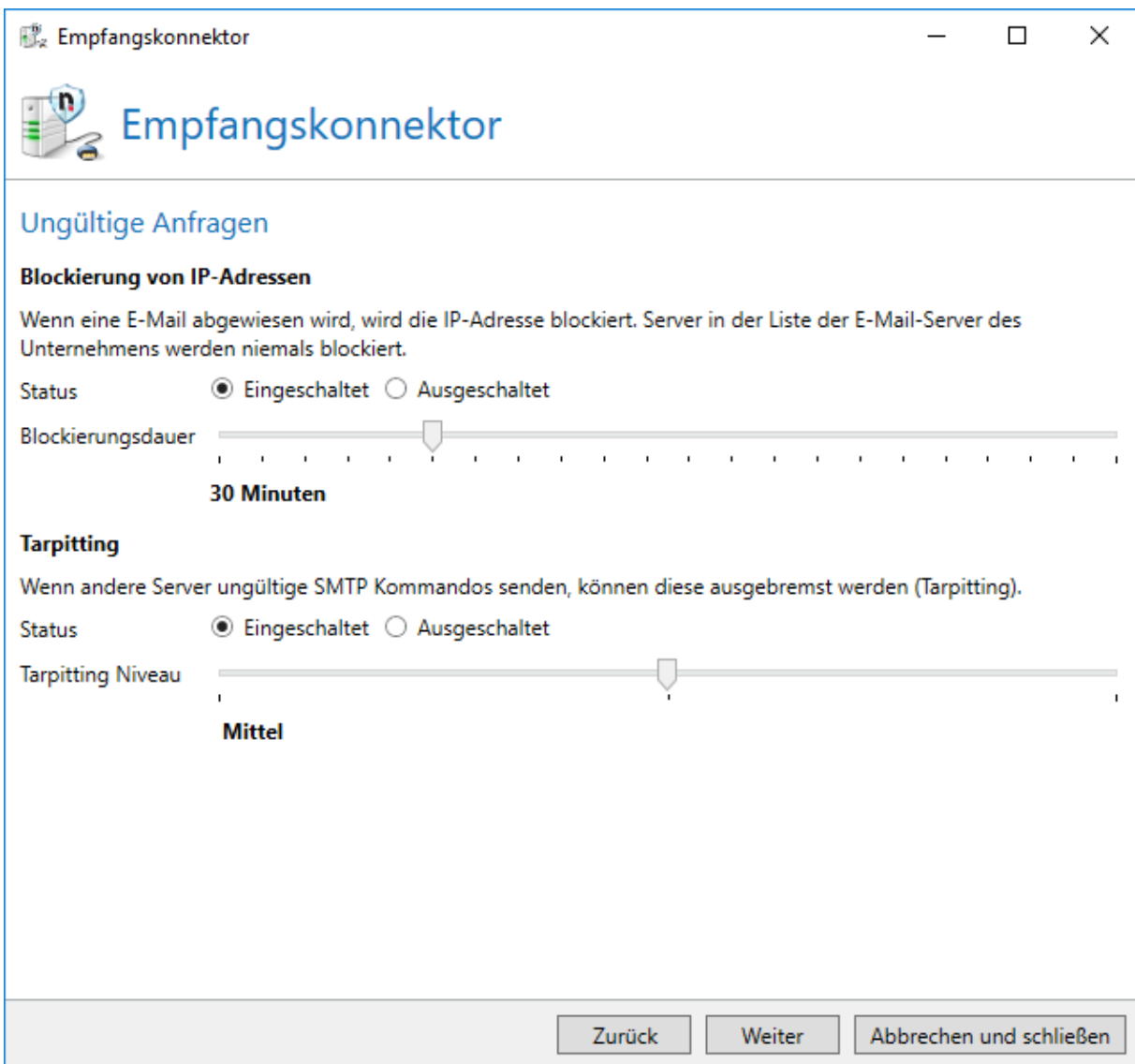
HINWEIS: Wenn Sie mehrere Gatewayrollen ausgewählt haben, dann können Sie keine Bindung auf einzelne IP-Adressen durchführen. Wählen Sie in diesem Fall **Alle** oder **Loopback** aus.

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**.

I 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



The screenshot shows a Windows-style window titled 'Empfangskonnektor'. Below the title bar is a header with a server icon and the text 'Empfangskonnektor'. The main content area is titled 'Ungültige Anfragen' and contains two sections:

- Blockierung von IP-Adressen**: A sub-header followed by a descriptive sentence: 'Wenn eine E-Mail abgewiesen wird, wird die IP-Adresse blockiert. Server in der Liste der E-Mail-Server des Unternehmens werden niemals blockiert.' Below this is a 'Status' row with radio buttons for 'Eingeschaltet' (selected) and 'Ausgeschaltet'. A 'Blockierungsdauer' slider is positioned below, with a value of '30 Minuten' displayed.
- Tarpitting**: A sub-header followed by a descriptive sentence: 'Wenn andere Server ungültige SMTP Kommandos senden, können diese ausgebremst werden (Tarpitting)'. Below this is a 'Status' row with radio buttons for 'Eingeschaltet' (selected) and 'Ausgeschaltet'. A 'Tarpitting Niveau' slider is positioned below, with a value of 'Mittel' displayed.

At the bottom of the window, there are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

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 Smarhosts zuzustellen. Die Reihenfolge ist hierbei weder konfigurierbar noch vom Benutzer beeinflussbar. Sobald ein Smarhost die E-Mail empfängt, ist die E-Mail erfolgreich zugestellt.

Konfiguration des Smarhost| Die Konfiguration eines Smarhosts für die lokale Zustellung läuft ab, wie im Kapitel Smarhost: E-Mail-Zustellung über dedizierten Server beschrieben. Der Sendekonnektor für lokale Adressen nutzt in der Verbindungssicherheit eine Client-Identität.

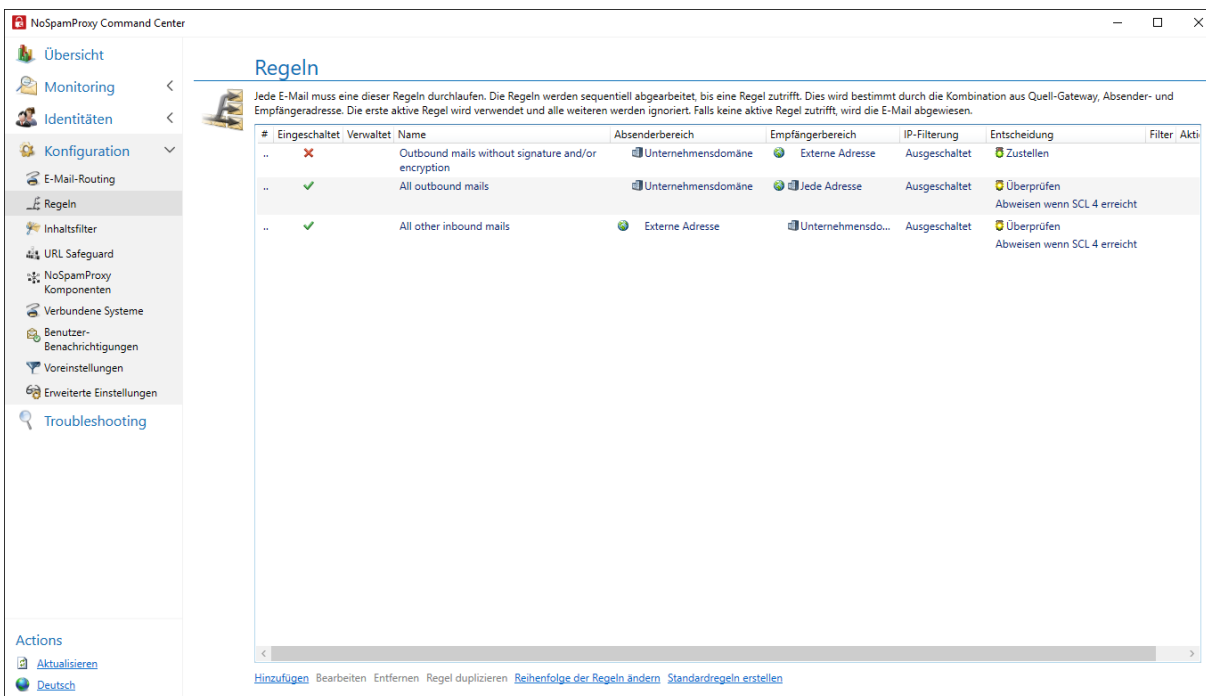
DNS-Routing-Einschränkungen| Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter DNS Routing Einschränkungen. Die Konfiguration der Einschränkungen für die lokale Zustellung läuft ab, wie unter DNS-Routing-Einschränkungen durch Konnektor-Namensräume beschrieben.

| 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.



TIP: 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 **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 Virens Scanner 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.

I 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.

Regel #5: Neue Regel

Regel #5: Neue Regel

Allgemein

Name

Status Eingeschaltet Ausgeschaltet

Regelindex ist **5**

Level of Trust System Eingeschaltet Ausgeschaltet

Inhaltsfilterung Eingeschaltet Ausgeschaltet

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

Kommentar

Zurück Weiter Abbrechen und schließen

Name| Vergeben Sie einen eindeutigen Namen für die Regel.

Status| Schalten Sie die Regel ein oder aus.

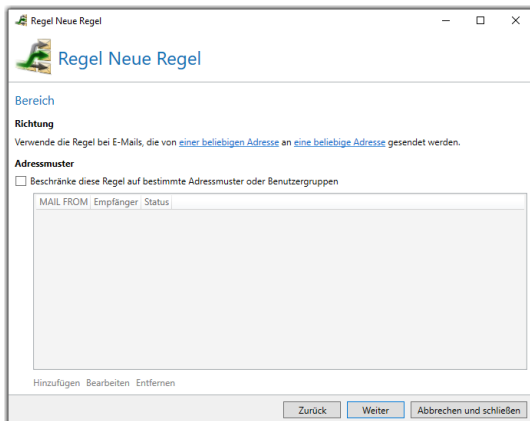
Regelindex| Legen Sie fest, an welcher Position innerhalb der Rangliste sich die Regel befinden soll.

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](#).

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.

Regel #5: Neue Regel

Regel #5: Neue Regel

IP-Filterung

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

IP-Adresse oder Subnetz

Serveradresse

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.

I Nächste Schritte

Wenn Sie gerade dabei sind, eine neue Regel zu erstellen, wählen Sie jetzt die Filter aus. Siehe [Filter konfigurieren](#).

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**.

I 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.



TIP: 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.

EXAMPLE:

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.

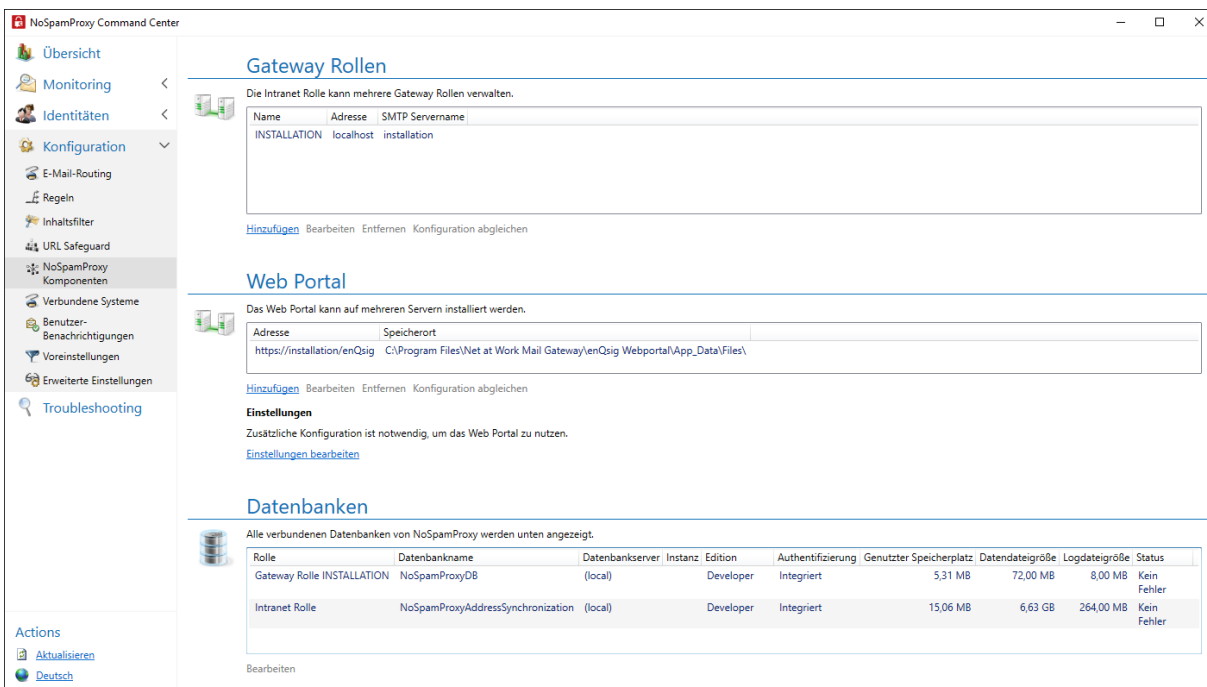
Das Level-of-Trust-System hat immer einen Multiplikator; dieser Multiplikator setzt sich zusammen aus

- 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 $6+2 \cdot -4$. Damit ergibt sich ein SCL von -2. Die E-Mail würde NoSpamProxy Protection passieren.

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\

I 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 entsprechende 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 entsprechenden Benutzern die gewünschten Rollen zu.
4. Melden Sie sich einmal von Windows ab und mit dem entsprechenden Benutzer wieder an, um die hinzugefügten Rechte zu nutzen.

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.

I 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.



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.

EXAMPLE: 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**.

Gateway Rolle

Gateway Rolle auf dem Server **localhost**

Name

Der SMTP Servername sollte mit Ihrem MX-Eintrag übereinstimmen.

SMTP Servername

[Finde die DNS-Einstellungen heraus](#)

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**.

The screenshot shows a configuration interface with two main sections:

- Basic Sensor Settings:**
 - Sensor Name: NoSpamProxy Queue momentan Aktiv
 - Parent Tags: nav_nospamproxy Windows NSP enqsig SMTP mail
 - Tags: performancecounter x performancecountercustom x
 - Priority: ★★☆☆☆
 - Buttons: Create, Refresh
- Performance Counter Settings:**
 - List of Counters: \NoSpamProxy Queues(_total)\Currently active
 - Mode:
 - Absolute (recommended)
 - Difference

At the bottom, there is a section for **Scanning Interval**.

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.

EXAMPLE: `<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="AnzahlDerVerbindungen" />
```

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 maximale Limit an Verbindungen fest.
- Der Wert `minimumNumberOfConcurrentSessions` bestimmt die minimale Anzahl von gleichzeitigen Verbindungen.

EXAMPLE: `<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

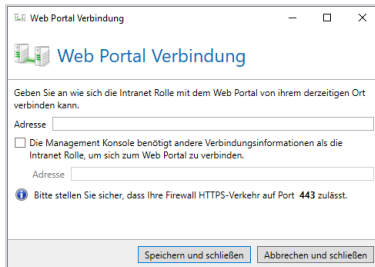


HINWEIS: Um ein hochverfügbares System aufzubauen, kann das Webportal auf mehreren Servern installiert werden.

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.

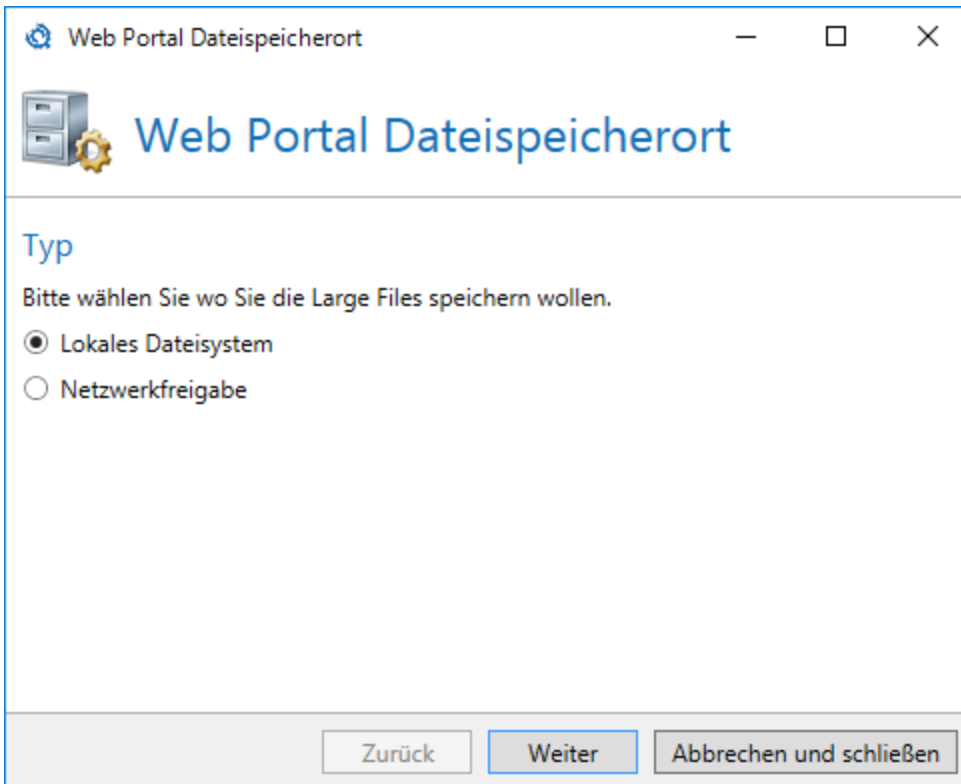
- Klicken Sie in diesem Fall **Konfiguration abgleichen**, um die Konfiguration mit den markierten Webportalen zu synchronisieren.



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 derzeitigen Einstellungen für das Webportal angezeigt.

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

Registerkarte Allgemein

Web Portal Einstellungen

Web Portal Einstellungen

Allgemein PDF Mail Large Files

Die Adresse des Web Portals wird bei externen E-Mail-Empfängern genutzt.

Adressen des Portals

Externe HTTPS-Adresse

Benutze eine andere Adresse für Zugriffe von innerhalb Ihres Unternehmens

Interne HTTPS-Adresse

Sichere Web Mails

Erlaube sichere Web Mails ohne Einladungslink

Die Adresse <https://webportal.mailgateway.test/enQsig/mail/new> kann durch Ihre Partner genutzt werden.

Speichern und schließen Abbrechen und schließen

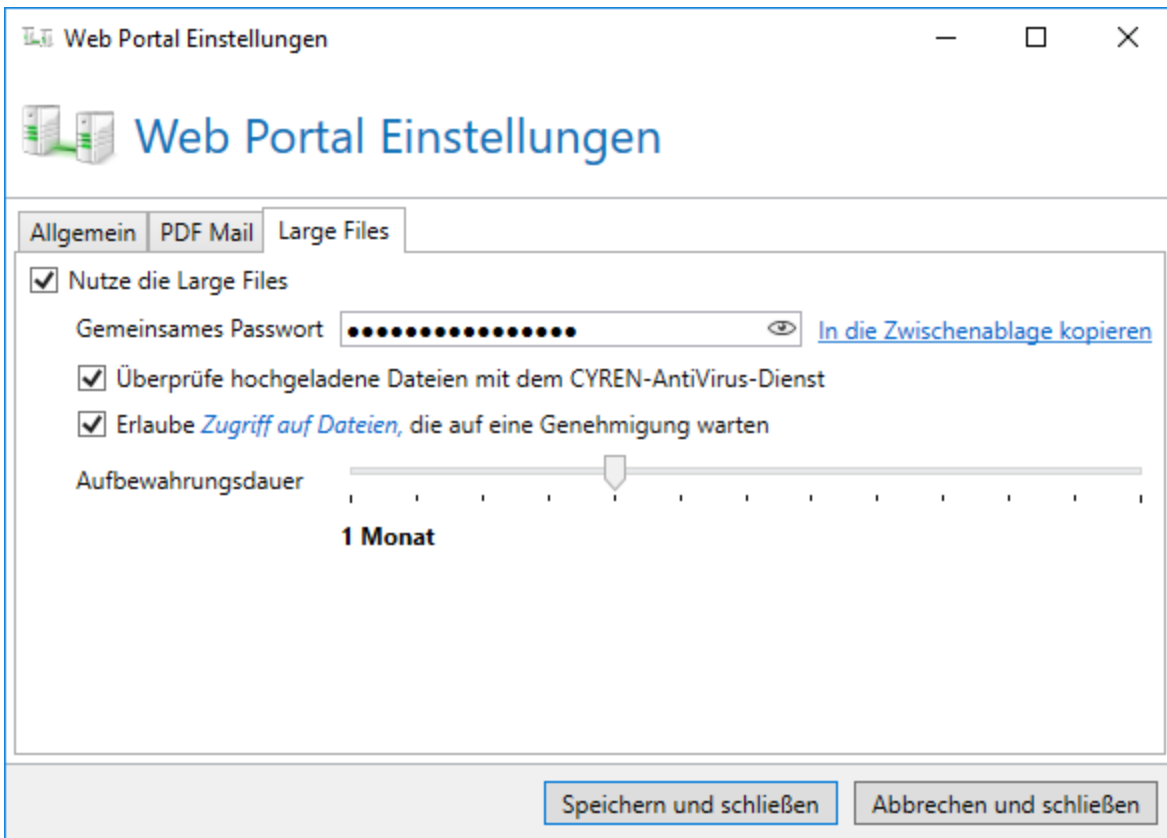
Adressen des Portals| Bei Benutzung des Web Portals wird in E-Mails gegebenenfalls ein Link auf das Web Portal eingefügt. Der Link beinhaltet dabei die Adresse, unter der das Web Portal aus dem Internet erreichbar ist

- 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.



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

In diesem Fall müssen Sie die Hostnamen der Local Security Authority erstellen, auf die in einer NTLM-Authentifizierungsanfrage verwiesen werden kann. Führen Sie dazu die folgenden Schritte für alle Knoten auf dem Clientcomputer aus:

1. Drücken Sie **Windows + R**, um **Ausführen** zu öffnen.
2. Geben Sie **regedit** ein und klicken Sie dann **OK**.
3. Suchen Sie den folgenden Registrierungsunterschlüssel und klicken Sie darauf: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**.
4. Klicken Sie mit der rechten Maustaste auf **MSV1_0**, zeigen Sie auf **Neu** und klicken Sie dann **Wert der mehrteiligen Zeichenfolge**.



HINWEIS: Die angezeigte Fehlermeldung können Sie ignorieren.

5. Geben Sie in der Spalte Name **BackConnectionHostNames** ein und drücken Sie dann **Enter**.

6. Klicken Sie mit der rechten Maustaste auf **BackConnectionHostNames** und klicken Sie dann **Ändern**.
7. Geben Sie in das Datenfeld Wert den **CNAME** oder den **DNS-Alias** ein, der für die lokalen Freigaben auf dem Computer verwendet wird.
8. Klicken Sie **OK**.
9. Beenden Sie den Registrierungseditor und starten Sie den Computer neu.



HINWEIS:

- Geben Sie jeden Hostnamen in eine eigene Zeile ein.
- Wenn der Registrierungseintrag **BackConnectionHostNames** als REG_DWORD-Typ existiert, müssen Sie den Registrierungseintrag **BackConnectionHostNames** löschen.
- Beachten Sie hierzu auch den [Artikel KB926642 in der Microsoft-Dokumentation](#).

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:

```

```

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

I 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

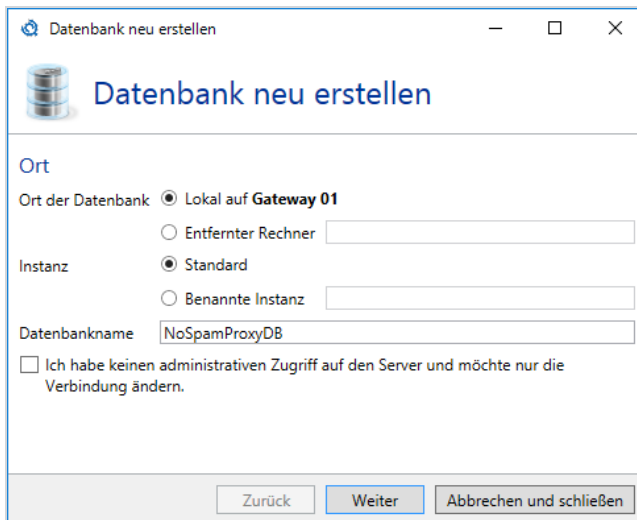


HINWEIS: Bevor Sie die Verbindungseinstellungen ändern, sichern Sie die bestehende Datenbank und spielen Sie diese Sicherung auf dem neuen Datenbank-Server ein.



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 Domännennamen (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 klicken

Sie **Weiter**.

Datenbank neu erstellen

Datenbank neu erstellen

Administrative Authentifizierung

Ihre derzeitigen Benutzerinformationen können nicht genutzt werden um die Datenbank zu konfigurieren. Bitte geben Sie administrative Benutzerinformationen ein.

Typ Windows SQL Server

Benutzername

Passwort

Zurück Weiter Abbrechen und schließen

- 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.

- Wählen Sie auf der nächsten Seite die gewünschte Aktion aus. Abhängig von den verfügbaren Datenbanken stehen hier unterschiedliche Optionen zur Verfügung.
- 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:

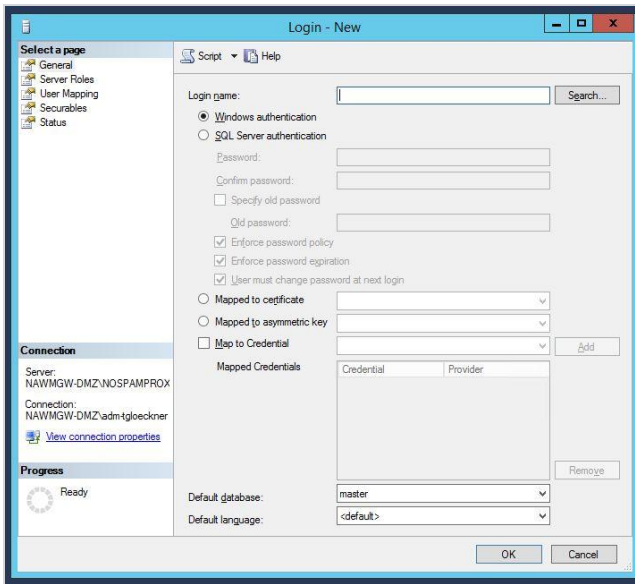


HINWEIS:

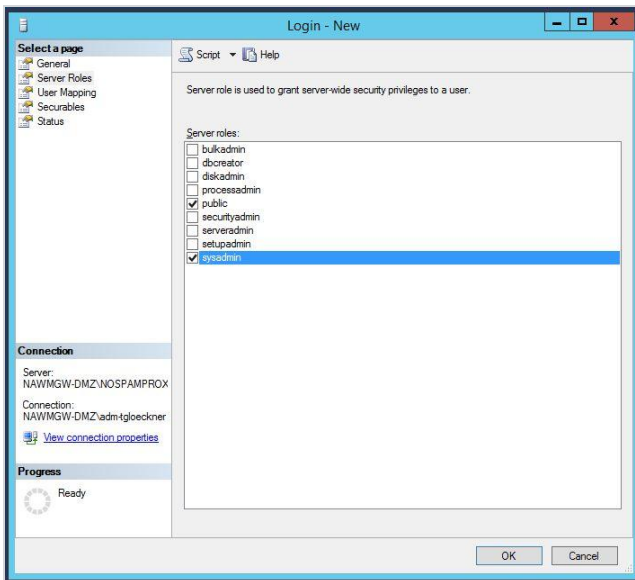
- Alle Schritte gelten für alle Rollen von NoSpamProxy; sie unterscheiden sich nur in den Datenbanknamen.
 - Datenbank Intranetrolle: NoSpamProxyIntranetRole
 - Datenbank Gatewayrolle: NoSpamProxyGatewayRole
 - Datenbank Web Portal: NoSpamProxyWebPortal
- Es können Benutzer sowie Benutzergruppen (lokal 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

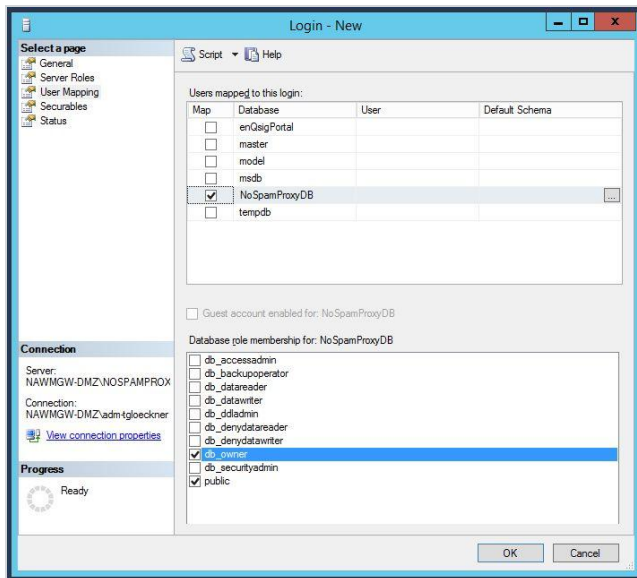
Authentication”) bei.



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
LegacyMessage Track...	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.



WARNING: 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.

The screenshot shows the NoSpamProxy Command Center interface. The sidebar on the left contains the following menu items: Übersicht, Monitoring, Identitäten, Konfiguration (with a dropdown arrow), E-Mail-Routing, Regeln, Inhaltsfilter, URL Safeguard, NoSpamProxy Komponenten, **Verbundene Systeme** (highlighted), Benutzer-Benachrichtigungen, Voreinstellungen, Erweiterte Einstellungen, and Troubleshooting. Below the sidebar are 'Actions' for 'Aktualisieren' and 'Deutsch'. The main content area is titled 'Verbundene Systeme' and contains the following sections:

- DNS-Server**: Externe DNS-Abfragen können entweder durch die DNS-Server, die in Windows konfiguriert wurden, durchgeführt werden oder durch einen Server eines Drittanbieters. Bedenken Sie, dass Funktionen wie DANE einen DNSSEC-fähigen DNS-Server benötigen. Der Server der in **Windows** konfiguriert ist, wird für externe DNS-Auflösung genutzt. [Bearbeiten](#)
- SMS-Anbieter**: Sie können Profile für SMS-Anbieter definieren.

Profilname	Name	Absender	Standard Ländervorwahl
<input type="text"/>			

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)
- Archivkonnektoren**: Ein Archivkonnektor stellt eine Verbindung zwischen der Gateway Rolle und einem Archiv her. Jeder Konnektor besitzt ein oder mehrere Profile, die angeben wie E-Mails archiviert werden.

Konnektorname	Profil	Profilanzahl
<input type="text"/>		

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)
- De-Mail-Anbieter**: **Telekom De-Mail-Verbindungen**: Die Anbieter werden verwendet, um sich mit den Telekom-De-Mail-Gateways zu verbinden.

Name	Zertifikat	Gateway Rolle	Ziel	Domänen
<input type="text"/>				

[Hinzufügen](#) [Bearbeiten](#) [Entfernen](#)
Verbindung zu Mentana-Claimssoft: Es wurden bis jetzt noch keine Verbindungen konfiguriert. [Hinzufügen](#)
- digiSeal server Verbindung**: Es wurden bis jetzt noch keine Verbindungen konfiguriert. [Bearbeiten](#)
- CSA Whitelist**: Die CSA Whitelist wird alle 24 Stunden heruntergeladen. [Bearbeiten](#) [CSA Whitelist jetzt herunterladen](#)

DNS-Server

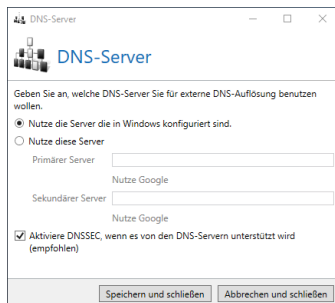
Beim Einsatz von DANE benötigen Sie einen DNS-Server, der DNSSEC unterstützt. Da die in Windows-Server-Betriebssystemen mitgelieferten DNS-Server diese Funktion derzeit nicht unterstützen, können Sie hier eine Verbindung zu einem solchen Server einrichten.



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.



TIP: 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.

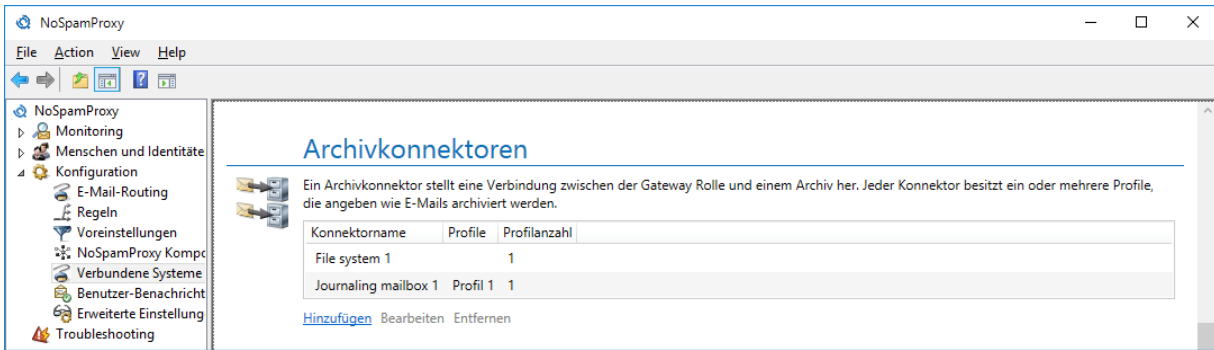
5. Klicken Sie **Speichern und schließen**.



HINWEIS: DANE wird für die Überprüfung der Transportverschlüsselung bei der Zustellung von E-Mails zu Ihren Partnern verwendet. Siehe [Standardeinstellungen für Partner](#).

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.

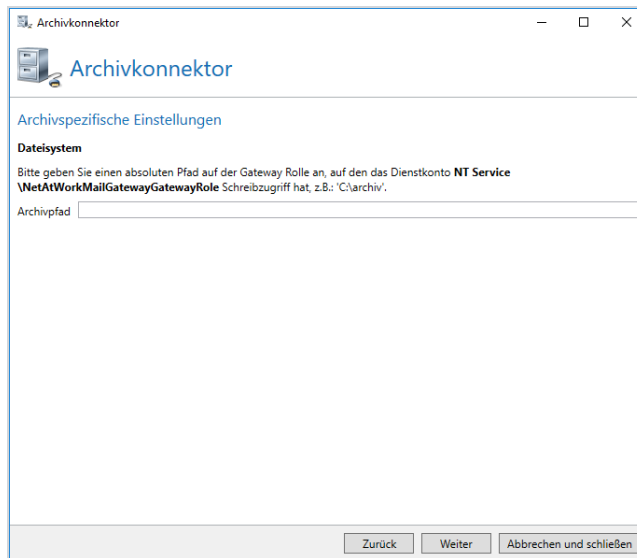


HINWEIS: E-Mails werden so archiviert, wie sie von NoSpamProxy empfangen werden. NoSpamProxy nimmt weder eine Ver- oder Entschlüsselung vor noch lädt NoSpamProxy Anhänge in das Webportal. Beachten Sie, dass E-Mails nur dann archiviert werden, wenn NoSpamProxy die E-Mail nicht ablehnt. Schlägt beispielsweise der Malwarescanner an oder kann die E-Mail nicht entschlüsselt werden, so wird die jeweilige E-Mail nicht archiviert.

Archivkonnektoren konfigurieren

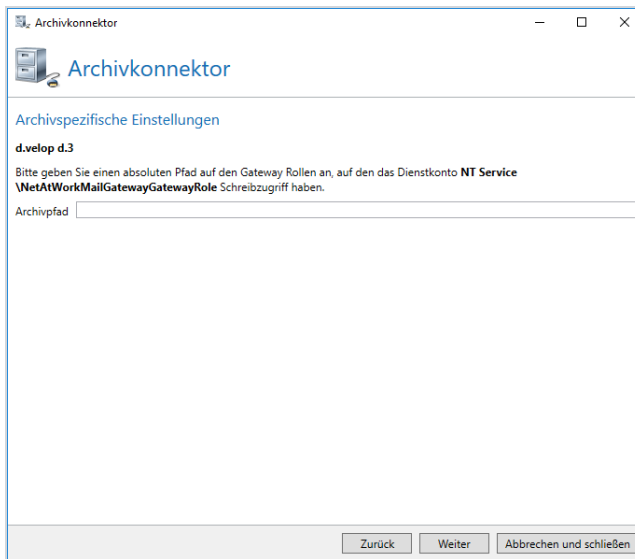
1. Gehen Sie zu **Konfiguration > Verbundene Systeme > Archivkonnektoren**.
2. Klicken Sie **Hinzufügen**.

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.

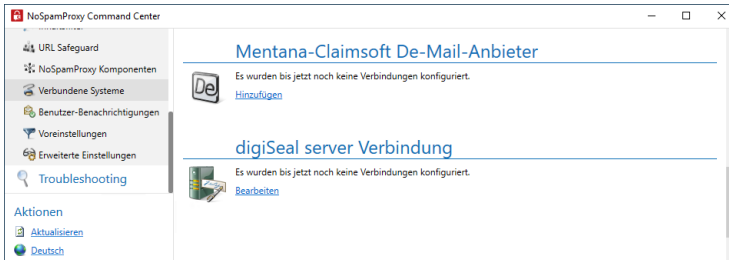


HINWEIS: Profile ermöglichen es Ihnen zum Beispiel, E-Mails und Dokumente innerhalb eines Archivsystems auf verschiedene Ordner zu verteilen. Geben Sie dem neuen Profil einen Namen und Sie aus, welche E-Mails durch dieses Profil archiviert werden. Beachten Sie, dass E-Mails mit einem qualifiziert signierten Anhang immer archiviert werden. Sie können optional auch alle anderen E-Mails archivieren.

6. Klicken Sie **Fertigstellen**.

De-Mail über Mentana-Claimsoft

Hier können Sie die Verbindungen zum De-Mail-System über Mentana-Claimsoft hinterlegen.



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 > Mentana-Claimsoft De-Mail-Anbieter**.
2. Klicken Sie **Hinzufügen**.

The dialog box is titled 'Verbindung zu Mentana-Claimsoft'. It contains a 'De' icon and the title. Below the icon, it asks the user to provide the service address: 'Bitte geben Sie die Adresse Ihres Mentana-Claimsoft-Web-Services an.' The 'Dienstadresse' field contains 'https://mentana.example.com:8989/'. Below this, it asks for user information: 'Benutzerinformationen werden für die erfolgreicher Verbindung zum Webservice benötigt.' The 'Benutzername' field contains 'user' and the 'Passwort' field is masked with dots. At the bottom, there are two buttons: 'Speichern und schließen' and 'Abbrechen und schließen'.

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.

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**.



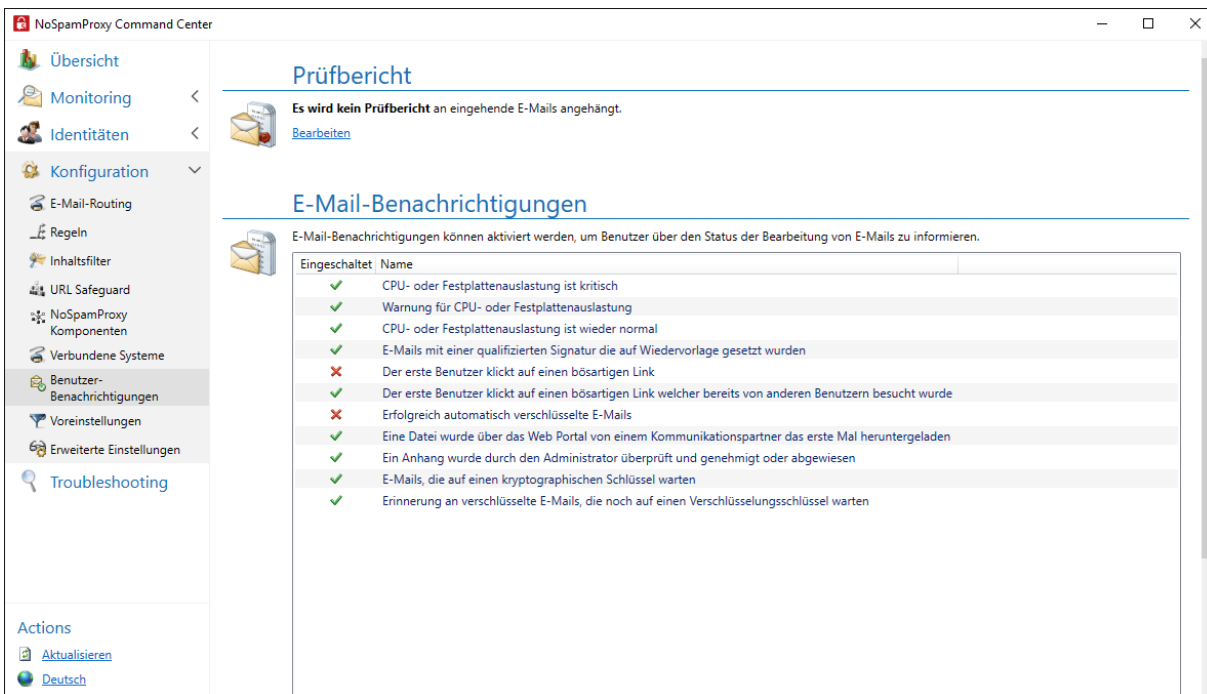
HINWEIS: Um die CSA Certified IP List manuell herunterzuladen, klicken Sie **CSA Certified IP List jetzt herunterladen** unter **Konfiguration > Verbundene Systeme > CSA Certified IP List**.



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.

Prüfbericht

Es kann ein Prüfbericht an eingehende E-Mails angehängt werden.

Anhängen falls sie **sicherheitsverwandte Eigenschaften** besitzt (empfohlen)

Sogar anhängen wenn nur Informationen über Transportsicherheit verfügbar sind

Niemals anhängen

Immer anhängen

Es kann kein Prüfbericht an signierte E-Mails angehängt werden wenn die Signatur an der E-Mail verbleibt. Diese würde sonst die bestehende Signatur brechen.

Es sind unterschiedliche Prüfberichte verfügbar, die an eingehende E-Mails angehängt werden können.

Nutze das NoSpamProxy **Outlook Add-In**, um den Report anzuzeigen

Einen **menschenlesbaren** Prüfbericht an mit dieser Vorlage anhängen:

English

Einen maschinenlesbaren **XML** Prüfbericht

Einen maschinenlesbaren **OSCI konformen** Prüfbericht

Um die Authentizität des Prüfberichts sicherzustellen, können Sie ein Zertifikat zum Signieren des Berichts auswählen.

Kein Zertifikat ausgewählt.

Zertifikat auswählen Zertifikat entfernen

Speichern und schließen Abbrechen und schließen

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.
 - **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.
 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.

I Benutzerbenachrichtigungen anpassen

Um die Benutzerbenachrichtigungen anzupassen, müssen Sie die entsprechenden Standard-Templates anpassen und in einem speziellen Ordner für angepasste Templates speichern.

Beachten Sie dabei die folgenden Punkte:

- Die Standard-Templates liegen als CSHTML-Dateien vor (Ausnahmen bilden hier zwei HtmlProcessCardTemplate-Dateien) und befinden sich im Verzeichnis **%Program Files%\Net at Work Mail Gateway\Intranet Role\Templates**, oder bei Neuinstallationen im Verzeichnis **%Program Files%\NoSpamProxy\Intranet Role\Templates**.
- Stellen Sie sicher, dass Sie die angepassten Template-Dateien unter **C:\ProgramData\Net at Work Mail Gateway\Templates Customizations** speichern, um sie updatesicher zu machen. Die Original-Dateien müssen im Standardordner verbleiben.
- Änderungen müssen Sie nur auf der Intranetrolle vornehmen. Die Inhalte werden automatisch auf alle angeschlossenen Gatewayrollen repliziert.

I Vorgehen nach Updates

Nach Updates von NoSpamProxy ist es möglich, dass in einem oder mehreren Standard-Templates Änderungen vorliegen. Sie erkennen dies unter anderem an einer veränderten Versionsnummer. Die Versionsnummer einer Template-Datei finden Sie ganz am Anfang der entsprechenden Datei, also beispielsweise `@* Version: 1 *@` oder `<?xml version="1.0" encoding="utf-8" ?>`. In diesen Fällen müssen Sie die von Ihnen angepassten Template-Dateien manuell aktualisieren, da sonst wieder das Standard-Template verwendet wird.

Gehen Sie zum Aktualisieren der angepassten Template-Dateien folgendermaßen vor:

1. Kopieren Sie die entsprechenden Standard-Templates in den Ordner für angepasste Dateien (siehe oben).
2. Ziehen Sie deren Versionsnummern mit den Versionsnummern der Standard-Templates gleich.
3. Nehmen Sie die gewünschten Änderungen an den Dateien (erneut) vor.

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 Benachrichtigung 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 Quarantäne 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 Quarantäne 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” 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.

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 beispielsweise signiert und / oder verschlüsselt war.

EmailHintsHTML.cshtml

In dieser Datei können die Texte für die HTML-Versionen der E-Mail-Hinweise editiert werden.

EmailPlainText.cshtml

In dieser Datei können die Texte für die Klartext-Versionen der E-Mail-Hinweise editiert 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.

English.HtmlProcessCardTemplate

Der Inhalt des englischen Prüfberichts, kann in dieser Datei editiert werden. Prüfberichte werden auf Wunsch des Administrator erzeugt, wenn eine E-Mail beispielsweise signiert und / oder verschlüsselt war.

LargeFileApprovalRequest.cshtml

In dieser Datei können Sie die Freigabeanforderung für Dateien anpassen.

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 Benachrichtigung kann man hier editieren.

MailOnHoldExpired.cshtml

Wenn ein Benutzer eine E-Mail als “Automatisch verschlüsseln” kennzeichnet und ein Schlüssel 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 E-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 Benachrichtigung 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.

Branding

Die unten stehenden Einstellungen werden im NoSpamProxy Web Portal und in E-Mails für Benachrichtigungen verwendet.

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

Die Farben sind **#000000** für die Textfarbe, **#C01B1B** für die Akzentfarbe, **#d2d6d9** für Rahmen und **#F8F8F8** für den Hintergrund des Inhalts.

Das unten stehende Logo ist **links** ausgerichtet und hat eine Bildhintergrundfarbe von **#ffffff**.

[Bearbeiten](#)

Wortübereinstimmungen

Globale Wortgruppen

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

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

Realtime Blocklists

Globale Blocklists

Name	Typ	URL
Bonded Sender	DNS	query.bondedsender.org
CBL Composite Blocking List	DNS	cbl.abuseat.org
DNSWLorg	DNS	list.dnswl.org
MailSpike	DNS	rep.mailspike.net
NixSpam RBL	DNS	ix.dnswl.manitu.net
Passive Spam Block List	DNS	psbl.surriel.com
SpamCop	DNS	bl.spamcop.net
Spamhaus SBL (Spam Block List)	DNS	sbl.spamhaus.org
Spamhaus Whitelist	DNS	swl.spamhaus.org
Spamhaus XBL (Exploits Block List)	DNS	xbl.spamhaus.org
Spamhaus ZEN	DNS	zen.spamhaus.org
SpamRats	DNS	spams.pamrats.com

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

Actions

[Aktualisieren](#)

[Deutsch](#)



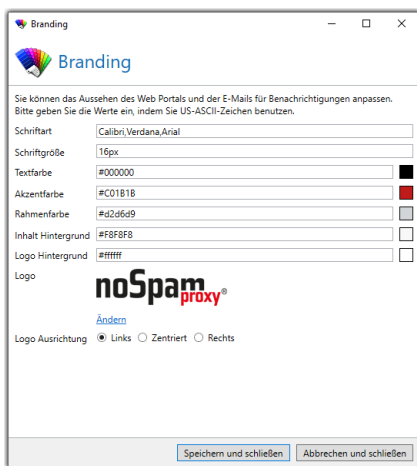
HINWEIS: Die hier vorgenommenen Änderungen wirken sich auch auf bestehende Regeln, Partner oder Unternehmensbenutzer aus. Die Einstellungen gelten immer für alle Konfigurationen, in denen sie referenziert werden.

Wortübereinstimmungen

Realtime Blocklists

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.

Inhalt der Wortgruppe

Allgemein Wörter

Name

Vergebe Punkte Für *jede* Übereinstimmung mit der Wortliste
 Falls **keine** Übereinstimmung gefunden wird

Bereich Betreffzeile
 E-Mail-Inhalt

Punkte
10 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.

Inhalt der Wortgruppe

Allgemein Wörter

Art

- Einfach (*schnell*, empfohlen)
- Platzhalter (langsamer, '?' und '*' erlaubt)
- Regulärer Ausdruck (langsamer, mit Vorsicht verwenden)

Neues Wort

Wort

- https://bit.ly/*

Entfernen

Auch ähnliche Wörter finden

5. Klicken Sie auf **Fertigstellen**.

I 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

The screenshot displays the 'NoSpamProxy Command Center' interface. On the left is a navigation sidebar with categories: Übersicht, Monitoring, Identitäten, Konfiguration (expanded), and Troubleshooting. The 'Konfiguration' section includes sub-items like E-Mail-Routing, Regeln, Inhaltsfilter, URL Safeguard, NoSpamProxy Komponenten, Verbundene Systeme, Benutzer-Benachrichtigungen, Voreinstellungen, and 'Erweiterte Einstellungen' (highlighted). The main content area is titled 'Erweiterte Einstellungen' and contains three sections:

- Schutz sensibler Daten:** States 'Sensible Daten sind geschützt.' with a 'Bearbeiten' link.
- Monitoring:** Lists retention periods: 'Nachrichtenübersichtsinformationen werden für 1 Monat gespeichert...', 'Klickbare URL-Safeguard-Besuche werden für 10 Tage gespeichert.', 'Nachrichtenstatistiken werden für 1 Jahr gespeichert.', and 'E-Mails werden für 3 Tage angehalten, wenn auf Verschlüsselungsschlüssel von Partnern gewartet wird.' with a 'Bearbeiten' link.
- Betreffkennzeichnungen:** Includes a table for adding tags to email subjects to influence processing.

Name	Betreffkennzeichnung	Kopfzeile
De-Mail: Versandbestätigung anfordern	Versandbestätigung	X-de-mail-confirmation-of-dispatch
De-Mail: Empfangsbestätigung anfordern	Eingangsbestätigung	X-de-mail-confirmation-of-receipt
De-Mail: Abholbestätigung anfordern	Abholbestätigung	X-de-mail-confirmation-of-retrieve
De-Mail: E-Mail als absenderbestätigt markieren	Absenderbestätigt	X-de-mail-authoritative
De-Mail: E-Mail als privat markieren	Persönlich	X-de-mail-private
Anhangspasswort	AP	X-NoSpamProxy-RequireAttachmentPassword
PDF-Verschlüsselungspasswort	PW	X-enQsig-SymmetricEncryptionPassword
Nummer für SMS-Benachrichtigung	SMS	X-enQsig-SymmetricEncryptionNotificationAddress

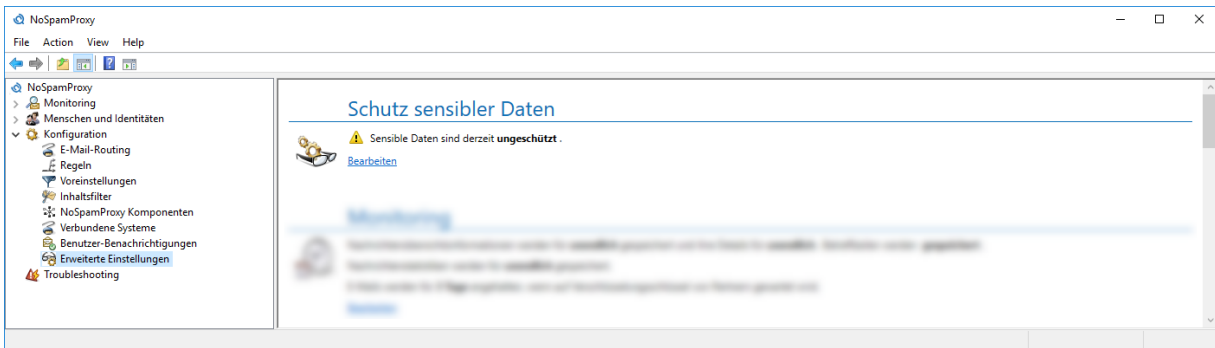
Below the table, it notes 'Eckige Klammern werden benutzt, um Betreffkennzeichnungen zu markieren. Beispiel: [PW:123]' with a 'Bearbeiten' link.

- Level-of-Trust-Konfiguration:** States 'MAIL FROM' and 'Header-From' addresses are evaluated. It specifies a trust bonus of 200 points for address relationships and a 25-point domain bonus. It notes that domain bonuses are not granted for emails from free providers and that authentication is required for all bonuses. Intelligent DSN filtering is set to automatic, with 50 penalty points for invalid DSNs and 50 bonus points for valid ones. A 'Bearbeiten' link is provided.

At the bottom left, there are 'Actions' including 'Aktualisieren' and 'Deutsch'.

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.

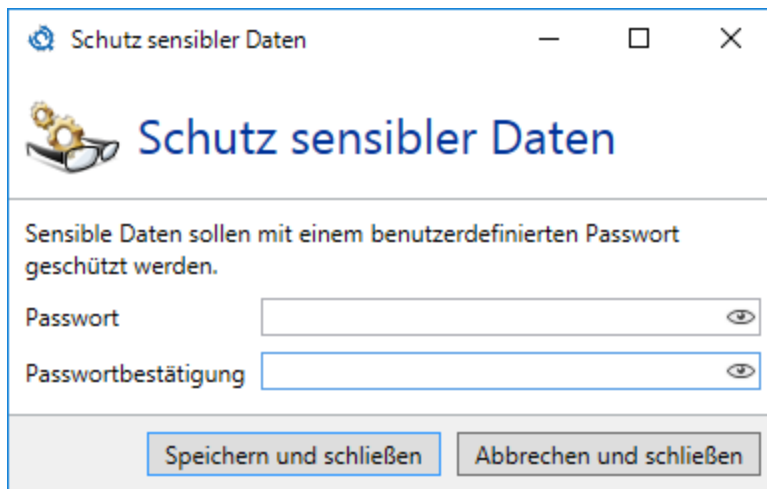


HINWEIS: Nach der Aktivierung kann der Schutz nicht rückgängig gemacht werden.


Schutz sensibler Daten aktivieren

1. Gehen Sie **Konfiguration > Erweiterte Einstellungen > Schutz sensibler Daten**.

2. Klicken Sie **Bearbeiten**.



Schutz sensibler Daten

 **Schutz sensibler Daten**

Sensible Daten sollen mit einem benutzerdefinierten Passwort geschützt werden.

Passwort

Passwortbestätigung

Speichern und schließen Abbrechen und schließen

3. Geben Sie ein Passwort für den Schutz ein.

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

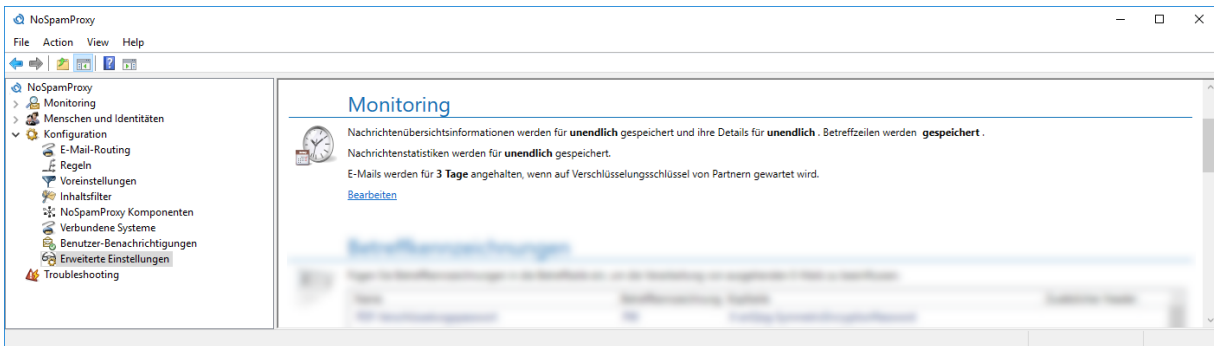


HINWEIS: Sie können das Passwort zu einem späteren Zeitpunkt ändern.



WARNING: 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.

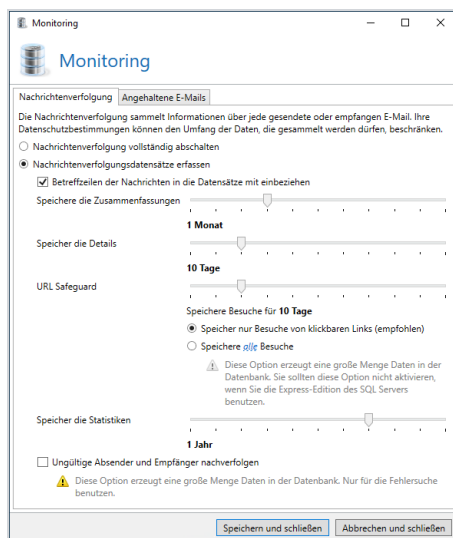
Monitoring



NoSpamProxy kann jede Verbindung in der Nachrichtenverfolgung mitprotokollieren. So können Sie nachvollziehen, wie die einzelnen E-Mails verarbeitet wurden.

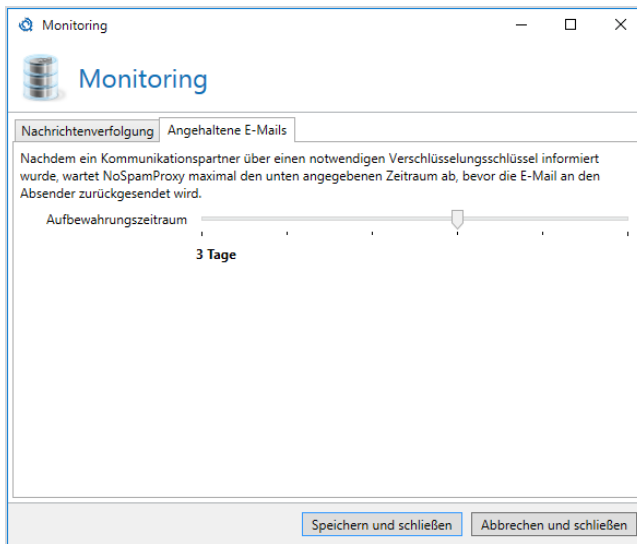
Nachrichtenverfolgung aktivieren

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

EXAMPLE:

- 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

[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.
[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.
[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.
[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.

PDF-Verschlüsselungspasswort

PDF-Verschlüsselungspasswort

Betreffkennzeichnungen können genutzt werden um die Verarbeitung von ausgehenden E-Mails zu kontrollieren. Sie können diese Kennzeichnungen in die Betreffzeile einfügen. Geben Sie an, wie Sie diese Betreffkennzeichnung über die Betreffzeile einer E-Mail steuern möchten.

Benutze den Standardnamen **PW**

Nutze einen alternativen Namen

Name

Die Zeichen 'A-Z', 'a-z', '0-9' and '_' sind in der Betreffkennzeichnung erlaubt.
Es wird keine Unterscheidung zwischen Groß- und Kleinbuchstaben gemacht.

Der Header **X-enQsig-SymmetricEncryptionPassword** wird benutzt um die Betreffkennzeichnung zu kontrollieren.

Verwende zusätzlich zu obigem Header den Folgenden

Header-Name



WARNING: 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

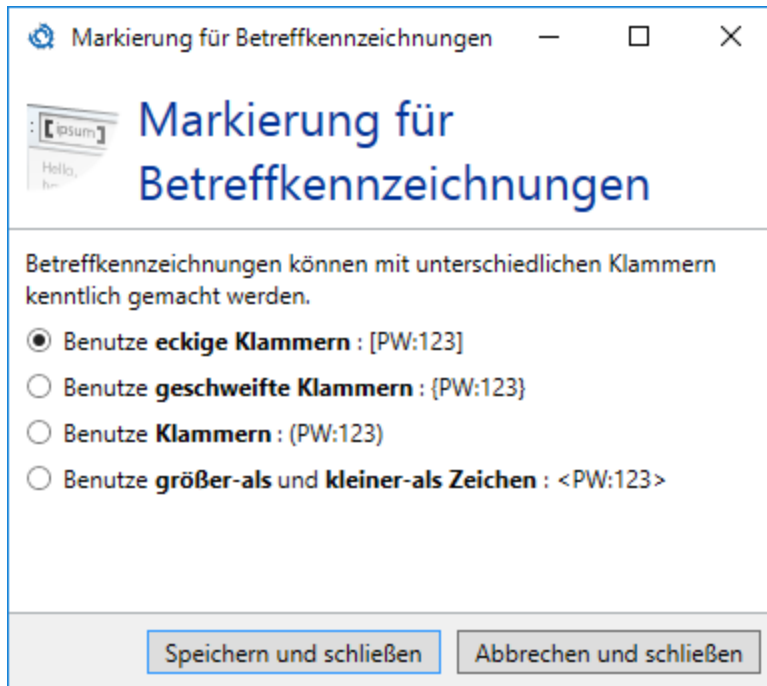
An Stelle der Betreffkennzeichnungen können Sie auch das Outlook Add-In für NoSpamProxy installieren. Das Outlook Add-In wird an Stelle der Betreffkennzeichnungen mit Microsoft Outlook verwendet.

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**.

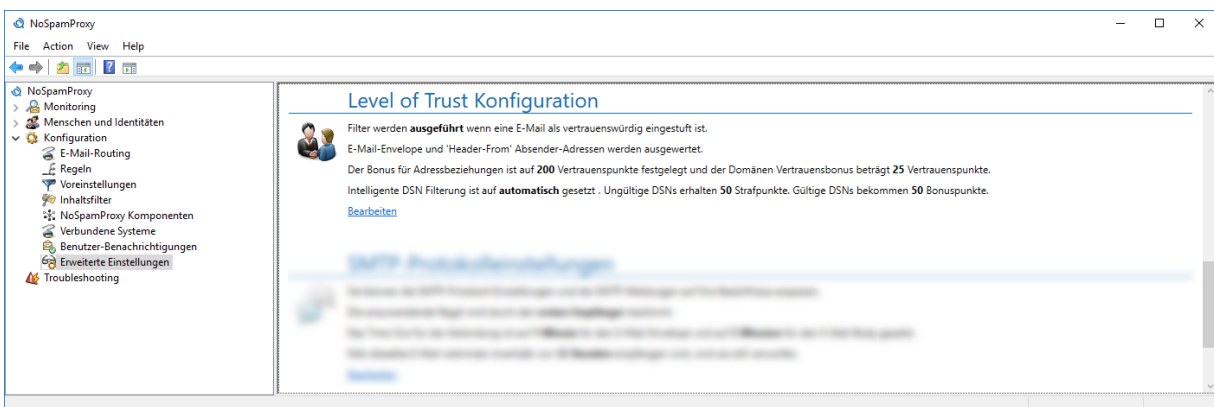
2. Klicken Sie **Bearbeiten**.



3. Wählen Sie den gewünschten Markertyp aus.

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

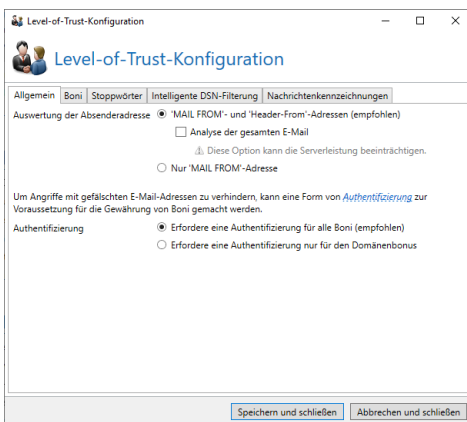
Level-of-Trust-Konfiguration



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



- **Auswertung der Absenderadresse** | 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.

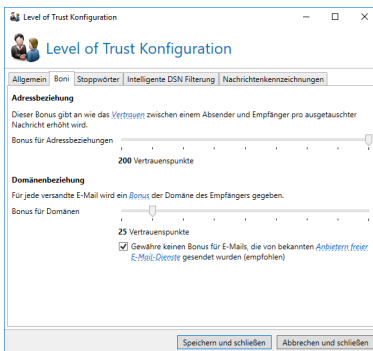
- 'MAIL FROM'- und 'Header-From-Adressen (empfohlen)
 - (Optional) Die gesamte E-Mail (kann die Serverleistung beeinträchtigen)



HINWEIS: Wird die gesamte E-Mail analysiert, so wird diese unter Anwendung aller in der jeweiligen Regel konfigurierten Filter ausgewertet. Das Ergebnis dieser Auswertung ist entsprechend genauer als die alleinige Auswertung von 'MAIL FROM' und 'Header-From' und kann letztere Auswertung überstimmen. Da alle E-Mails vollständig empfangen werden, kann diese Option negative Auswirkungen auf die Serverleistung haben.

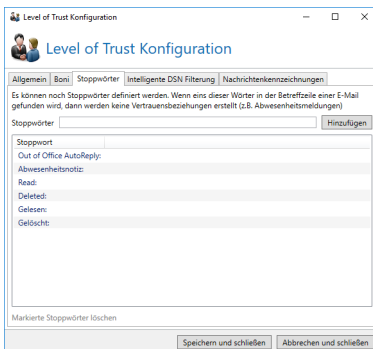
- Nur 'MAIL FROM'-Adressen
 - **Authentifizierung** | Bestimmt, ob eine erfolgreiche Authentifizierung durch DKIM-, S/MIME- und SPF-Prüfungen die Vorbedingungen für alle Boni oder nur für den Domänenbonus ist (siehe Registerkarte **Boni**).

Registerkarte Boni



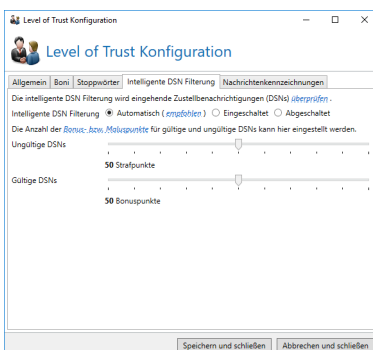
- **Adressbeziehung** | Bestimmt, um wie viele Punkte das Vertrauen zwischen einem Absender und einem Empfänger pro Nachricht erhöht wird. Mit dem Schieberegler können Sie hier einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht dabei (-0,1) Punkten für den **Spam Confidence Level (SCL)**. 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.

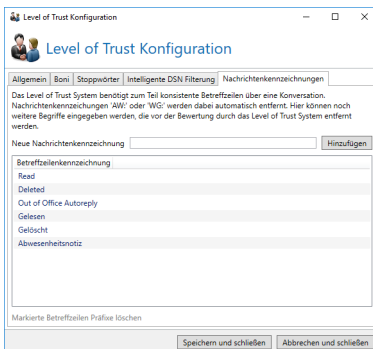
EXAMPLE:

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



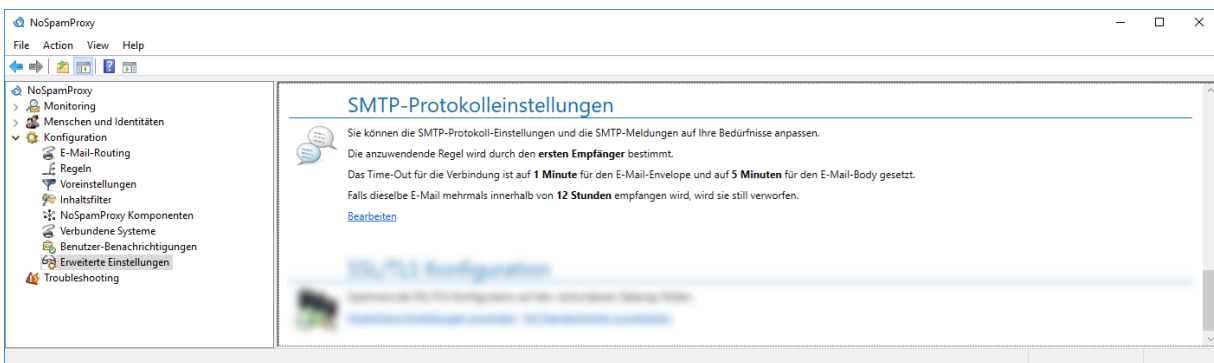
Das Level-of-Trust-System benötigt zum Teil konsistente Betreffzeilen über eine Konversation. Nachrichtenbezeichnungen wie beispielsweise **AW:** oder **WG:** müssen dazu entfernt werden. Hier konfigurieren Sie alle Kennzeichnungen, die Ihr E-Mail-System verwendet.

| Siehe auch

[Level of Trust](#)

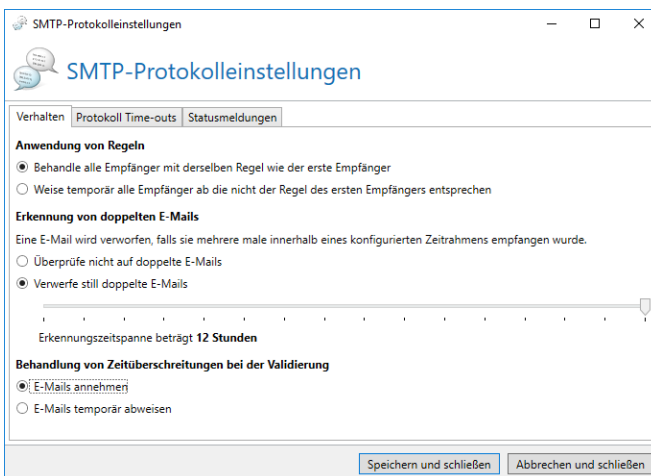
[Punktevergabe für Domänen bei Level of Trust](#)

| 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. Nachteile 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.

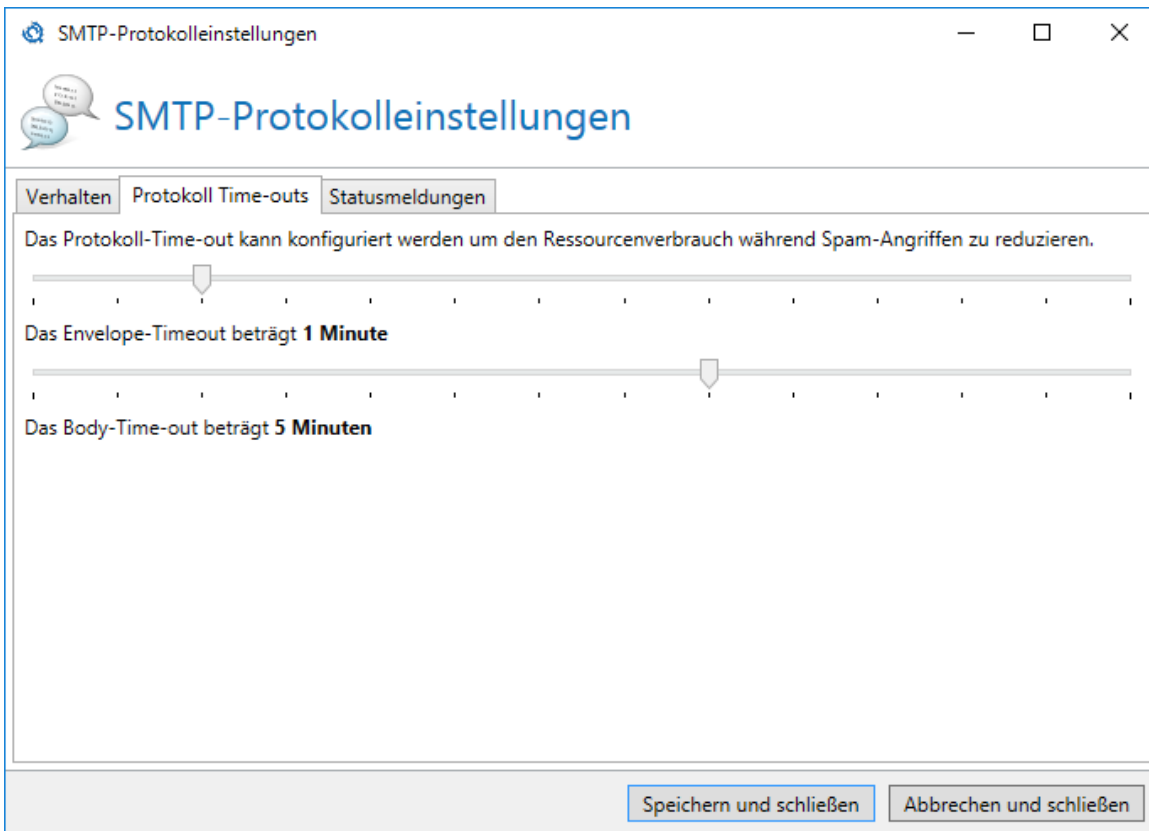


HINWEIS: Falls die Malwareüberprüfung nicht abgeschlossen ist, wenn ein Validierungs-Timeout erfolgt, wird die jeweilige E-Mail in jedem Fall temporär abgewiesen.



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

SMTP-Protokolleinstellungen

SMTP-Protokolleinstellungen

Verhalten Einstellungen Statusmeldungen

SMTP Antworten

Willkommensnachricht Net at Work Mail Gateway ready

Zurückgewiesene E-Mails This email was rejected because it violates our security policy

Verbindungsende Service closing transmission channel

Verbindung zurückgewiesen The connection was not accepted at this time. Please try again later.

Weiterleitung nicht möglich Unable to relay

i Alle SMTP Antworten müssen eingetragen werden. Alle druckbaren ASCII Zeichen dürfen genutzt werden.

Speichern und schließen Abbrechen und schließen

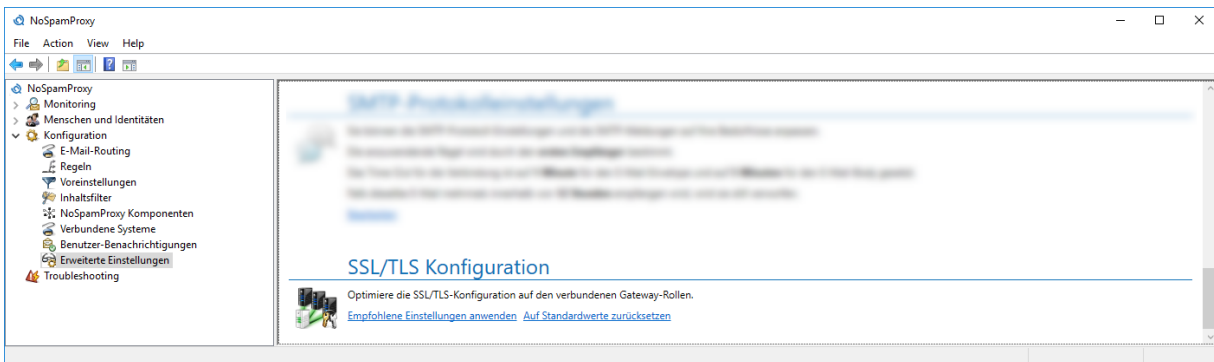
Die Statusmeldungen bestimmen, welche Texte NoSpamProxy an andere Server sendet. Die SMTP-Antworten sind Standardangaben im SMTP-Handshake, die für den normalen Anwender in der Regel nicht sichtbar sind. Dennoch kann es sinnvoll sein, die Angaben nach eigenem Bedarf zu ändern. Dies kann Administratoren 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



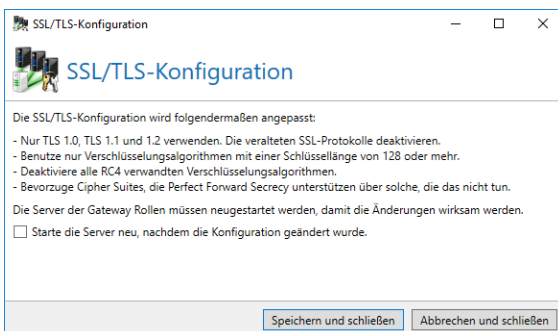
Bei der Transportverschlüsselung wird die Verbindung über SSL oder TLS abgesichert. Dabei greift die Gatewayrolle auf das Betriebssystem zurück. Dessen Einstellungen werden bei Verbindungen verwendet.



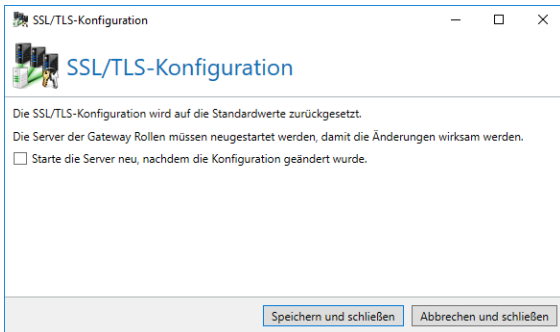
HINWEIS: In letzter Zeit haben sich einige Verschlüsselungsverfahren (z.B. DES oder RC4) als nicht mehr sicher herausgestellt. Daher ist sinnvoll, diese zu deaktivieren. Einige Cipher Suites unterstützen ein Verfahren namens Perfect Forward Secrecy. Dies verhindert - kurz gesagt - dass die Inhalte von 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

The screenshot shows the NoSpamProxy Command Center interface. The left sidebar contains a navigation menu with the following items: Übersicht, Monitoring, Identitäten, Unternehmensdomänen, Unternehmensbenutzer, Partner, Zertifikate, PGP-Schlüssel, Öffentliche Schlüsselservers, Schlüsselanforderung, E-Mail-Authentifizierung, Zusätzliche Benutzerfelder, Konfiguration, E-Mail-Routing, Regeln, Inhaltsfilter, URL Safeguard, NoSpamProxy Komponenten, Verbundene Systeme, Benutzer-Benachrichtigungen, Voreinstellungen, Erweiterte Einstellungen, and Troubleshooting. The Troubleshooting section is currently selected and displays four sub-sections:

- Protokolleinstellungen:** A table showing protocol settings for different roles.

Rolle	Aktive Protokolle	Ort der Protokolldatei	Sammle E-Mails	Protokoll automatisch abschalten
Gateway Rolle INSTALLATION	0	C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\	Nein	
Intranet Rolle	0	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\		
- Geblockte IP-Adressen:** A section indicating a table of blocked servers, with a link to 'Geblockte Adressen löschen'.
- Berechtigungen korrigieren:** A section for correcting database and file permissions, with a table listing roles: Intranet Rolle and Gateway Rolle INSTALLATION.
- Web Portal Sicherheit:** A section for web portal security, with a table showing the status of a specific URL: https://installation/enQsig, which is 'Alles ist in Ordnung'.

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	254
Geblockte IP-Adressen	257

Berechtigungen korrigieren	258
Marktkommunikation mit AS4	260
Schritt 1: Aktivieren des AS4-Moduls	261
Schritt 3: Erstellen der erforderlichen Windows-Gruppe	263
Schritt 4: Key-Management-Dienst konfigurieren	265
Dienstadresse hinterlegen	265
(Optional) HSM hinzufügen	266
(Optional) Token konfigurieren	268
Häufige Fragen	268
Schritt 5: Ihr Marktpartner-Konto konfigurieren	270
Ihr Marktpartner-Konto hinzufügen	270
Zertifikatsanfrage für die AS4-Kommunikation erstellen	272
Zertifikate importieren	273
Einstellungen ändern	274
Schritt 6: Marktpartner-Kommunikation aktivieren	275
Ausgehendes AS4 anfragen	275
Eingehendes AS4 bestätigen	276
Testen der AS4-Konnektivität	277
AS4-Nachrichtenverfolgung	279
Marktpartner manuell hinzufügen	283
Schlüsselspeicher ändern	285
Speicherort für EDIFACT-Dokumente konfigurieren	286

Protokolleinstellungen

Um die Protokolleinstellungen für die jeweilige Gateway- oder Intranetrolle zu ändern, gehen Sie folgendermaßen vor:

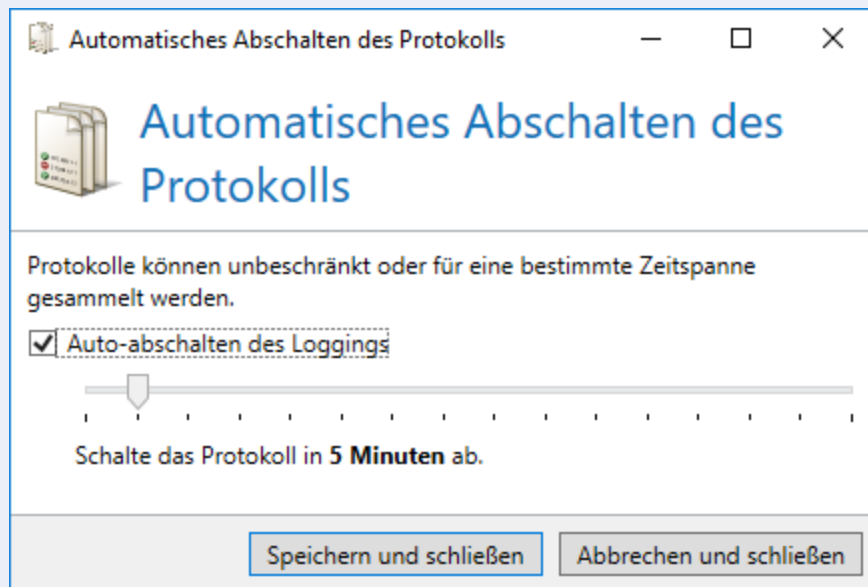
1. Gehen Sie zu **Troubleshooting > Protokolleinstellungen**.
2. Markieren Sie die gewünschte Rolle.
3. Klicken Sie **Bearbeiten**.
4. Nehmen Sie die gewünschten Einstellungen vor (siehe unten).
5. Klicken Sie **Speichern und schließen**.

| 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.



I Registerkarte **Debug**einstellungen

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.

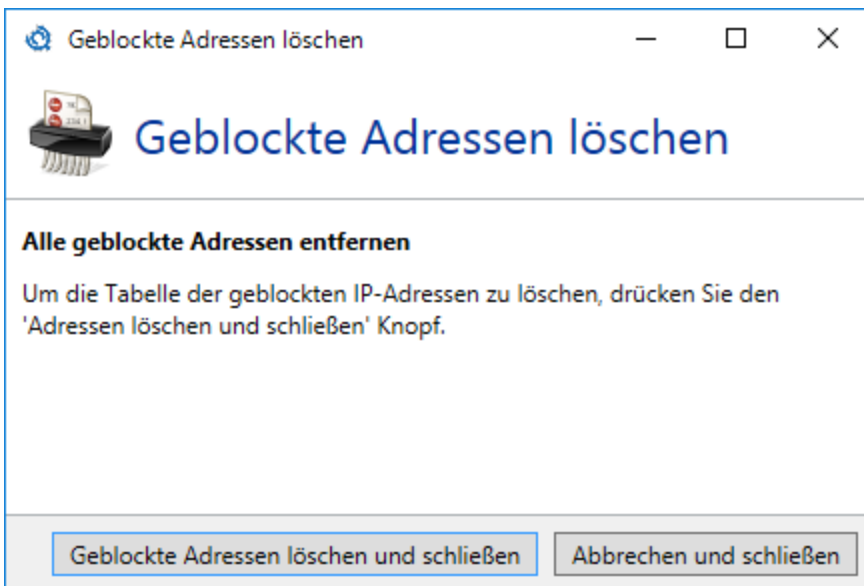


HINWEIS: Dieser Reiter ist nur bei Gatewayrollen vorhanden.

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

Berechtigungen korrigieren

 **Berechtigungen korrigieren**

Die Anmeldeinformationen unten müssen einen Benutzer angeben, der Datenbank ändern darf.

Ein bestimmtes Windows Benutzerkonto

Benutzername

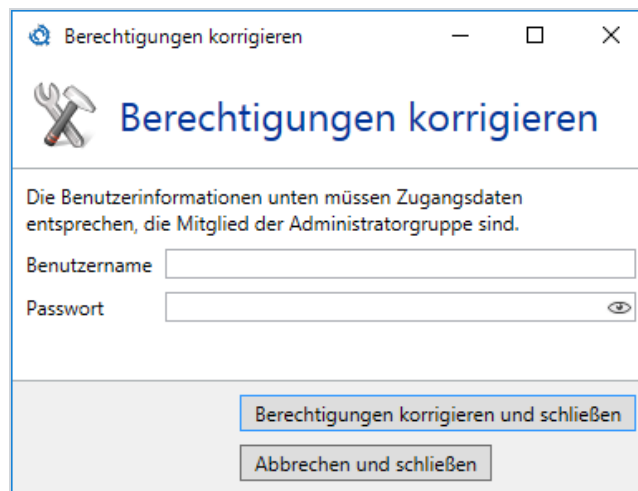
Passwort

Ein bestimmtes SQL Benutzerkonto

Benutzername

Passwort

- Dateisystem berichtigen



4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie **Berechtigungen korrigieren und schließen**.

Marktkommunikation mit AS4

Marktkommunikation (MaKo) steht für den Dateiaustausch zwischen Marktteilnehmern des deutschen Energiemarkts. NoSpamProxy unterstützt die automatisierte EDIFACT-Marktkommunikation für die Energiewirtschaft nach den Vorgaben der verbändeübergreifenden Expertengruppe EDI@Energy.

I AS4-Marktkommunikation in NoSpamProxy einrichten

Um das Senden und Empfangen von AS4-Nachrichten in NoSpamProxy einzurichten, sind vier Schritte notwendig:

Schritt 1: Aktivieren des AS4-Moduls

Schritt 2: Aktivieren der TLS-ECC-Kurve Brainpool P256r1

Schritt 3: Erstellen der erforderlichen Windows-Gruppe

Schritt 4: Key-Management-Dienst konfigurieren

Schritt 5: Ihr Marktpartner-Konto konfigurieren

Schritt 6: Marktpartner-Kommunikation aktivieren

Schritt 1: Aktivieren des AS4-Moduls

Um AS4-Marktkommunikation einzurichten, müssen Sie die entsprechenden Komponenten **vor der Installation** von NoSpamProxy aktivieren. Ansonsten werden diese während der Installation nicht angezeigt.

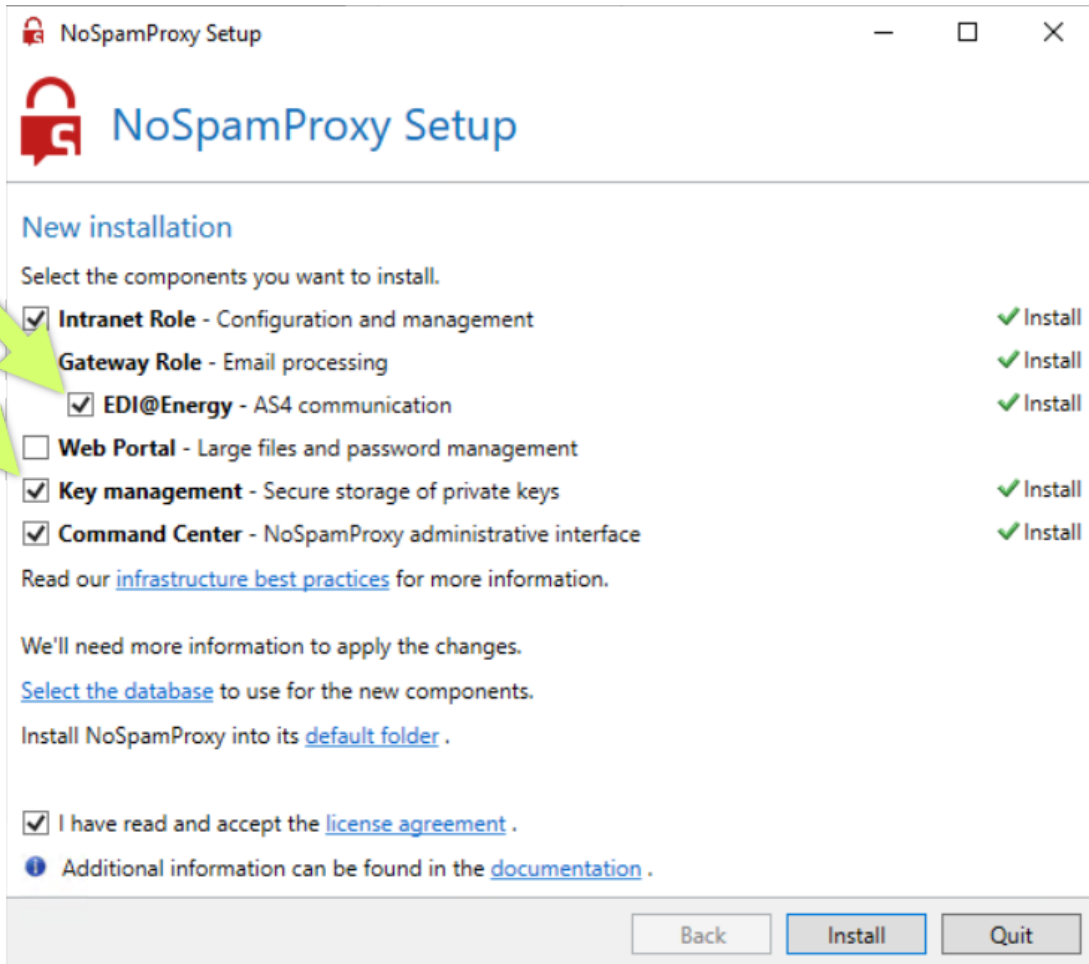
- Führen Sie den folgenden Kommandozeilen-Parameter in dem Verzeichnis aus, in dem die Installationsdatei von NoSpamProxy liegt:

```
setup.exe /EDI@Energy=1
```

Die NoSpamProxy-Installation startet nun. Stellen Sie sicher, dass Sie während der Installation die Komponenten

- **EDI@Energy** und
- **Key management**

auswählen.



Schritt 3: Erstellen der erforderlichen Windows-Gruppe

Nach der Installation von NoSpamProxy Server müssen Sie die erforderliche Windows-Gruppe **NoSpamProxy EDI at Energy Administrators** per PowerShell erstellen.

1. Wechseln Sie auf das System, auf dem die Intranetrolle installiert ist.
2. Führen Sie das in PowerShell das Cmdlet `New-NspEdiAtEnergyAdministratorsGroup` aus.

Dieses Cmdlet bewirkt die beiden folgenden Dinge:

- Es erstellt die Windows-Gruppe **NoSpamProxy EDI at Energy Administrators**.
- Es weist die erstellte Gruppe der Rolle **EdiAtEnergyAdministrator** zu.

Sie können der neuen Windows-Gruppe unter Verwendung der MMC **Lokale Benutzer und Gruppen** Benutzer hinzufügen. Sollte die Zuweisung der Gruppe zur Rolle fehlschlagen, müssen Sie die Gruppe manuell der Rolle zuweisen. Geben Sie dafür den folgenden Befehl in PowerShell ein:

```
New-NspUserRoleAssignment -Identity "NoSpamProxy EDI at Energy Administrators" -Role  
EdiAtEnergyAdministrator -TenantId IHRE_MANDANTEN_ID
```



HINWEIS:

- Die Umgebung muss eine NoSpamProxy Server-Installation sein.
- EDI@Energy muss lizenziert sein.
- Wenn bereits eine Windows-Gruppe mit demselben Namen vorhanden ist, schlägt das Cmdlet fehl.

Schritt 4: Key-Management-Dienst konfigurieren

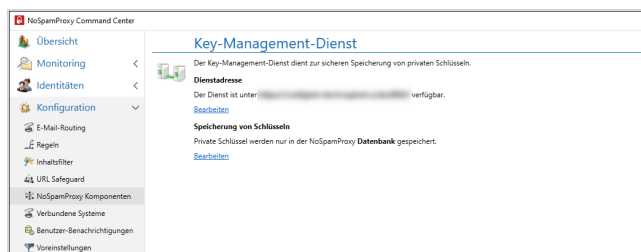
Um das Senden und Empfangen von AS4-Nachrichten in NoSpamProxy einzurichten, müssen Sie zuerst die Dienstadresse des Key-Management-Dienstes hinterlegen sowie optional ein Hardware-Sicherheitsmodul (HSM) in NoSpamProxy hinzufügen.



HINWEIS: Der Key-Management-Dienst dient zur sicheren Speicherung von privaten Schlüsseln. Für maximale Sicherheit empfehlen wir trotzdem die Verwendung eines HSM. Siehe unten, [Wer muss ein HSM verwenden?](#)

Dienstadresse hinterlegen

1. Die Dienstadresse ist die Adresse, unter der sich die Intranetrolle mit dem Key-Management-Dienst verbindet.
2. Gehen Sie im NoSpamProxy Command Center zu **NoSpamProxy-Komponenten > Key-Management-Dienst** und klicken Sie **Bearbeiten**.



3. Geben Sie unter **Verbindung** die Dienstadresse an.



HINWEIS: Die Standardadresse lautet **https://localhost:6064**. Stellen Sie in jedem Fall sicher, dass der HTTPS-Verkehr auf Port 6064 erlaubt ist.

Verbindung zum Dienst

Verbindung zum Dienst

Verbindung

Geben Sie an, wie sich die Intranetrolle mit dem Key-Management-Dienst verbindet.

Adresse

Bitte stellen Sie sicher, dass der HTTPS-Verkehr auf Port 6064 erlaubt ist.

Zurück Weiter Abbrechen und schließen

4. Geben Sie unter **Benutzerinformationen** die administrativen Benutzerinformationen für den Dienst an.

Verbindung zum Dienst

Verbindung zum Dienst

Benutzerinformationen

Geben Sie die administrativen Benutzerinformationen für den Key-Management-Dienst ein.

Benutzername

Passwort

Zurück Fertigstellen Abbrechen und schließen

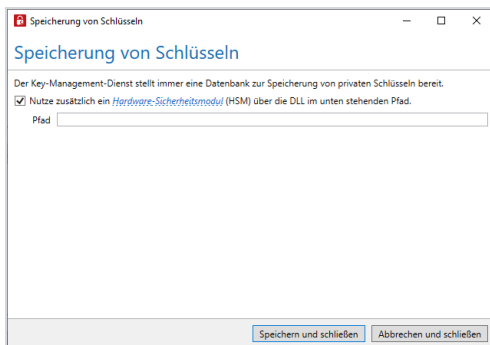
5. Klicken Sie **Fertigstellen**.

I (Optional) HSM hinzufügen

Wenn Sie zum Speichern Ihrer privaten Schlüssel zusätzlich ein HSM verwenden wollen, fügen Sie es hier hinzu.

1. Gehen Sie im NoSpamProxy Command Center zu **Konfiguration > NoSpamProxy-Komponenten > Key-Management-Dienst**.
2. Klicken Sie unter **Speicherung von Schlüsseln** auf **Bearbeiten**.

3. Setzen Sie das Häkchen bei **Nutze zusätzlich ein Hardware-Sicherheitsmodul (HSM) [...]**.



4. Geben Sie den Pfad zur DLL-Datei des HSM in das Eingabefeld ein.
5. Klicken Sie **Speichern und schließen**.

Unter **Key-Management-Dienst** erscheint nun der Bereich **Konfigurierte Token**.



HINWEIS:

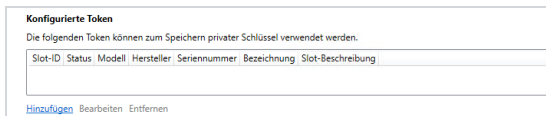
Die folgenden Voraussetzungen müssen erfüllt sein, damit Sie ein HSM zum Speichern Ihrer privaten Schlüssel verwenden können:

- Das HSM muss den **PKCS-#11**-Standard unterstützen.
- Das HSM muss für die Schlüsselgenerierung (CKM_EC_KEY_PAIR_GEN) den **Standard Elliptic Curve Brainpool P256r1** einsetzen.
- Das HSM muss für die Schlüsselableitung (CKM_ECDH1_DERIVE) die Schlüsselableitungsfunktion **SP-800 (CKD_SHA256_KDF_SP800)** einsetzen.

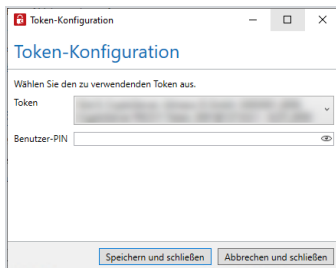
I (Optional) Token konfigurieren

Wenn Sie ein HSM verwenden und dieses hinzugefügt haben, können Sie auf die Token des HSM zugreifen und den gewünschten Token konfigurieren.

1. Klicken Sie unter **Konfigurierte Token** auf **Bearbeiten**.



2. Wählen Sie unter **Token** den gewünschten Token aus dem Drop-Down-Menü aus.



3. Geben Sie unter **Benutzer-PIN** die entsprechende PIN ein.
4. Klicken Sie **Speichern und schließen**.

Das HSM ist nun angebunden.

I Häufige Fragen

Wer muss ein HSM verwenden?

Bezüglich der Verwendung eines HSM wird in der Fassung der Certificate Policy der Smart Metering PKI vom 25.01.2023 (Version 1.1.2) gesagt, dass "[...] passive EMT Kryptografiemodule einsetzen [müssen], die mindestens konform zu den Key Lifecycle Security Requirements - Security Level 1 sind.

[...] Die konkreten Anforderungen an die Kryptografiemodule muss jeder Marktteilnehmer gemäß des von ihm zu erstellendem Sicherheitskonzept für sich ableiten."

Siehe [Regelungen zum Übertragungsweg für AS4](#), [BDEW AS4-Profil](#)

Was sind passive EMT?

Passive externe Marktteilnehmer (EMT) werden in der Certificate Policy der Smart Metering PKI 1.3.3.4 als Marktteilnehmer definiert, die Daten von den Smart Metering Gateways (SMGWs) empfangen oder austauschen, jedoch keine Steuerung dieser Geräte vornehmen.

Was sind aktive EMT?

Ein EMT, welcher ein SMGW nutzt, um darüber nachgelagerte Geräte (Controllable Local Systems, CLS) anzusprechen, wird als aktiver EMT bezeichnet.

Was sind Kryptografiemodule Security Level 1?

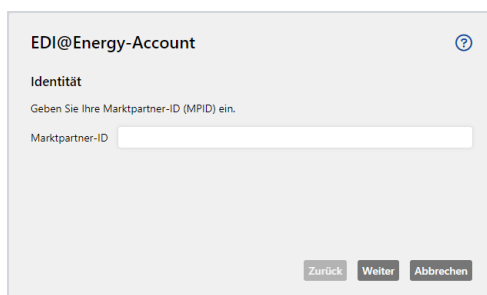
Kryptographische Module der Sicherheitsstufe 1 können als Software oder Server mit Zwei-Faktor-Authentifizierung und physisch eingeschränktem Zugang betrieben werden. Zur Erzeugung von Zufallszahlen für die Schlüsselgenerierung sowie für Signatur und Verschlüsselung muss ein Zufallszahlengenerator der Klassen NTG.1, DRG.4 oder PTG.3 gemäß AIS 20/31 verwendet werden.

Schritt 5: Ihr Marktpartner-Konto konfigurieren

In diesem Schritt hinterlegen Sie das zu Ihrer Marktpartner-ID (MPID) gehörende Konto in NoSpamProxy, erstellen die Zertifikatsanfragen und importieren die benötigten Zertifikate.

Ihr Marktpartner-Konto hinzufügen

1. Öffnen Sie die NoSpamProxy Web App.
2. Gehen Sie zu **EDI@Energy > Einstellungen > EDI@Energy-Unternehmenskonten**.
3. Klicken Sie **Hinzufügen**, geben Sie unter **Identität** Ihre MPID ein und klicken Sie **Weiter**.



The screenshot shows a web form titled "EDI@Energy-Account" with a help icon. Under the "Identität" section, there is a prompt: "Geben Sie Ihre Marktpartner-ID (MPID) ein." Below this is a text input field labeled "Marktpartner-ID". At the bottom of the form are three buttons: "Zurück", "Weiter", and "Abbrechen".

4. Geben Sie unter **Details** den mit Ihrem Konto verknüpften Namen und Ihre Funktion ein und klicken Sie **Weiter**.



The screenshot shows a web form titled "EDI@Energy-Account" with a help icon. Under the "Details" section, there is a message: "Die Kontodetails für die Marktpartner-ID [redacted] konnten nicht gefunden werden. Überprüfen Sie Ihre MPID oder geben Sie die Details manuell ein." Below this are two text input fields: "Name" and "Funktion". At the bottom of the form are three buttons: "Zurück", "Weiter", and "Abbrechen".

5. Geben Sie unter **Routing** den externen **Endpunkt** für die AS4-Kommunikation sowie das für den Prozesstyp **Marktprozesse** verwendete Postfach an. Geben Sie außerdem (falls genutzt)

- die E-Mail-Adresse der internen Mailbox für '**Redispatch 2.0**'-**Meldungen**,
- die E-Mail-Adresse der internen Mailbox für '**Fahrplan**'-**Nachrichten** und
- den **Energy Identification Code (EIC)** an.

The screenshot shows the 'EDI@Energy-Account' configuration page, specifically the 'Routing' section. The page title is 'EDI@Energy-Account' with a help icon. The 'Routing' section contains the following fields and options:

- Routing**: A heading with a help icon.
- Text**: 'Der externe Endpunkt wird von Marktpartnern verwendet, um EDI@Energy-Nachrichten im AS/4-Format an diesen Account zu senden.'
- Externer Endpunkt**: A text input field.
- Text**: 'Für jeden Prozesstyp wird ein eigenes Postfach verwendet.'
- Marktprozesse**: A dropdown menu with a domain selection icon and the text 'Domäne auswählen'.
- Checkbox**: 'Verarbeiten von 'Redispatch 2.0'-Meldungen'
- Interne Mailbox**: A text input field with a domain selection icon and the text 'Domäne auswählen'.
- Checkbox**: 'Verarbeiten von 'Fahrplan' Nachrichten'
- Interne Mailbox**: A text input field with a domain selection icon and the text 'Domäne auswählen'.
- EIC**: A text input field.
- Buttons**: 'Zurück', 'Weiter', and 'Abbrechen'.

6. Geben Sie unter **Details zum Zertifikat** den Namen, die Erweiterung (optional), den Ländercode sowie die im Zertifikat verwendete E-Mail-Adresse an.

The screenshot shows the 'EDI@Energy-Account' configuration page, specifically the 'Details zum Zertifikat' section. The page title is 'EDI@Energy-Account' with a help icon. The 'Details zum Zertifikat' section contains the following fields and options:

- Details zum Zertifikat**: A heading with a help icon.
- Common Name**: A heading with a help icon.
- Text**: 'Der Common Name (CN) des Zertifikatssubjekts wird aus folgenden Informationen abgeleitet.'
- Name**: A text input field with the value 'NeuerAccount'.
- Erweiterung (optional)**: A text input field with the value 'MAK'.
- Text**: 'Der Common Name wird **NeuerAccount.EMT.MAK** sein.'
- Land**: A heading with a help icon.
- Ländercode**: A text input field with the value 'DE'.
- Kontaktinformationen**: A heading with a help icon.
- Text**: 'Das Zertifikat enthält eine E-Mail-Adresse, über die Sie erreicht werden können.'
- E-Mail-Adresse**: A text input field.
- Buttons**: 'Zurück', 'Fertigstellen', and 'Abbrechen'.

7. Klicken Sie **Fertigstellen**.

Ihr Konto ist nun in NoSpamProxy hinterlegt.

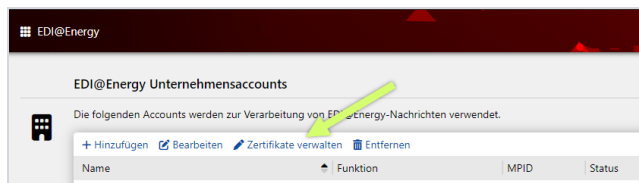


HINWEIS:

- Der Pfad des AS4-Endpunkts muss auf **/as4** enden.
- Der Port des AS4-Endpunkts ist 6063. Wenn ein Reverse-Proxy oder eine Netzwerkregel vorhanden ist, müssen Sie den Port auf 443 ändern.
- Der Port muss von außen erreichbar sein, ohne dass die Firewall eingreift.
- Der AS4-Dienst sollte sich innerhalb der DMZ befinden, das heißt, er sollte in der Lage sein, an jede Adresse und jeden Port zu senden.

Zertifikatsanfrage für die AS4-Kommunikation erstellen

1. Gehen Sie zu **EDI@Energy > Einstellungen > EDI@Energy-Unternehmenskonten**.
2. Markieren Sie das entsprechende Konto, klicken Sie **Zertifikate verwalten** und dann **Anfrage stellen**.



3. Prüfen Sie die angezeigten Informationen auf Richtigkeit und klicken Sie **Erstellen**.

Erstelle eine Zertifikatsanfrage ⓘ

Die Certificate Signing Requests (CSR) werden mit den unten stehenden Daten erstellt.

Betreffzelle

Common Name

Organization **SM-PKI-DE**

Organisatorische Einheit

Country

Alternativer Name des Betreffs

URI

DNS

E-Mail-Adresse

Erstellen **Abbrechen**

4. Laden Sie die für die Anfrage benötigten CSR-Dateien herunter.
5. Reichen Sie die CSR-Dateien bei einer der Root-CA der Smart Metering PKI untergeordneten Sub-CA ein.



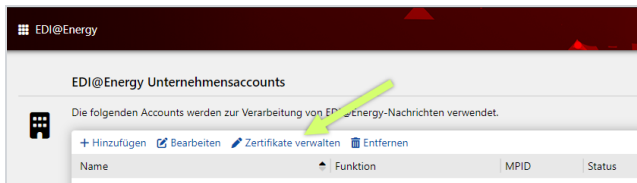
Eine Auflistung der bei der Root-CA der Smart Metering PKI registrierten Sub-CAs finden Sie auf der Seite Aktuelle Registrierungen bei der SM-PKI Root-CA des BSI.

| Zertifikate importieren

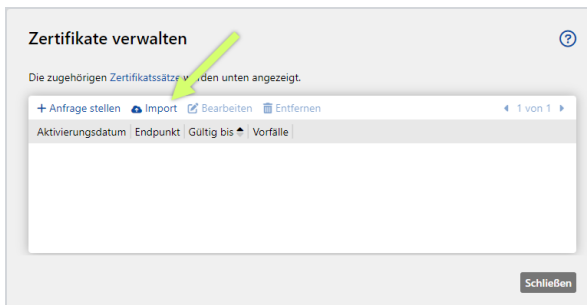
Sobald die Zertifikate ausgestellt worden sind und vorliegen, müssen Sie diese importieren.

1. Gehen Sie zu **EDI@Energy > Einstellungen > EDI@Energy-Unternehmensaccounts**.

2. Markieren Sie das entsprechende Konto und klicken Sie **Zertifikate verwalten**.



3. Klicken Sie **Import**.



4. Wählen Sie die jeweiligen Zertifikate aus und klicken Sie **Import**.

Nachdem die Zertifikate erfolgreich importiert wurden, wird der Status **Ok** für den jeweiligen Marktpartner angezeigt.

I Einstellungen ändern

Um die vorgenommenen Einstellungen später zu verändern, markieren Sie das entsprechende Konto und klicken Sie

- **Bearbeiten**, um den externen Endpunkt und den internen Empfänger anzupassen beziehungsweise
- **Zertifikate verwalten**, um weitere/andere Zertifikate zu importieren.

Schritt 6: Marktpartner-Kommunikation aktivieren

In diesem Schritt aktivieren die aus- und eingehende AS4-Kommunikation.

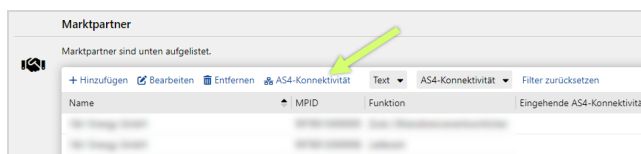


NoSpamProxy lädt die aktuelle Liste aller Marktpartner automatisch regelmäßig herunter.

Ausgehendes AS4 anfragen

Um die ausgehende AS4-Kommunikation mit einem Marktpartner zu aktivieren, müssen Sie eine entsprechende Anfrage stellen.

1. Gehen Sie zu **EDI@Energy > Marktpartner**.
2. Wählen Sie den gewünschten Marktpartner aus und klicken Sie **AS4-Konnektivität**.

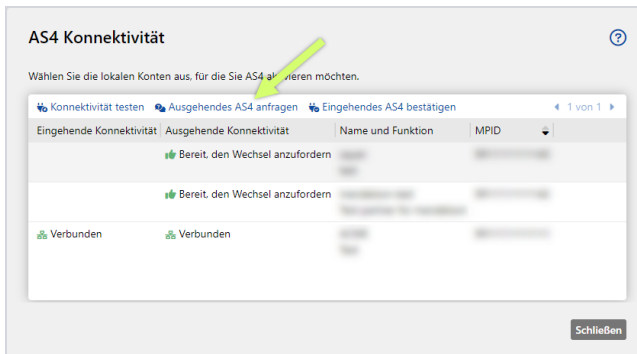


3. Wählen Sie das von Ihnen hinterlegte EDI@Energy-Unternehmenskonto aus, für das Sie die AS4-Kommunikation mit dem Marktpartner aktivieren wollen.



HINWEIS: Unter **Ausgehende Konnektivität** muss der Hinweis **Bereit, den Wechsel anzufordern** angezeigt werden. Ansonsten können Sie den Wechsel nicht anfragen.

4. Klicken Sie **Ausgehendes AS4 anfragen**.

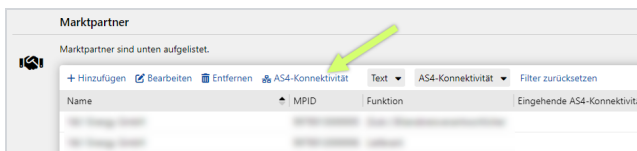


Sobald der Marktpartner den Wechsel zu AS4 bestätigt hat, wird unter **Ausgehende Konnektivität** der Hinweis **Verbunden** angezeigt. NoSpamProxy akzeptiert ausgehende EDI-Nachrichten dann nur noch über AS4. Dieser Vorgang ist nicht umkehrbar.

Eingehendes AS4 bestätigen

Um die eingehende AS4-Kommunikation mit einem Marktpartner zu aktivieren, müssen Sie die entsprechende Anfrage des Marktpartners bestätigen.

1. Gehen Sie zu **EDI@Energy > Marktpartner**.
2. Wählen Sie den gewünschten Marktpartner aus und klicken Sie **AS4-Konnektivität**.

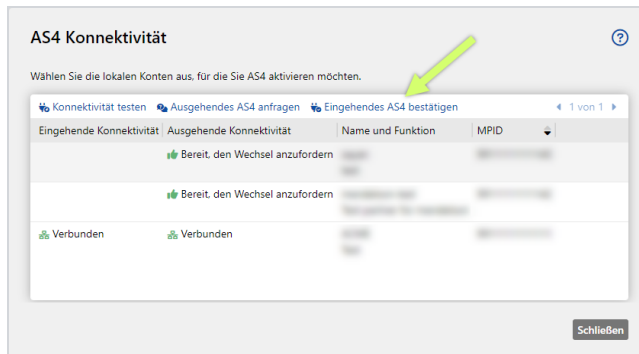


3. Wählen Sie das von Ihnen hinterlegte EDI@Energy-Unternehmenskonto aus, für das Sie die AS4-Kommunikation mit dem Marktpartner aktivieren wollen.



HINWEIS: Unter **Eingehende Konnektivität** muss der Hinweis **Anfrage ausstehend** angezeigt werden.

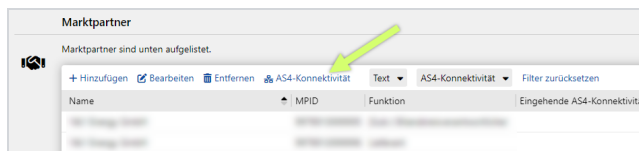
4. Klicken Sie **Eingehendes AS4 bestätigen**.



Sobald Sie den Wechsel zu AS4 bestätigt haben, wird unter **Eingehende Konnektivität** der Hinweis **Verbunden** angezeigt. NoSpamProxy akzeptiert eingehende EDI-Nachrichten dann nur noch über AS4. Dieser Vorgang ist nicht umkehrbar.

Testen der AS4-Konnektivität

1. Gehen Sie zu **EDI@Energy > Marktpartner**.
2. Wählen Sie den gewünschten Marktpartner aus und klicken Sie **AS4-Konnektivität**.





Es werden Informationen zur AS4-Konnektivität für die einzelnen, von Ihnen hinterlegten EDI@Energy-Unternehmenskonten angezeigt.

3. Sofern keine Zertifikatsfehler vorliegen: Klicken Sie **Konnektivität testen**.

AS4 Konnektivität ⓘ

Wählen Sie die lokalen Konten aus, für die Sie AS4 aktivieren möchten.

Konnektivität testen | Ausgehendes AS4 anfragen | Eingehendes AS4 bestätigen | 1 von 1

Eingehende Konnektivität	Ausgehende Konnektivität	Name und Funktion	MPID
🟢 Bereit, den Wechsel anzufordern			
🟢 Bereit, den Wechsel anzufordern			
🟢 Verbunden	🟢 Verbunden		



Schließen

AS4-Nachrichtenverfolgung

AS4-Nachrichten werden in einer AS4-spezifischen Nachrichtenverfolgung angezeigt.

Unter **EDI@Energy > Nachrichtenverfolgung** finden Sie neben allgemeinen Informationen auch Informationen zur AS4-Konformität.

Verwendete Icons

- | Konformität: Entspricht den Spezifikationen der AS4-Richtlinien.
- | Keine Konformität: Entspricht nicht den Spezifikationen der AS4-Richtlinien.
-  Aus dem Internet empfangen
-  Von einem E-Mail-Server des Unternehmens



TIP: Details zur Konformität einer E-Mail finden Sie auf der Registerkarte **Konformität** in der Detailansicht eines Message Tracks.

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

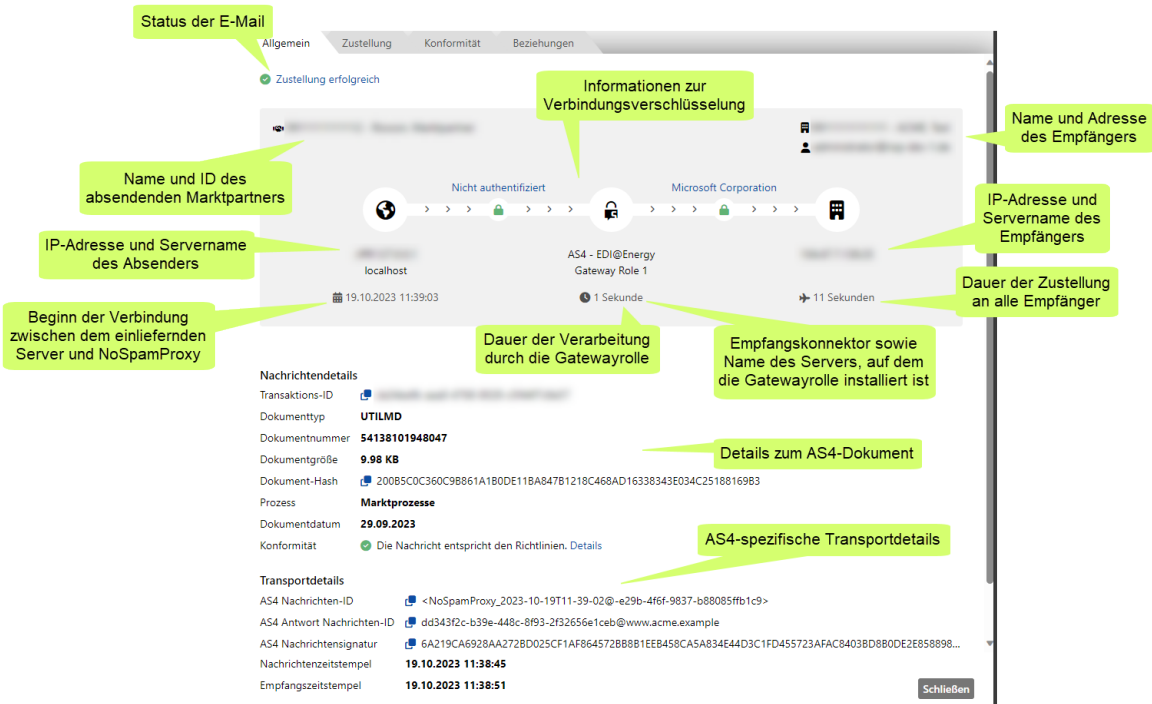
Verwenden Sie die Nachrichtenverfolgung, um herauszufinden, wie Ihre AS4-Nachrichten von NoSpamProxy verarbeitet wurden. Für eine bessere Übersicht stehen Ihnen verschiedene Filter zur Verfügung:



Details anzeigen

Registerkarte Allgemein

Hier finden Sie allgemeine Informationen zur E-Mail und deren Anhängen, zur Verbindung und Übertragung sowie zu AS4-spezifischen Details.



Registerkarte Zustellung

Hier finden Sie Informationen zu den einzelnen Zustellversuchen.

[Allgemein](#)
[Zustellung](#)
[Konformität](#)
[Beziehungen](#)

Empfänger
 Unternehmenskonto [redacted]
 Interner Empfänger [redacted]

Zustellversuche
 Der Status jedes einzelnen Zustellversuchs ist unten aufgeführt.

Status	Datum	Details
● Zustellung erfolgreich	19.10.2023 11:39:14	Zugestellt an [redacted] durch Office 365
■ Ausstehend (Warteschlange)	19.10.2023 11:39:03	

Der jüngste Zustellversuch erscheint oben in der Liste.

Registerkarte Konformität

Hier finden Sie Informationen zu den verwendeten Zertifikaten und Algorithmen.

[Allgemein](#)
[Zustellung](#)
[Konformität](#)
[Beziehungen](#)

● Die Nachricht entspricht den Richtlinien.

Sicherheit

Verschlüsselungs-Zertifikat [redacted]

Verschlüsselungs-Algorithmus ● **AES-128 GCM mit ECDH**

Signatur-Zertifikat [redacted]

● Das Zertifikat wurde erfolgreich validiert.

Signatur-Algorithmus ● **SHA-256 mit ECDSA** unter Verwendung der Kurve **Brainpool P256R1**

[Schließen](#)

Registerkarte Beziehungen

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

[Allgemein](#)
[Zustellung](#)
[Konformität](#)
[Beziehungen](#)

Diese Nachricht bezieht sich auf folgende E-Mails.

[Öffnen](#)

Typ	Status	Empfangsdatum	Empfänger	Betreff
Nachfolger	Zustellung erfolgreich	18.10.2023 08:11:50	[redacted]	Delivery failed - [redacted]

Typ der Beziehung

[Schließen](#)

I Fehler beim Senden

Wenn das Senden einer ausgehenden AS4-Nachricht fehlschlägt, wird ein neuer Versuch unternommen, unabhängig von den empfangenen EBMS-Fehlern. Wenn die Antwort fehlerhaft ist, wird der Versuch wiederholt. Die Wiederholungsschleife wird nach drei Minuten abgebrochen.

In den folgenden Fällen wird nach erstmaligem Fehlschlagen kein neuer Zustellungsversuch gestartet:

- DNS-Fehler sind aufgetreten.
- Die Verbindung wird verweigert. Dies bedeutet in der Regel, dass der Host zwar erreichbar ist, der Dienst aber nicht ausgeführt wird.
- Das TLS-Zertifikat des Empfängers ist nicht vertrauenswürdig.

Sie können den EDI@Energy-Dienst so konfigurieren, dass er EDIFACT-Dokumente auf Ihrem Datenträger speichert, falls das Senden der entsprechenden Nachricht fehlschlägt. Siehe [Speicherort für EDIFACT-Dokumente konfigurieren](#).

I Wann gilt eine E-Mail als AS4-Nachricht?

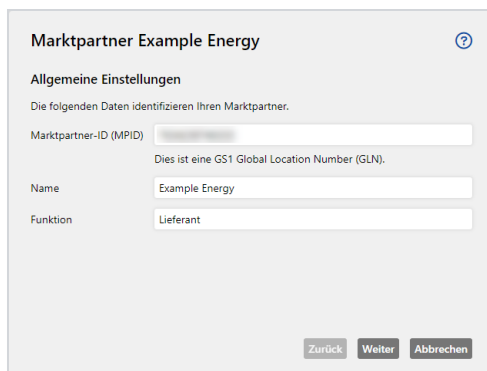
NoSpamProxy betrachtet E-Mails als AS4-Nachrichten, wenn alle folgenden Bedingungen erfüllt sind:

- Die E-Mail hat einen Empfänger.
- Die E-Mail hat einen EDIFACT-Anhang.
- Die Werte für den Betreff und den Namen des Anhangs sind identisch.
- Der Betreff der E-Mail ist [BDEW-konform](#).
- Die Absenderadresse entspricht einem der konfigurierten EDI@Energy-Postfächer.

Marktpartner manuell hinzufügen

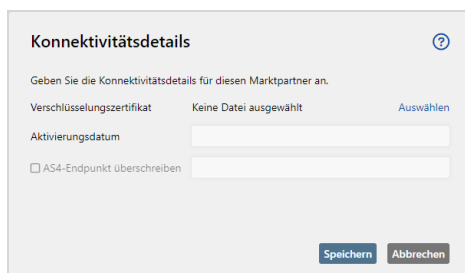
Sollte ein Marktpartner nicht in der Liste unter **Marktpartner** aufgeführt sein, können Sie diesen manuell hinzufügen.

1. Gehen Sie **EDI@Energy > Marktpartner**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie unter **Allgemeine Einstellungen** die MPID, den Namen und die Funktion des Marktpartners ein und klicken Sie **Weiter**.



The screenshot shows a web form titled "Marktpartner Example Energy" with a help icon. Under the "Allgemeine Einstellungen" section, there is a sub-header "Die folgenden Daten identifizieren Ihren Marktpartner." followed by three input fields: "Marktpartner-ID (MPID)" with a placeholder and a note "Dies ist eine GS1 Global Location Number (GLN).", "Name" with the value "Example Energy", and "Funktion" with the value "Lieferant". At the bottom are three buttons: "Zurück", "Weiter", and "Abbrechen".

4. Klicken Sie unter **Verschlüsselungszertifikate** auf **Hinzufügen**.
5. Fügen Sie die entsprechenden Zertifikate hinzu und geben Sie das jeweilige Aktivierungsdatum an.



The screenshot shows a web form titled "Konnektivitätsdetails" with a help icon. It contains the instruction "Geben Sie die Konnektivitätsdetails für diesen Marktpartner an." and two sections: "Verschlüsselungszertifikat" with the text "Keine Datei ausgewählt" and a blue "Auswählen" link, and "Aktivierungsdatum" with an empty input field. Below these is a checkbox labeled "AS4-Endpunkt überschreiben" which is unchecked. At the bottom are two buttons: "Speichern" and "Abbrechen".

6. Wählen Sie, ob Sie den AS4-Endpunkt überschreiben wollen.



HINWEIS: Aktivieren Sie diese Option, wenn Sie **nicht** die Adresse verwenden wollen, die im Zertifikat des Marktpartners genannt ist.

7. Klicken Sie **Beenden**.

Schlüsselspeicher ändern



HINWEIS: Diese Einstellung ist nur verfügbar, wenn Sie ein HSM einsetzen. Siehe [Schritt 4: Key-Management-Dienst konfigurieren](#).

Um den Speicherort der von Ihnen verwendeten EDI@Energy-Zertifikate zu ändern, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **EDI@Energy > Einstellungen > Zertifikatskonfiguration**.
2. Klicken Sie **Bearbeiten**.
3. Wählen Sie den HSM-Slot aus, den Sie für das Speichern der Zertifikate nutzen wollen.

Allgemeine Einstellungen ⓘ

Schlüsselspeicher

NoSpamProxy speichert neue private Schlüssel im unten ausgewählten HSM-Token.

HSM-Token

Speichern Abbrechen

4. Klicken Sie **Speichern**.

Speicherort für EDIFACT-Dokumente konfigurieren

Sie können den EDI@Energy-Dienst so konfigurieren, dass er EDIFACT-Dokumente auf Ihrem Datenträger speichert, falls das Senden der entsprechenden Nachricht fehlschlägt. Siehe [Fehler beim Senden](#).

1. Wechseln Sie zu dem Computer, auf dem der EDI@Energy-Dienst läuft.
2. Öffnen oder erstellen Sie die Datei **ProgramData/Net at Work Mail Gateway/Edi@Energy/outbound-diagnostics-config.json**.
3. Setzen Sie innerhalb der Datei die folgenden beiden Properties:
 - "SaveFailedDocuments": true
 - "FailedDocumentsPath": "C:/ProgramData/Net at Work Mail Gateway/Edi@Energy/attachments"



HINWEIS: Sie können diesen Pfad auch frei wählen. Stellen Sie aber sicher, dass der EDI@Energy-Dienst dort Schreibrechte hat.

4. Speichern Sie die Datei **outbound-diagnostics-config.json**.

Anhang

Filter in NoSpamProxy	288
In NoSpamProxy verfügbare Filter	291
Aktionen in NoSpamProxy	317
In NoSpamProxy verfügbare Aktionen	318
Grundlagen	340

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.

I 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
- CSA Certified IP List
- Erlaubte Unicode-Sprachbereiche
- 32Guards
- Realtime Blocklists
- Reputationsfilter
- Spamassassin Konnektor
- Spam URI Realtime Blocklists
- Wortübereinstimmungen

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

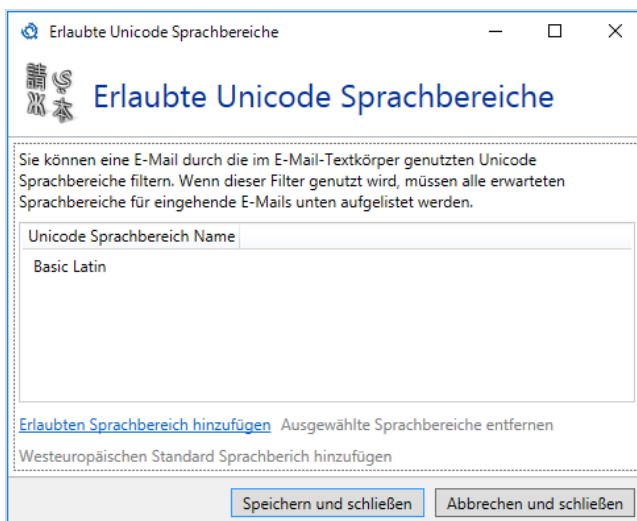


Dieser Filter ist gültig für folgende Absender: Extern und Lokal.
Standard SCL-Wert bei einfachem Multiplikator ist 4.

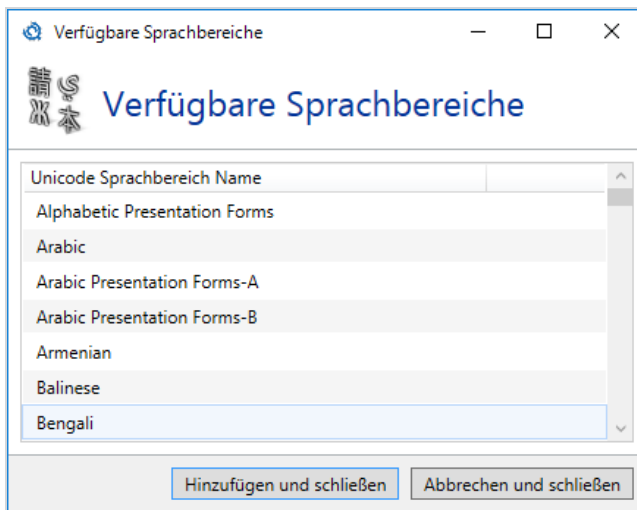
Spam-E-Mails kommen teilweise aus Sprachräumen, mit denen man üblicherweise keine Kommunikation unterhält. So kann zum Beispiel Spam eintreffen, der chinesische Schriftzeichen enthält. Dieser Filter kann E-Mails abblocken, in dem er alle enthaltenen Zeichensätze analysiert und die E-Mail nur passieren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



TIP: 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



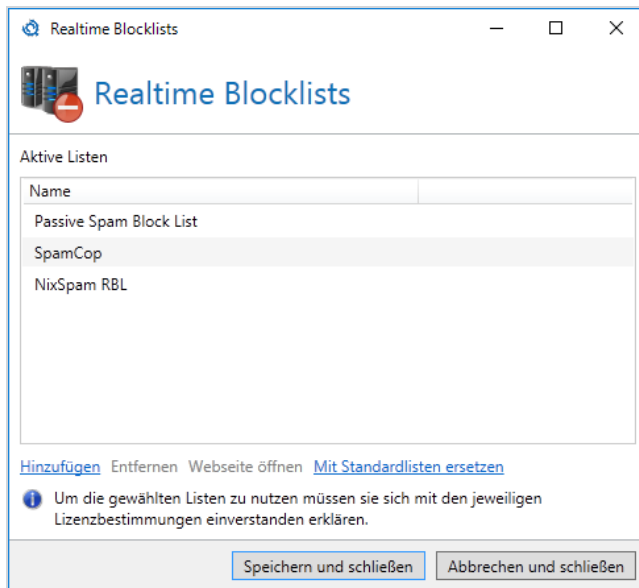
Dieser Filter ist gültig für folgende Absender: Extern. Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Listen. Pro Treffer werden die in der Liste eingestellten SCL-Punkte vergeben.

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.

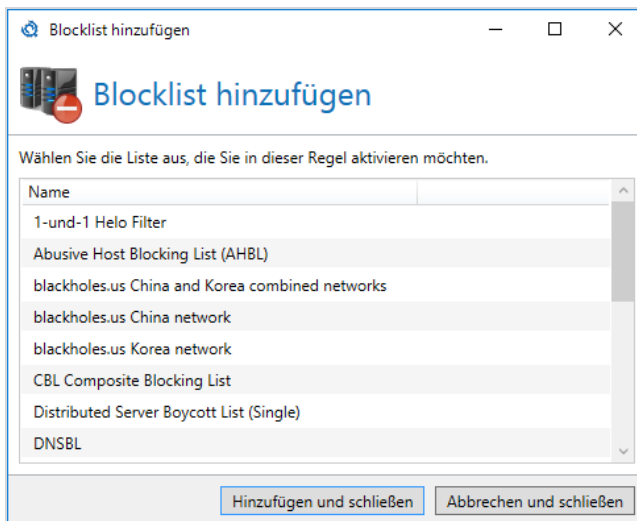
Anwendung

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**.



TIP: 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	<p>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.</p> <p>Dieser Test vergibt nur SCL-Punkte, falls keine DMARC-Policy aktiv ist.</p>
DMARC-Ergebnis 'Quarantäne'	<p>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.</p> <p>Die Höhe der vergebenen Punkte hängt vom</p>


Titel	Beschreibung
	angewandten DMARC-Ergebnis ab.
DMARC-Ergebnis 'Abweisen'	<p>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.</p> <p>Die Höhe der vergebenen Punkte hängt vom angewandten DMARC-Ergebnis ab.</p>
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 **Vetruenswürdige ARC-Unterzeichner**.

Titel	Beschreibung
Ungültige spitze Klammern	<p>Prüft, ob der 'Header-From' eine spitze Klammer mit einer ungültigen E-Mail-Adresse enthält, was nicht RFC-konform ist.</p> <p>Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.</p>
Fehlender Absender	<p>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</p>

Titel	Beschreibung
	ein Missbrauch nicht erkannt wird.
Unternehmensdomäne in der E-Mail-Adresse	<p>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.</p> <p>Beachten Sie, dass ein solcher Fall auch auftreten kann, wenn ein externes E-Mail-System im Namen der Unternehmensdomäne sendet, aber nicht als <u>E-Mail-Server des Unternehmens hinzufügen</u> konfiguriert ist.</p> <p>EXAMPLE: <xyz@netatwork.de></p>

Titel	Beschreibung
	 <p>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 <u>Aufheben der DKIM-Signatur im Reputationsfilter.</u></p>
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
	<p>Anzeigenamen verwendet, da in vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint. Der Absender kann so eine falsche Identität vortäuschen.</p> <p>EXAMPLE: "Uwe Ulbrich uwe.ulbrich@netatwork.de" <spam@spammer.de></p>
<p>Unterdomäne einer Unternehmensdomäne in der E-Mail-Adresse</p>	<p>Prüft, ob eine Unterdomäne einer Unternehmensdomäne verwendet wird. Ist diese Unterdomäne legitim, wird der Test 'Unternehmensdomäne in der E-Mail-Adresse' angewendet.</p> <p>EXAMPLE: <xyz@hr.netatwork.de></p>
<p>Unterdomäne einer Unternehmensdomäne im Anzeigenamen</p>	<p>Prüft, ob der Anzeigename eine Subdomäne einer Unternehmensdomäne enthält. Domänen im Anzeigenamen werden von Spammern verwendet, da in vielen Mobilgeräten und E-Mail-</p>

Titel	Beschreibung
	<p>Programmen zunächst nur dieser Name erscheint. Der Absender kann so eine falsche Identität vortäuschen.</p> <p>EXAMPLE: "hr.netatwork.de" <spam@spammer.de></p>
<p>Verschleierte Unternehmensdomäne in der E-Mail-Adresse</p>	<p>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.</p> <p>EXAMPLE: <xyz@n3tatw0rk.de></p>
<p>Verschleierte Unternehmensdomäne im Anzeigenamen</p>	<p>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, da in vielen Mobilgeräten und E-Mail-</p>

Titel	Beschreibung
	<p>Programmen zunächst nur dieser Name erscheint.</p> <p>EXAMPLE: "Uwe Ulbrich uwe.ulbrich@n3tatw0rk.de" <spam@spammer.de></p>
<p>Unterdomäne einer verschleierte Unternehmensdomäne in der E-Mail-Adresse</p>	<p>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.</p> <p>EXAMPLE: <xyz@hr.n3tatw0rk.de></p>
<p>Unterdomäne einer verschleierte Unternehmensdomäne im Anzeigenamen</p>	<p>Wie der Test 'Unterdomäne einer Unternehmensdomäne im Anzeigenamen'. Zusätzlich wird hier geprüft, ob ASCII-Schriftzeichen in der Domäne verwendet wurden, die bestimmten Buchstaben ähnlich sehen. Domänen im Anzeigenamen</p>

Titel	Beschreibung
	<p>werden von Spammern verwendet, da in vielen Mobilgeräten und E-Mail-Programmen zunächst nur dieser Name erscheint.</p> <p>EXAMPLE: Uwe Ulbrich uwe.ulbrich@hr.n3tatw0rk.de" <spam@spammer.de></p>
Mehrere E-Mail-Adressen	<p>Prüft, ob der 'Header-From' mehr als eine E-Mail-Adresse enthält, was nicht RFC-konform ist.</p> <p>Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.</p>
Domäne im Anzeigenamen abweichend von der E-Mail-Adresse	<p>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 vielen Mobilgeräten und E-Mail-</p>

Titel	Beschreibung
	<p>Programmen zunächst nur dieser Name erscheint.</p> <p>EXAMPLE:</p> <pre>"service@paypal.com" <spam@spammer.de></pre>

Titel	Beschreibung
Ungültiges '@'	<p>Prüft, ob der 'Header-To' ein '@'-Zeichen enthält, das nicht Teil einer E-Mail-Adresse ist, was nicht konform mit RFC 5322 ist.</p> <p>Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.</p>
Ungültige spitze Klammern	<p>Prüft, ob der 'Header-To' spitze Klammern mit einer ungültigen E-Mail-Adresse enthält, was nicht konform mit RFC 5322 ist.</p>

Titel	Beschreibung
	<p>Fehlende RFC-Konformität deutet auf Spam hin, da Spammer sich unter Umständen weniger Mühe geben, eine solche Konformität sicherzustellen.</p>
<p>Fehlendes 'Header-To'</p>	<p>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.</p>
<p>Fehlende Unternehmens-E-Mail-Adresse</p>	<p>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.</p>

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



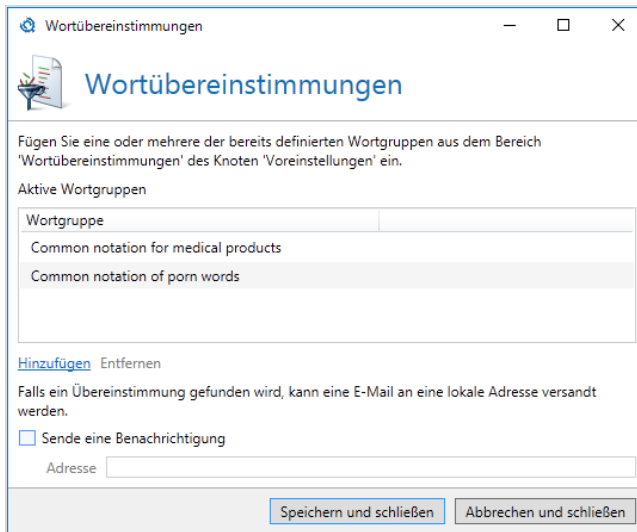
Dieser Filter ist gültig für folgende Absender: Extern und Lokal. Der Standard SCL-Wert bei einfachem Multiplikator ist abhängig von den im Filter gewählten Wortgruppen. Pro Treffer werden die in der Wortgruppe eingestellten SCL-Punkte vergeben.

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.

Inhalt der Wortgruppe

Allgemein **Wörter**

Name

Vergebe Punkte Für *jede* Übereinstimmung mit der Wortliste
 Falls **keine** Übereinstimmung gefunden wird


Bereich Betreffzeile
 E-Mail-Inhalt

Punkte
10 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.



Inhalt der Wortgruppe

Allgemein Wörter

Art

Einfach (*schnell*), empfohlen

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

Regulärer Ausdruck (langsamer, mit Vorsicht verwenden)

Neues Wort

Wort
https://bit.ly/*

Entfernen

Auch ähnliche Wörter finden

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 Virens Scanner oder die Aktion [Greylisting](#).

I 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.

I 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
- Automatische Antwort
- CxO-Betrugserkennung
- Disclaimer anwenden
- DKIM-Signatur anwenden
- Greylisting
- Leite E-Mail um
- Malware-Scanner
- 32Guards
- URL Safeguard (Aktion)
- Verberge interne Topologie

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:

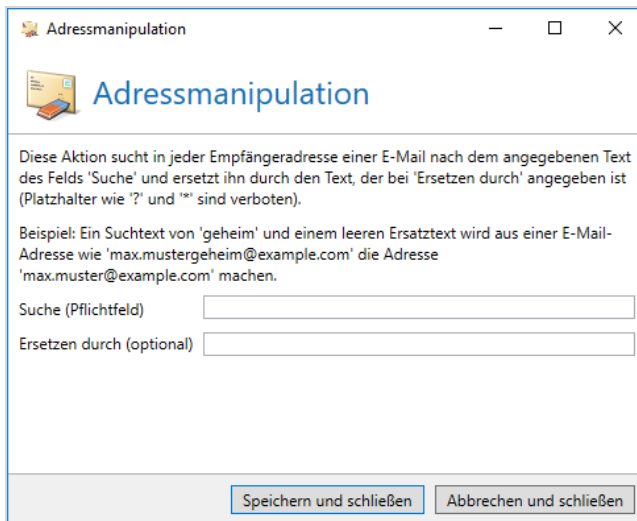
Position	Von	An	Entscheidung	Aktion
1	*@*	*geheim@example.com	Pass	Adressmanipulation

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**.



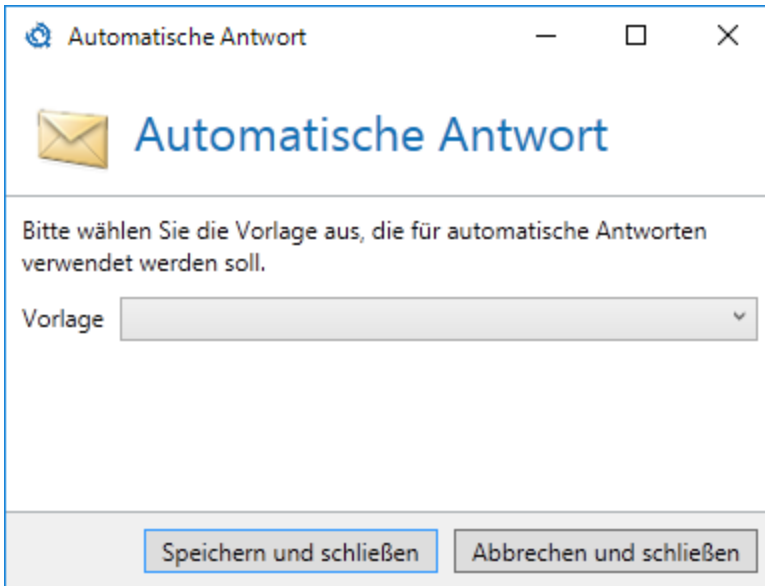
TIP: Es ist beispielsweise sinnvoll, den String "topsecret" in der "Geheim"-Adresse "user1topsecret@example.com" durch einen leeren String für die korrekte Adresse "user1@example.com" zu ersetzen.

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 anderen, eindeutigen Namen in dem Ordner **%ProgramData%\Net at Work Mail Gateway\Intranet\Templates**.

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. 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.

I 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.

I Die CxO-Betrugserkennung kennenlernen

Die CxO-Betrugserkennung kennenlernen

Um sich mit der Funktionsweise der CxO-Betrugserkennung vertraut zu machen, empfehlen wir die folgende Vorgehensweise:

1. Fügen Sie der entsprechenden AD-Gruppe die E-Mail-Adressen Ihrer IT-Mitarbeiter hinzu. Siehe Benutzerimport automatisieren.
2. Erstellen Sie eine separate, temporäre Regel, die unter **Bereich** auf die **privaten** E-Mail-Adressen des IT-Personals als **Absender** und die **Unternehmens-E-Mail-Adressen** als **Empfänger** filtert.
3. Simulieren Sie nun Angriffe, indem Sie E-Mails von den privaten E-Mail-Adressen der IT-Mitarbeiter an deren Unternehmens-E-Mail-Adressen senden.
4. Beobachten Sie, wie sich die CxO-Betrugserkennung verhalten würde, wenn sie vollständig aktiviert wäre. Die Informationen auf der Registerkarte

Aktivitäten einer E-Mail in der Nachrichtenverfolgung sind hierbei hilfreich.
Siehe [Details zu einer E-Mail anzeigen](#).

So kann Ihr IT-Personal die Funktionsweise der CxO-Betrugserkennung nachvollziehen.



TIP:

Vor der eigentlichen Aktivierung der CxO Betrugserkennung in NoSpamProxy sollte die IT-Abteilung dem höheren Management mitteilen, dass sie nun sorgfältiger geschützt sind. Es zeigt sich häufig, dass auch höhere Führungsebenen zwischen privaten und geschäftlichen Identitäten kommunizieren. Bei aktivierter CxO-Betrugserkennung ist es wahrscheinlich, dass diese Art der Kommunikation seitens NoSpamProxy unterbunden wird.

Das höhere Management sollte deshalb darüber informiert werden, wie **Level of Trust** helfen kann, diese Kommunikation weiterhin zuzulassen, also beispielsweise eine E-Mail von intern an extern zu senden und auf diese E-Mail zu antworten.

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 [NoSpamProxy 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**.

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

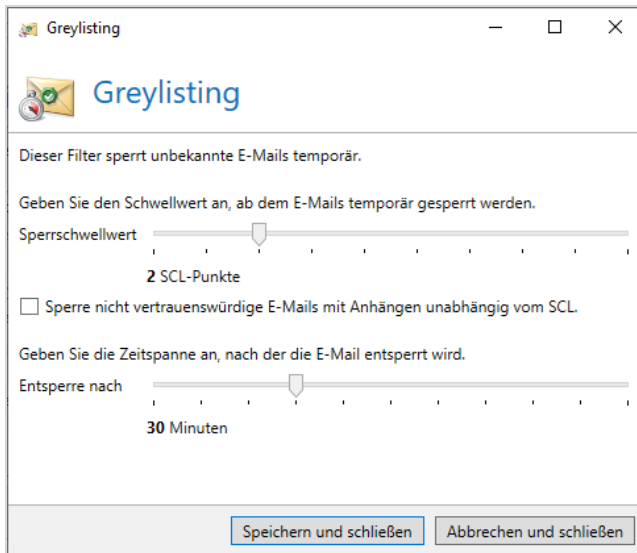
anweist, die E-Mail nach einiger Zeit erneut zu senden. Die E-Mail wird dann erneut zugestellt. Dabei kann eingestellt werden, ab wann der einliefernde Server einen zweiten Versuch starten darf.

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.

Leite E-Mails um

Nutzen Sie dies Aktion um E-Mails zu neuen Empfängern umzuleiten.

Versende nur zu den **neuen** Empfängern

Versende **zusätzlich** zu den neuen Empfängern

Neue Empfänger

Adresse

Adresse

Entfernen

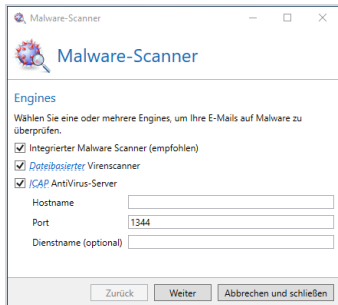


HINWEIS: Es muss mindestens eine Empfängeradresse in der Liste hinterlegt werden, um die Aktion nutzen zu können.

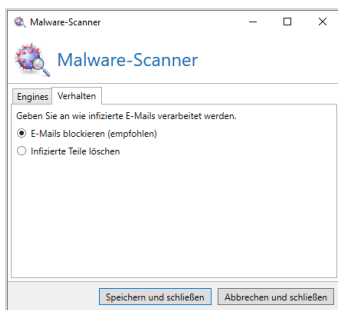
Malware-Scanner

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 Virenschannern auf der Gatewayrolle zu gewährleisten, beachten Sie auch die Hinweise unter [Installierte On-Access-Virenschanner konfigurieren](#).

Siehe auch

[Melden von False Negatives und False Positives](#)

Dateibasierter Virenschanner

Diese Aktion ist gültig für folgende Absender: Extern und Lokal.

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

Auch Anhänge aus E-Mails im RTF-Format können von Virensclannern 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 `C:\ProgramData\Net at Work Mail Gateway\Temporary Files\Netatwork.NoSpamProxy.Addins.Core.Actions.MalwareScan.FilebasedMalwareScanner`.

Um (wiederkehrende) Probleme beim Zusammenspiel von installierten On-Access-Virensclannern zu beheben, konfigurieren Sie Ihren Virensclanner 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



HINWEIS: Sollten Sie ein Update von Version 13 vorgenommen haben, so lautet der Pfad **C:\Program Files\Net at Work Mail Gateway\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



HINWEIS: Sollten Sie ein Update von Version 13 vorgenommen haben, so lautet der Pfad **C:\Program Files\Net at Work Mail Gateway\enQsig Webportal**.

Ansonsten kann es bei einigen Virenschannern 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-Virenschanner dies ermöglicht.



HINWEIS: Stellen Sie sicher, dass Ihr lokal eingesetzter Virenschanner nicht durch verhaltensbasierte Analysen Rückschlüsse daraus zieht, dass im Pfad **C:\ProgramData\Net at Work Mail Gateway\Temporary Files\Netatwork.NoSpamProxy.Addins.Core.Actions.MalwareScan.FilebasedMalwareScanner** durch Prozesse aktiv Malware abgelegt wird. Eine Prüfung der Dateien an sich sollte beziehungsweise muss stattfinden, jedoch darf das Ablegen von Malware im besagten Ordner nicht zur Klassifizierung des entsprechenden Prozesses führen, der dies durchführt.

**TIP:**

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 Virenskan 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 Virenskan" 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 Virenschanner 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.

I 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](#).

I URL Safeguard (Aktion)

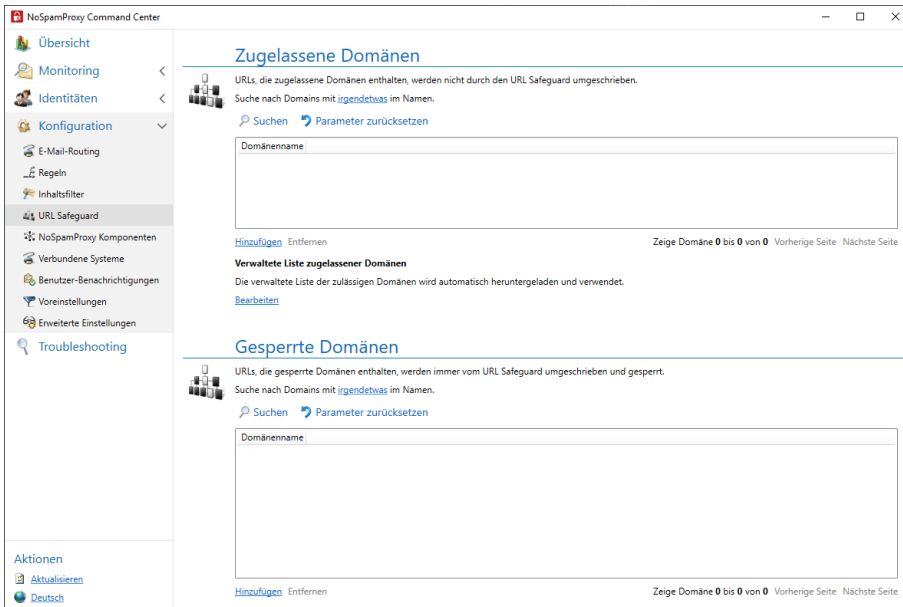
Den URL Safeguard aktivieren

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](#).

Zugelassene und gesperrte Domänen konfigurieren



Zugelassene Domänen

URLs, die zugelassene Domänen enthalten, werden nicht durch den URL Safeguard umgeschrieben.

1. Gehen Sie zu **Konfiguration > URL Safeguard > Zugelassene Domänen**.
2. Klicken Sie **Hinzufügen**.
3. Führen Sie eine der beiden folgenden Aktionen durch:
 - Geben Sie die gewünschte Domäne in das Eingabefeld ein und klicken Sie **Hinzufügen**.
 - Klicken Sie **Aus Zwischenablage hinzufügen**, um eine Liste von Domänen aus der Zwischenablage hinzuzufügen.
4. Klicken Sie **Speichern und schließen**.

Verwaltete Liste zugelassener Domänen

NoSpamProxy bietet eine verwaltete Liste zulässiger Domänen bekannter Websites.

1. Gehen Sie zu **Konfiguration > URL Safeguard > Verwaltete Liste zugelassener Domänen**.
2. Klicken Sie **Bearbeiten**.
3. Setzen oder entfernen Sie das Häkchen bei **Automatisches Herunterladen und Verwenden der verwalteten Liste**.
4. Klicken Sie **Speichern und schließen**.

Gesperrte Domänen

URLs, die gesperrte Domänen enthalten, werden immer vom URL Safeguard umgeschrieben und gesperrt.

1. Gehen Sie zu **Konfiguration > URL Safeguard > Gesperrte Domänen**.
2. Klicken Sie **Hinzufügen**.
3. Führen Sie eine der beiden folgenden Aktionen durch:
 - Geben Sie die gewünschte Domäne in das Eingabefeld ein und klicken Sie **Hinzufügen**.
 - Klicken Sie **Aus Zwischenablage hinzufügen**, um eine Liste von Domänen aus der Zwischenablage hinzuzufügen.
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

I 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.

**TIP:**

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.

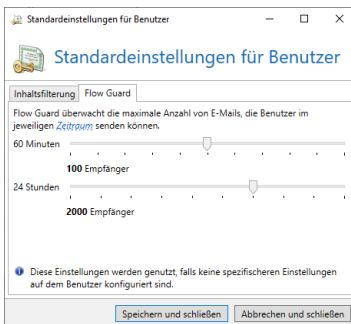
Updates auf NoSpamProxy 14 und höher

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



TIP: 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

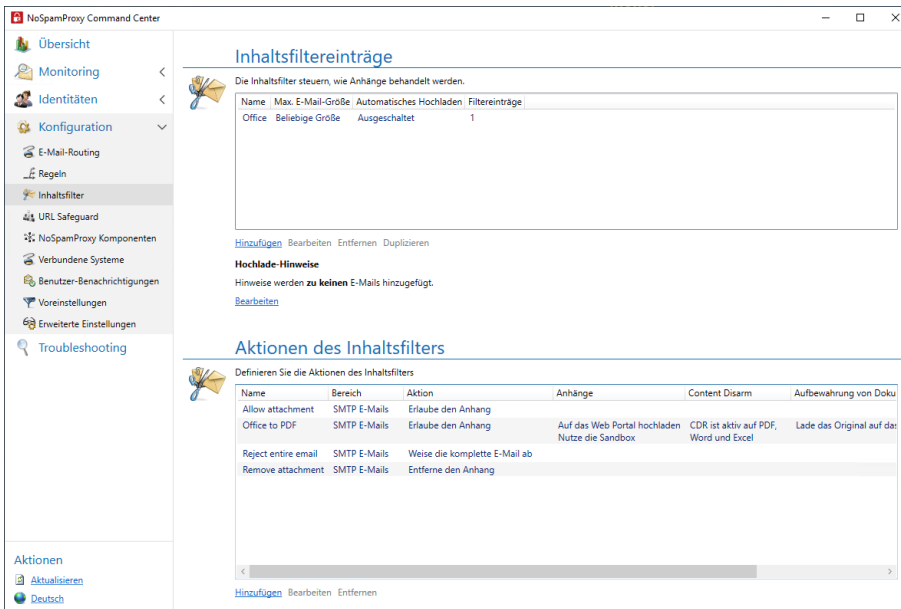
- die Standardeinstellungen für Benutzer konfigurieren beziehungsweise
- die Einstellungen unter **Identitäten > Unternehmensbenutzer** für den jeweiligen Unternehmensbenutzer konfigurieren.

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**, unter denen die Inhaltsfilteraktionen ausgelöst werden.

Sie konfigurieren sowohl Inhaltsfilteraktionen als auch Bedingungen, indem Sie einem Inhaltsfilter einen oder mehrere Inhaltsfiltereinträge zuweisen. Siehe **Inhaltsfilter anlegen** sowie **Inhaltsfilteraktionen anlegen**.

Sie können das Level-of-Trust-System nutzen, um verschiedene Aktionen für einen Dateityp zu triggern, beispielsweise

- ein Word-Dokument mit Makros (2007-2016, DOCM) aus nicht vertrauenswürdigen E-Mails komplett blockieren, aber
- eine CDR-Aktion für vertrauenswürdige E-Mails von Ihren Partnern ausführen lassen.

Verwandte Schritte

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

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**.

I 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.

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.

I 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](#).

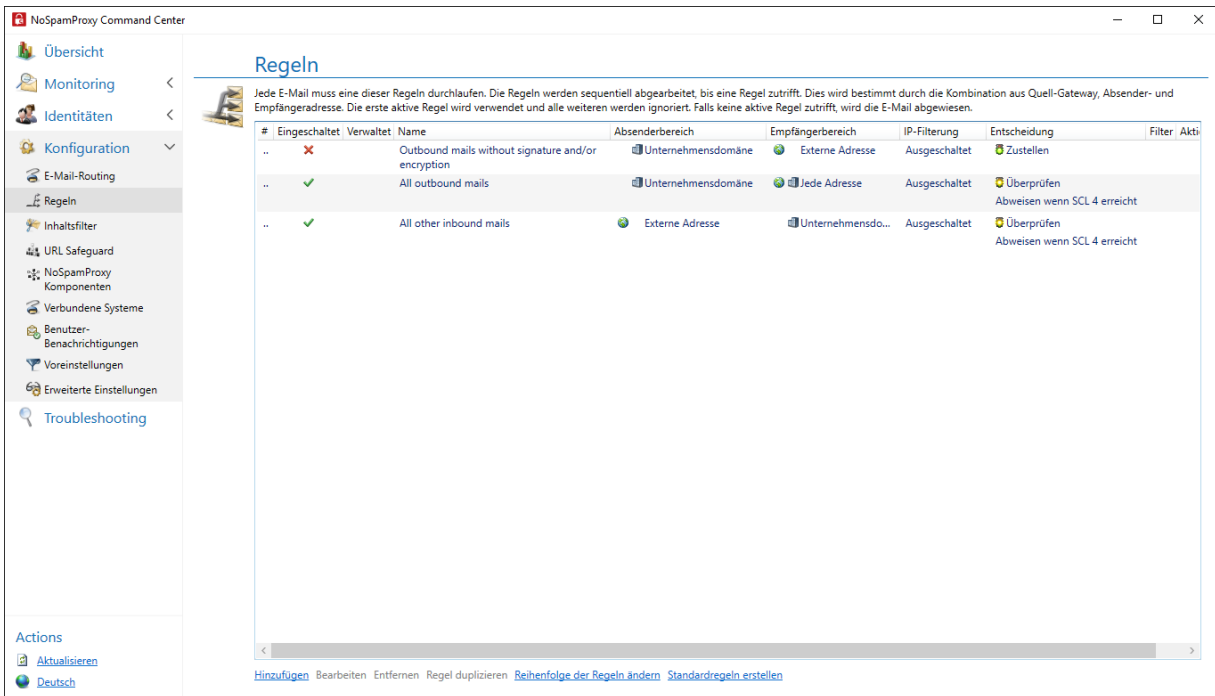
| Siehe auch

[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.



TIP: 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 **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 Virenschanner 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](#).

I 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

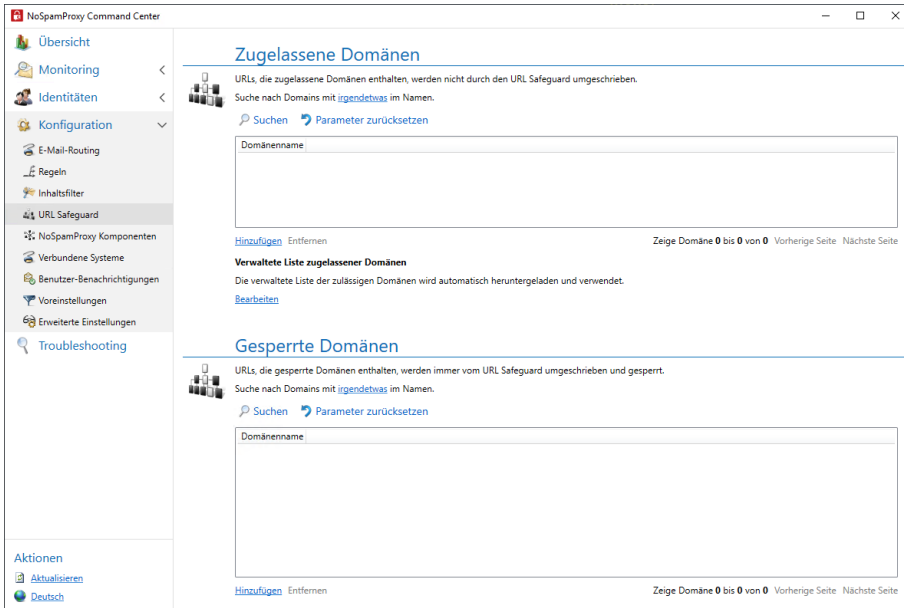
Falls entsprechend konfiguriert, prüft der URL Safeguard die Links in eingehenden E-Mails gegen Einträge in den folgenden Listen:

- 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.



TIP: 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 Qualified 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 \(Aktion\)](#)

[Vorschaltseiten URL Safeguard](#)

[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.

Unser Support-Team erreichen Sie

- per Telefon unter +49 5251304-636
- per E-Mail unter support@nospamproxy.de.

