noSpam proxy® SERVER

Installationshandbuch

Version 14

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

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

DIESES DOKUMENT WURDE ZULETZT AM 31. MÄRZ 2023 ÜBERARBEITET.

Inhalt

Systemvoraussetzungen

Allgemeine Voraussetzungen

Hardware

- Eigener, vollwertiger E-Mail-Server (cloudbasiert oder on-premises)
- 4GB RAM Hauptspeicher
- 2 CPU-Kerne (virtualisiert oder physisch)
- Ausreichender Speicherplatz. Die benötigte Größe hängt von der Zahl der empfangenen E-Mails und von den eingesetzten Modulen ab. Sprechen Sie unser Support-Team an, um Unterstützung bei der Planung zu bekommen.

Kommunikation

- SMTP-Protokoll für ein- und ausgehende Nachrichten. NoSpamProxy Encryption unterstützt außerdem den Empfang von Nachrichten über das POP3-Protokoll.
- Port-Umleitung oder Relay-System. NoSpamProxy nimmt statt Ihres bisherigen E-Mail-Servers die Mails auf Port 25 an. Wenn der E-Mail-Server und NoSpamProxy auf dem gleichen System installiert werden, muss der bisherige Port des E-Mail-Servers geändert werden.

HINWEIS: NoSpamProxy kann **nicht** in der Kombination **Domänencontroller + Exchange + NoSpamProxy** auf einem System betrieben werden, da der Betrieb von Exchange auf einem Domänencontroller untersagt wird.

HINWEIS: NoSpamProxy kann auf einem System parallel mit Exchange installiert werden. Diese Kombination ist aber nicht empfohlen, da es auf Grund von doppelten Portbelegungen immer wieder zu Problemen beim Betrieb kommt:

- Port 6060/6061 TCP (interne Kommunikation zwischen den NoSpamProxy-Rollen)
- Port 25 (SMTP, wird ebenfalls vom Exchange verwendet)
- Port 443 (SSL, wird für das Web Portal benötigt, kann aber geändert werden)
- Port 465 TCP (POP3, kein Support für NoSpamProxy Server Protection)

Troubleshooting

TIPP: Wir empfehlen den Einsatz von **Telnet Client** oder **PuTTY** auf allen Servern (zum Testen der Netzwerkkonnektivität).

NoSpamProxy

HINWEIS: Für die Gatewayrolle und die Intranetrolle benötigen Sie einen Microsoft SQL Server. Sie können **entweder** Microsoft SQL Express **oder** Microsoft Server Standard/Enterprise einsetzen.

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.

HINWEIS: Falls Sie NoSpamProxy und Microsoft Exchange auf demselben Server installiert haben, stellen Sie vor Installation oder Aktualisierung des Microsoft .NET-Frameworks sicher, dass die jeweilige Version des Frameworks von Exchange unterstützt wird. Eine Übersicht der unterstützten Versionen bietet die **Exchange-Server-Unterstützbarkeitsmatrix**.

HINWEIS:
Wenn das NoSpamProxy Command Center auf einem Windows Server 2012 R2 verwendet wird, kann es vorkommen dass auf der Startseite der die neuesten Meldungen nicht angezeigt werden. Die Ursache hierfür ist, dass das Betriebssystem keine sichere Verbindung zur Quelle der Meldungen öffnen kann.

Hierfür müssen im Betriebssystem die folgenden beiden TLS Ciphers aktiviert werden:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Starten Sie anschließend das Betriebssystem neu.

Weitere Informationen erhalten Sie in der **Microsoft-Dokumentation**.

- Windows Server 2012 R2 oder neuer (Windows Server 2012 R2 ist zum 31.12.2023 abgekündigt)
- Microsoft SQL Server Standard/Enterprise 2012 Service Pack 4 oder neuer (abgekündigt zum 31.12.2023) **oder** Microsoft SQL Express 2019 (auf Windows Server 2016 oder neuer) beziehungsweise Microsoft SQL Express 2017 (auf Windows Server bis einschließlich 2012 R2)
- Microsoft .NET Framework 4.8
- Microsoft Visual Studio 2010 Tools for Office Runtime

Gatewayrolle

- Funktionierende DNS-Auflösung. Diese wird von NoSpamProxy Protection für die Auflösung von Realtime Blocklists und Spam URL Blocklists genutzt. NoSpamProxy Encryption benötigt eine DNS-Auflösung für die Überprüfung von Zertifikaten (Zugriff auf 'Certificate Revocation Lists' und 'OCSP').
- HTTP- und HTTPS- sowie LDAP-Zugriff auf das Internet. NoSpamProxy Protection benötigt den Zugriff für eine der Realtime Blocklists, die Core Antispam Engine und den integrierten Malware Scanner. NoSpamProxy Encryption verwendet HTTP und HTTPS sowie LDAP für die Überprüfung von Zertifikaten (Zugriff auf 'Certificate Revocation Lists' und 'OCSP').
- Bei Einsatz einer Firewall entsprechende Portfreigaben für alle Ports, die für NoSpamProxy vorgesehenen sind (in der Regel ist dies Port 25).
- TCP-Verbindung über Port 6060 und HTTPS-Verbindung über Port 6061 von der Oberfläche zur Gatewayrolle. Diese Ports werden für den initialen Verbindungsaufbau zwischen Gatewayrollen und der Intranetrolle benötigt. Nachdem alle Gatewayrollen verbunden sind, erfolgt die Kommunikation zu diesen nur noch über die Intranetrolle.
- Optional: Beliebiger, dateibasierter On-Access-Virenscanner.
- Zugriff auf die URL nimbus.bitdefender.net.

HINWEIS: Geben Sie, wenn Sie Ports freigeben, diese sowohl auf der Windows-Firewall wie auch auf Ihrer Perimeter-Firewall frei.

Intranetrolle

- TCP-Verbindung über Port 6060 und HTTPS-Verbindung über Port 6061 von der Oberfläche zur Intranetrolle
- TCP-Verbindung über Port 6060 und HTTPS-Verbindung über Port 6061 von Intranetrolle zur Gatewayrolle
- Optional: TCP-Verbindung zum Domain Controller über LDAP oder Global Catalog
- Optional: TCP-Verbindung zum Web Portal über HTTPS.

NoSpamProxy Command Center

- TCP-Verbindung über Port 6060 und HTTPS-Verbindung über Port 6061 von der Oberfläche zur Intranetrolle

Outlook Add-In

- Outlook 2010 mit Service Pack 2 oder neuer
- Microsoft Visual Studio 2010 Tools for Office Runtime
- Microsoft .NET Framework 4.8
- Zugriff auf die URL nimbus.bitdefender.net.

HINWEIS: Stellen Sie sicher, dass alle von Ihnen eingesetzten Applikationen von Drittanbietern, die eine Verbindung zu NoSpamProxy aufbauen, durch den jeweiligen Herstellersupport abgedeckt sind. Ist dies nicht der Fall, kann das NoSpamProxy-Supportteam keine Supportleistung anbieten.

HINWEIS: Falls Sie NoSpamProxy und Microsoft Exchange auf demselben Server installiert haben, stellen Sie vor Installation oder Aktualisierung des Microsoft .NET-Frameworks sicher, dass die jeweilige Version des Frameworks von Exchange unterstützt wird. Eine Übersicht der unterstützten Versionen bietet die **Exchange-Server-Unterstützbarkeitsmatrix**.

Web Portal

- Windows Server 2012 R2 oder neuer (Windows Server 2012 R2 ist zum 31.12.2023 abgekündigt)
- Microsoft .NET Framework 4.8
- Microsoft SQL Server Standard/Enterprise 2012 Service Pack 4 oder neuer (abgekündigt zum 31.12.2023) **oder** Microsoft SQL Express 2019 (auf Windows Server 2016 oder neuer) oder Microsoft SQL Express 2017 (auf Windows Server bis einschließlich 2012 R2).

> **HINWEIS:** Falls Sie NoSpamProxy und Microsoft Exchange auf demselben Server installiert haben, stellen Sie vor Installation oder Aktualisierung des Microsoft .NET-Frameworks sicher, dass die jeweilige Version des Frameworks von Exchange unterstützt wird. Eine Übersicht der unterstützten Versionen bietet die **Exchange-Server-Unterstützbarkeitsmatrix**.

Vorbereitungen

In Abhängigkeit von der geplanten Installationsumgebung sind unterschiedliche Vorbereitungen notwendig.

- **Portfreigaben auf der Firewall|** Wenn Sie eine Firewall verwenden, muss der für das Web Portal von NoSpamProxy vorgesehene Port freigegeben sein. In der Regel ist dies Port 443.
- **IIS auf einer Gatewayrolle|** Wenn der IIS auf dem gleichen System wie eine der Gatewayrollen installiert ist, deaktivieren Sie die SSL-Loopbackprüfung. Das Verfahren wird in der **Microsoft Knowledge Base** beschrieben.
    - Nutzen Sie die Methode 1, um eine Ausnahme für die Verbindung auf diese Adresse einzurichten.
    - Methode 2 wird nicht empfohlen, da so eine wesentliche Sicherheitsfunktion Ihres Servers deaktiviert würde.
- **Web Portal in der DMZ/auf Computer außerhalb der Domäne|** Wenn das Web Portal auf einem Computer in der DMZ bzw. auf einem Computer außerhalb

der Domäne installiert ist, deaktivieren Sie bitte die UAC-Remote-Restrictions. Das Verfahren wird in der **Microsoft Knowledge Base** beschrieben.

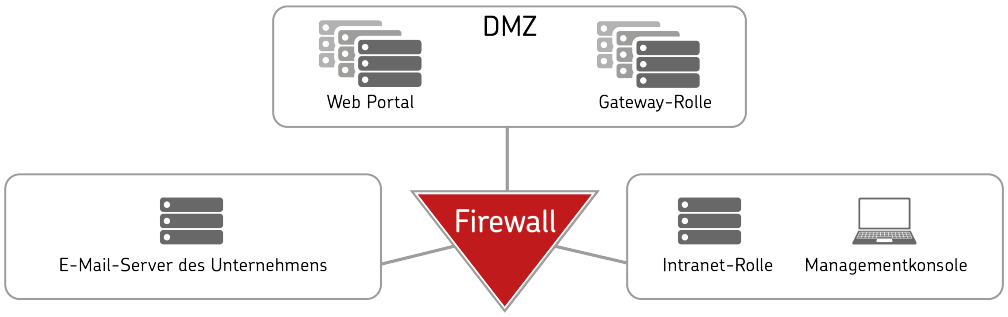
Infrastruktur-Empfehlungen

Verteilung auf unterschiedlichen Servern

Wir empfehlen Ihnen, die beteiligten Komponenten auf unterschiedlichen Servern zu installieren. Dies hat zwei entscheidende Vorteile:

- Sie ermöglichen so eine hohe Verfügbarkeit Ihrer E-Mail-Infrastruktur.
- Sie erhöhen damit die Sicherheit Ihrer E-Mail-Infrastruktur, da Sie die Gatewayrollen und Web-Portale in einer demilitarisierten Zone (DMZ) ansiedeln können.

Eine Verteilung der Komponenten könnte wie folgt aussehen:



HINWEIS: In größeren Umgebungen mit hohem E-Mail-Aufkommen haben Sie die Möglichkeit, in der DMZ mehrere Server mit Gatewayrollen zu installieren. So können Sie ein hochverfügbares System aufbauen.

TIPP: Detaillierte Informationen zur Kommunikation der Komponenten untereinander finden Sie unter **Portbelegung**.

Installation auf einem Server

Sie können alle beteiligten Komponenten auf einem Server installieren. Dies kann für kleine Umgebungen sinnvoll sein.

WARNUNG: Die Installation aller Komponenten auf einem Server wirkt sich unter Umständen negativ auf die Verfügbarkeit und Sicherheit Ihrer E-Mail-Infrastruktur aus.

NoSpamProxy installieren

Vor der Installation

- Schließen Sie vor Beginn der Installation alle Windows-Programme.
- Überlegen Sie sich E-Mail-Adressen für die folgenden Anwendungsfälle (nur bei Neuinstallation):
  - **Benachrichtigungen an externe Empfänger|** Die Adresse, die NoSpamProxy als Absenderadresse nutzt, um E-Mails nach extern zu versenden (beispielsweise non-delivery reports oder PDF-Verschlüsselung)
  - **Benachrichtigungen an interne Empfänger|** Die Adresse, die NoSpamProxy als Absenderadresse nutzt, um E-Mails nach intern zu versenden (beispielsweise Verzögerungsbenachrichtigungen oder Downloadbestätigungen)
  - **Benachrichtigungen an interne Administratoren|** Die Adresse, die zum Empfang von administrativen Benachrichtigungen genutzt wird (beispielsweise Probleme bei der Ausführung von NoSpamProxy oder Large-Files-Freigaben)

Offline-Installation

Informationen zur Installation ohne Zugang zum Internet Sie unter **Offline-Installation**.

Starten der Installation

- Klicken Sie die Setup-Datei von NoSpamProxy. Der Assistent führt Sie durch die Installation.

Installationspfad

WARNUNG: Die Verwendung eines benutzerdefinierten Installationspfads beeinträchtigt unter Umständen den Schutz Ihrer IT-Umgebung vor unauthorisiertem Zugriff und Malware. Wir empfehlen Ihnen dringend, den Standardinstallationspfad zu verwenden.

Installationsarten

Das Setup unterscheidet sich, je nachdem, ob Sie eine Neuinstallation, eine Änderung oder ein Upgrade durchführen wollen:

Installationsart	Definition	Eigenschaften des Setups
Neuinstallation	Es ist aktuell keine NoSpamProxy-Installation installiert.	Sie haben während der Installation die Möglichkeit, einzelne Komponenten für die Installation auszuwählen. Außerdem müssen Sie die Datenbank, den Datenbankserver und den Installationsordner einrichten.
Änderung der Installation	Es ist aktuell eine NoSpamProxy-Installation in der	Sie haben während der Installation die Möglichkeit, einzelne Komponenten zu behalten, zu installieren oder zu entfernen. Außerdem können Sie die Einstellungen

Installationsart	Definition	Eigenschaften des Setups
	gleichen Version wie der des Setups installiert.	für die Datenbank, den Datenbankserver und den Installationsordner anpassen.
Update	Es ist aktuell eine NoSpamProxy-Installation in einer niedrigeren Version als der des Setups installiert.	Sie aktualisieren Ihre NoSpamProxy-Installation. Die bestehenden Einstellungen werden übernommen.

Komponentenauswahl

Hier können Sie entscheiden, welche Rolle(n) auf dem jeweiligen Computer installiert werden sollen.

> **TIPP:** Hinweise zur NoSpamProxy-Infrastruktur finden Sie unter **Infrastruktur-Empfehlungen**.

Über die Komponenten von NoSpamProxy

Intranetrolle

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

Gatewayrolle

Hinter der Gatewayrolle verbirgt sich der eigentliche Kern von NoSpamProxy. NoSpamProxy nimmt die E-Mails auf Port 25 an, prüft diese auf Spam und weist sie gegebenenfalls ab. NoSpamProxy Encryption prüft E-Mails an Unternehmensempfänger auf gültige Signaturen und entschlüsselt sie. E-Mails an externe Empfänger werden, je nach Konfiguration, signiert und verschlüsselt. Es stellt außerdem eine Schnittstelle zu De-Mail, Deutschland-Online-Infrastruktur und POP3- Postfächern bereit.

Web Portal

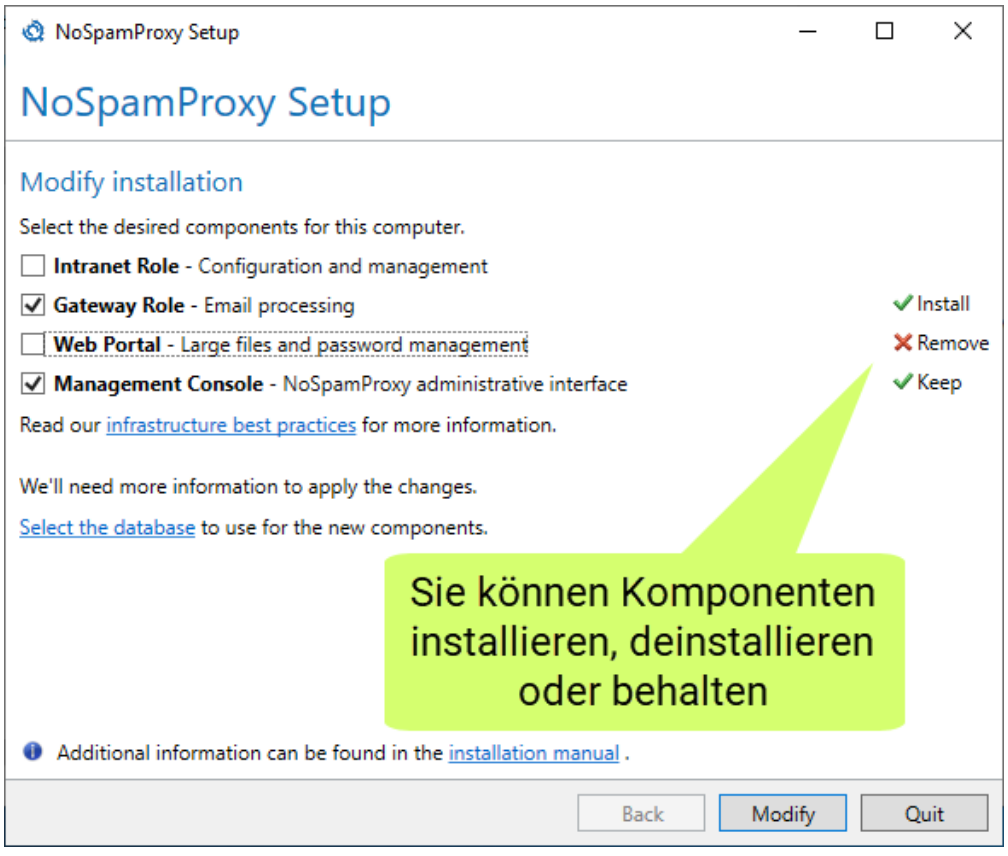
Das Web Portal ermöglicht Benutzern das Hinterlegen von Passwörtern für PDF Mail sowie das Verfassen von Antworten auf PDF Mails. Siehe **Hinweise zur Installation des Web Portals**.

NoSpamProxy Command Center

Das NoSpamProxy Command Center ist die Benutzeroberfläche von NoSpamProxy. Das NCC dient der zentralen Verwaltung und Administration von NoSpamProxy.

NoSpamProxy Web App

Die NoSpamProxy Web App wird als Teil der Intranetrolle mitinstalliert. Die Web App bietet über ein webbasiertes Interface weitere Funktionen wie beispielsweise zusätzliche Suchoptionen für die Nachrichtenverfolgung.



Datenbankkonfiguration

Auswählen der Datenbank

Für den Einsatz von NoSpamProxy benötigen Sie einen Microsoft SQL Server. Sie können **entweder** Microsoft SQL Express **oder** Microsoft Server Standard/Enterprise einsetzen. Siehe **Systemvoraussetzungen**.

> **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.

Anmeldeinformationen

Wir benötigen zwei Arten von Anmeldeinformationen:

Informationen zum Einrichten der Datenbank| Diese Informationen werden ausschließlich während der Installation benötigt, um die Datenbank initial einzurichten.

Informationen für den Zugriff während des Betriebs| Diese Informationen werden benötigt, damit NoSpamProxy während des Betriebs auf die Datenbank zugreifen kann.

HINWEIS: Klicken Sie **Recheck access**, um die Datenbankkonfiguration zu überprüfen, nachdem Sie Änderungen vorgenommen haben.

Nach der Installation

Nach Abschluss der Installation finden Sie im Startmenü einen Eintrag für das NoSpamProxy Command Center, falls Sie dieses installiert haben.

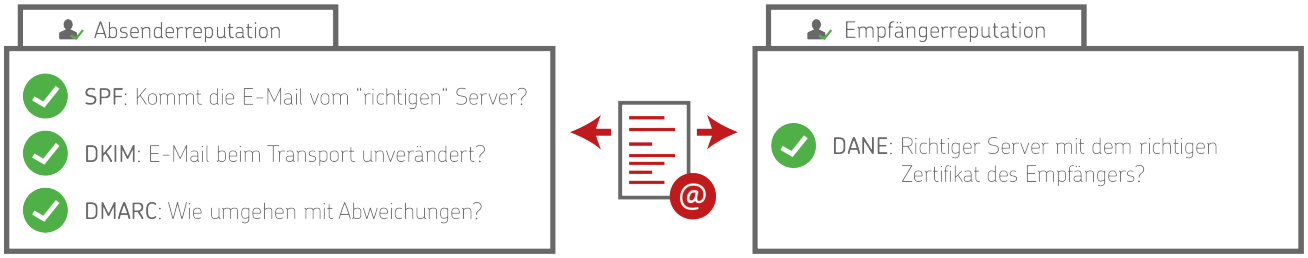
Wenn Sie alle Rollen auf demselben Server installiert haben, erscheint auf der Übersichtsseite der Konfigurationsoberfläche ein Link auf den Konfigurationsassistenten. Über diesen Assistenten können Sie Ihre Lizenz einspielen und die Konfiguration von NoSpamProxy vervollständigen.

Einrichten der DNS-Konfiguration

Die automatische Absenderidentifikation ermöglicht es dem empfangenden Server einer E-Mail, eindeutig festzustellen, ob diese tatsächlich vom angegebenen Absender stammt. Darüber hinaus kann der Server feststellen, ob der einliefernde Server autorisiert ist, im Namen der absendenden Domain E-Mails zuzustellen. Möglich wird dies durch die Verwendung von speziellen Methoden zur Absenderidentifizierung, die als Standardinstrumentarium für E-Mail-Sicherheit immer mehr Verbreitung finden. Die einzelnen Methoden sind unter den Abkürzungen

- SPF (Sender Policy Framework),
- DKIM (DomainKeys Identified Mail) sowie
- DMARC (Domain-based Messaging, Authentication, Reporting and Conformance)

bekannt und bauen aufeinander auf. Mit DANE (DNS-based Authentication of Named Entities) kommt ein Verfahren zur Validierung des Empfängers ergänzend hinzu.



Die entsprechenden Informationen zu SPF, DKIM, DMARC und DANE müssen in der DNS-Konfiguration der jeweiligen Unternehmensdomäne veröffentlicht und damit den externen Kommunikationspartnern zur Verfügung gestellt werden. So wird dem Kommunikationspartner die Möglichkeit gegeben, zweifelsfrei festzustellen, ob die E-Mail tatsächlich vom korrekten Absender kommt. Zudem sinkt auch das Reputationsrisiko für die Unternehmensdomänen.

NoSpamProxy auf einem Domaincontroller

Nach der Installation von NoSpamProxy auf einem Domaincontroller finden Sie die vier Benutzergruppen

- NoSpamProxy Configuration Administrators
- NoSpamProxy Monitoring Administrators
- NoSpamProxy People and Identities Administrators
- NoSpamProxy Disclaimer Administrators

unter **Active Directory > Benutzer und Computer**.

Herstellen der Verbindung zur Intranetrolle

Die Verbindung des NoSpamProxy Command Center zur Intranetrolle steht nach der Installation auf **localhost**.

Bei einer Installation des NCC auf einem anderen Rechner als dem Rechner der Intranetrolle müssen Sie die Verbindung anpassen.

Gehen Sie folgendermaßen vor:

1. Führen Sie einen der beiden Schritte durch:
    - Klicken Sie **NoSpamProxy** und wählen Sie im Menü **Aktion > Server ändern**.
    - Rechtsklicken Sie **NoSpamProxy** und wählen Sie im Kontextmenü **Server ändern**.
2. Geben Sie den Namen des Servers (zum Beispiel **mail.example.com**) und den Port (normalerweise **6060**) ein.
3. Klicken Sie **Speichern und schließen**.

Damit die Änderung wirksam wird, müssen Sie das NoSpamProxy Command Center schließen und neu starten.

> **HINWEIS:** Falls das Gateway in einer DMZ betrieben wird und Sie aus dem LAN über das NoSpamProxy Command Center den Dienst fernsteuern möchten, müssen Sie auf der Firewall lediglich den TCP-Port 6060 und für HTTPS den Port 6061 freischalten. Diese Verbindung ist zertifikatsbasierend verschlüsselt. Weitere Informationen finden Sie unter **Portbelegung**.

Konfigurieren des Zertifikats für die Web App

Damit Benutzer die NoSpamProxy Web App sowie Backend-Dienste sicher nutzen können, wird ein Zertifikat benötigt.

> **HINWEIS:** Nach der Installation ist bereits ein selbstsigniertes Zertifikat hinterlegt, das eine Verbindung zur Web App ermöglicht. Wir raten von der Nutzung dieses Zertifikats ab und empfehlen, zur Optimierung der Sicherheit die Nutzung eines zuvor importierten Zertifikats.

1. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten > NoSpamProxy Web App**.
2. Klicken Sie **Bearbeiten**.
3. Geben Sie unter **DNS-Name** den Hostnamen an, unter dem die Web App erreichbar ist.

4. Geben Sie den genutzten Port an und klicken Sie **Weiter**.

> **HINWEIS:** Standardmäßig wird Port 6061 genutzt. Falls Sie eine HTTPS-Verbindung aufbauen möchten, nutzen Sie Port 443.

5. Konfigurieren Sie das Zertifikat, das Sie zur Absicherung der NoSpamProxy Web App nutzen möchten:
   - **Privates Zertifikat**| NoSpamProxy erstellt sowohl ein privates Zertifikat als auch ein Stammzertifikat. Sie müssen das Stammzertifikat auf allen Computern installieren, von denen aus Sie eine Verbindung zur Web App herstellen möchten.
   - **Existierendes Zertifikat**| Sie nutzen ein existierendes Zertifikat, das Sie zuvor bei einer Zertifikatsstelle erworben und in NoSpamProxy hinterlegt haben.
6. Klicken Sie **Fertigstellen und neu starten**.

Konfigurieren installierter On-Access-Virenscanner

Um (wiederkehrende) Probleme beim Zusammenspiel von installierten On-Access-Virenscannern zu beheben, konfigurieren Sie Ihren Virenscanner so, dass die **Verzeichnisse**

- C:\ProgramData\Net at Work Mail Gateway\Core Antispam Engine

- C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailQueues
- C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailsOnHold

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\enQsig Webportal\

Ansonsten kann es bei einigen Virenscannern vorkommen, dass der Zugriff auf das Web Portal stark verzögert wird und Kommunikationsprobleme auftreten.

Zusätzlich sollte eine Ausnahme auf die **Prozesse**

- amserver.exe sowie
- NoSpamProxy.CoreAntispamEngine.exe

eingestellt werden, falls der On-Access-Virenscanner dies ermöglicht.

TIPP:
Falls Sie den oben beschriebenen Pfad nicht finden, handelt es sich sehr wahrscheinlich um eine ältere NoSpamProxy-Installation, die bereits mehrfach aktualisiert worden ist. Prüfen Sie in diesem Fall bitte zunächst die Datei **C:\ProgramData\Net at Work Mail Gateway\Configuration\Gateway Role.config** und suchen Sie dort nach dem Eintrag **<storageLocation path=**.

Dieser Pfad wird derzeit von der Gatewayrolle benutzt.

Falls Sie den dateibasierten Virenscan in den Regeln aktiviert haben, stellen Sie ebenfalls sicher, dass Ihr Scanner so konfiguriert wird, dass infizierte Dateien und Archive komplett gelöscht oder in Quarantäne verschoben werden. Sollte der Scanner auf **Bereinigen** konfiguriert sein, kann NoSpamProxy oftmals nicht erkennen, dass diese vom installierten Scanner verändert wurden. Somit schlägt der “dateibasierte Virenscan” dann trotz erfolgreicher Erkennung durch NoSpamProxy fehl. Dies tritt insbesondere bei Archiven auf.

Hinterlegen eines TLS-Zertifikats für eingehende Verbindungen

Wenn im Empfangskonnektor eine eigene TLS-Identität genutzt werden soll, muss diese zuerst auf allen Systemen mit NoSpamProxy-Komponenten im Computer-Zertifikatsspeicher hinterlegt werden. Anschließend müssen den folgenden Dienstkonten Leseberechtigungen auf dem privaten Schlüssel eingeräumt werden:

- NT Service\NetatworkMailGatewayGatewayRole
- NT Service\NetatworkMailGatewayManagementService
- NT Service\NetatworkMailGatewayIntranetRole
- NT Service\NetatworkMailGatewayPrivilegedService

Konfigurieren des SSL-Zertifikats für das Web Portal

Um ein Zertifikat zur Absicherung des Web Portals zu hinterlegen, muss dieses zuerst dem Computer-Zertifikatsspeicher hinzugefügt werden. Bei dem Zertifikat kann es sich um

- ein Wildcard-Zertifikat,
- ein SAN-Zertifikat oder um
- ein einzelnes Zertifikat handeln.

Anschließend muss das Zertifikat im Bereich der Bindungen der Default Website für HTTPS ausgewählt werden.

Konfigurieren des Verzeichnisses für Large Files

Um die vollständige Funktionalität des Web Portals – insbesondere für die Large-Files-Funktionalität – zu ermöglichen, müssen die unten genannten Dienstkonten mit den entsprechenden Rechten auf dem für Large Files konfigurierten Verzeichnis ausgestattet sein:

- IS AppPool\enQsigPortal – **Schreiben**
- NT Service\NetatworkMailGatewayFileSynchronizationService – **Ändern**

Einrichten der Mehrfachbelegung von Service-Ports

Wenn Sie einen Port für mehrere Web Services verwenden möchten, müssen Sie einen *Host Header* setzen. Ein Host Header wird auch als *Hostname* bezeichnet. Dieser dient der Unterscheidung unterschiedlicher Services, die über einen gemeinsamen Port beziehungsweise eine gemeinsame IP-Adresse betrieben werden. So ist es möglich, beispielsweise das Web Portal und die Web App über den Port 443 (oder einen anderen Port) zu betreiben.

Das Setzen eines Host Headers ist ausschließlich mit Hilfe des PowerShell-Cmdlets `Set-NspWebApiConfiguration` möglich. Im folgenden finden Sie eine Beschreibung:

Vorgehen

Geben Sie den folgenden Befehl in die Kommandozeile ein:

```
Set-NspWebApiConfiguration -Port <DerVerwendetePort> -DnsName
<DerDNSName> -UseHostHeader true -ShowCertificateSelectorUI
```

Durch das Setzen des Wertes `true` für den Parameter `UseHostHeader` wird die Verwendung des Host Headers konfiguriert. In diesem Beispiel wird durch die Verwendung des Parameters `ShowCertificateSelectorUI` zudem bestimmt, dass ein Windows-Dialog angezeigt wird, mit Hilfe dessen Sie den Thumbprint des Zertifikats angeben können.

> **HINWEIS:** Nach dem Ausführen des Cmdlets müssen Sie das NoSpamProxy Command Center neu starten.

Installation auf einem Cloud-Dienst

Einbinden des TCP Proxy

> **HINWEIS:** Sie müssen über einen gültigen Vertrag über Softwarewartung verfügen, um den TCP Proxy nutzen zu können.

Bei einigen cloudbasierten Systemen – zum Beispiel in Microsoft Azure – kann es vorkommen, dass der Port 25 ausgehend vom Anbieter blockiert wird. Port 25 wird aber zum Versand von E-Mails benötigt, was einen Betrieb von NoSpamProxy auf einem solchen System behindert.

Hierzu bieten wir eine Alternative an, um solche Systeme trotzdem zu nutzen: unseren *TCP Proxy*. Dieses System kann auf unten beschriebene Weise in NoSpamProxy aktiviert werden. Dabei wird jede ausgehende Verbindung an eine routing-fähige IPv4-Adresse auf TCP-Ebene durch den TCP Proxy für NoSpamProxy geroutet. Die E-Mails werden dann vom Server aus über Port 443 an den TCP Proxy gesendet und von dort dann über Port 25 weiter zum Empfängersystem geleitet.

1. Stoppen Sie den Dienst der Gatewayrolle über das NoSpamProxy Command Center oder die Windows-Dienste
2. Öffnen Sie als Administrator einen Texteditor auf dem System, auf dem die Gatewayrolle installiert ist.
3. Öffnen Sie die Konfigurationsdatei **Gateway Role.config** aus dem Verzeichnis **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

4. Suchen Sie in der Datei nach `<smtpServicePointConfiguration>` und ändern/fügen Sie den Wert

```
isProxyTunnelEnabled="true"
proxyTunnelAddress="proxy.nospamproxy.com"
```

als Attribute hinzu. Falls `<smtpServicePointConfiguration` nicht vorhanden ist, suchen Sie nach `<netatwork.nospamproxy.proxyconfiguration` und fügen Sie

```
<smtpServicePointConfiguration
isProxyTunnelEnabled="true"
proxyTunnelAddress="proxy.nospamproxy.com" />
```

direkt unter diesem Wert hinzu.

5. Speichern Sie die Datei ab und schließen Sie den Editor.
6. Legen Sie das **Root CA Zertifikat** im Zertifikatsspeicher von Microsoft im Computerkonto unter **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** auf dem Server mit der Gatewayrolle ab.
7. Bearbeiten Sie im NoSpamProxy Command Center unter **Konfiguration > NoSpamProxy Komponenten > Gatewayrollen** die entsprechende Gatewayrolle und ändern Sie den Wert für **SMTP Servername** auf den Wert `outboundproxy.nospamproxy.com`.

8. Starten Sie den Gatewayrollen-Dienst wieder
9. Öffnen Sie die Datei **Gateway Role.config** erneut und prüfen Sie, ob der Wert beim Start erhalten geblieben ist.

Anpassen des SPF-Eintrags

- Wenn der TCP-Proxy implementiert ist, tritt dieser als absendendes System auf. Somit muss der TCP-Proxy auch mit in Ihrem SPF-Eintrag aufgenommen werden. Wir empfehlen dringend, folgenden Eintrag in Ihren SPF-Eintrag hinzuzufügen:

```
include:_spf.proxy.nospamproxy.com
```

Gegebenenfalls: Anpassen von Office 365

Falls Sie aus Azure heraus E-Mails an eine eigene Office-365-Instanz schicken, bei der ein Konnektor auf die IP-Adressen gebunden ist, aktualisieren Sie bitte die IP-Adressen passend zum Namen outboundproxy.nospamproxy.com. Da bei Office 365 die TLS-Zertifikate gegen die HELO-Domain geprüft werden, ist es nur mit deutlich erhöhtem Aufwand möglich, dies entsprechend umzusetzen. Wir empfehlen daher eine Validierung anhand des Namens.

Gegebenenfalls: Anpassen der Firewall

- Falls Sie ausgehende Verbindungen gezielt blockieren, sollten Sie die Ausnahme für den TCP Proxy so anpassen, dass Verbindungen zum **IP-Netz 193.37.132.0/24** erlaubt sind.

Einrichten einer statischen IP-Adresse

Wenn Sie NoSpamProxy oder Teile davon in einer virtuellen Maschine in einer Microsoft-Azure-Umgebung betreiben möchten, benötigen Sie eine IP-Adresse, die auch nach dem Neustart der Maschine erhalten bleibt. Um dies zu erreichen, müssen Sie eine statische IP-Adresse (Reserved IP Address) einrichten. Ansonsten ist es möglich, dass nach dem Neustart der Maschine eine andere IP-Adresse zugewiesen wird.

HINWEIS: Diese Einstellung nehmen Sie auf dem virtuellen Computer in Microsoft Azure vor, auf dem NoSpamProxy installiert ist.

1. Öffnen Sie die Webseite **portal.azure.com**.
2. Klicken Sie unter **Home > Virtuelle Computer** auf den virtuellen Computer, auf dem NoSpamProxy installiert ist.
3. Gehen Sie zu **Netzwerk > Netzwerkschnittstelle > IP-Konfigurationen** und wählen Sie die für NoSpamProxy relevante Konfiguration.

4. Aktivieren Sie die Option **Öffentliche IP-Adresse** und klicken sie danach **Neu erstellen**.
5. Geben Sie einen Namen ein und wählen Sie die Option **Statisch** aus.
6. Klicken Sie **OK**.

Die IP-Adresse wird nun unter dem angegebenen Namen angezeigt.

> **HINWEIS:** Beachten Sie beim Einrichten einer statischen IP-Adresse die Informationen von der entsprechenden **Seite der Microsoft-Dokumentation**.

Anpassen des Reverse-DNS-Eintrags für den NoSpamProxy-Server

1. Öffnen Sie **portal.azure.com**.
2. Gehen Sie zu **Dashboard > Ressourcengruppen > [DieRessourcengruppeZuDerDerVirtuelleComputerGehoert] > [IhrVirtuellerComputer] > Eigenschaften**.
3. Geben Sie unter **DNS-Namensbezeichnung** einen Namen für die öffentliche IP-Adresse an.
4. Starten Sie die Azure Shell.
5. Geben Sie den folgenden Befehl ein und ersetzen Sie dabei die vorhandenen Platzhalter:

```
az network public-ip update --resource-group
[Ressourcengruppe] --name [NameDerIPAdresse] --
reverse-fqdn [VollstaendigerDNSName]  --dns-name
[DNSName]
```

HINWEIS: Beachten Sie auch die Anweisungen auf der entsprechenden **Seite der Microsoft-Azure-Dokumentation**.

Offline-Installation

Falls Sie die Setup-Datei auf einem Rechner ausführen wollen, der keinen oder nur eingeschränkten Zugang zum Internet hat, gehen Sie folgendermaßen vor:

1. Wechseln Sie zu einem Rechner, der auf das Internet zugreifen kann. Dies kann auch ein Rechner mit Client-Betriebssystem sein.
2. Laden Sie die Setup-Datei auf diesen Rechner herunter oder legen Sie die Datei auf diesem Rechner ab.
3. Öffnen Sie die Kommandozeile und geben Sie den folgenden Befehl ein:

```
NameDerSetupDatei.exe /layout
```

4. Geben Sie den Download-Pfad an.
5. Kopieren Sie nach Beendigung des Downloads den Ordner mit den heruntergeladenen Dateien auf den Rechner, auf dem Sie NoSpamProxy installieren wollen.
6. Führen Sie die Datei Bundle.exe aus.

Portbelegung

Die Komponenten von NoSpamProxy kommunizieren unter Verwendung der folgenden Ports:

Intranetrolle

Eingehend	Ausgehend
NoSpamProxy Command Center: 6060 TCP, 6061 TCP	LDAP-Server: 389/3268 LDAP/GC, 636/3269 LDAPS/GC Web Portal: 443 HTTPS (UDP und TCP) Gatewayrolle: 6060 TCP, 6061 TCP Internet: 443 HTTPS (TCP)

Gatewayrolle

Eingehend	Ausgehend
Intranetrolle: 6060 TCP, 6061 TCP Interner E-Mail-Server: 25 SMTP Externer E-Mail-Server: 25 SMTP	DNS-Server: 53 DNS digiSeal server: 2001 TCP Interner E-Mail-Server: 25 SMTP Externer E-Mail-Server: 25 SMTP Web Portal: 443 HTTPS (UDP und TCP) POP3-Abruf (falls benötigt): 465 TCP Internet: 443 HTTPS (TCP) Internet: 80 HTTP (TCP)

Web Portal

Eingehend	Ausgehend
Intranetrolle: 443 HTTPS (UDP und TCP)	Internet: 443 HTTPS (TCP)

NoSpamProxy Command Center

Eingehend	Ausgehend
n/a	Intranetrolle: 6060 TCP, 6061 TCP

HINWEIS: Port 443 über UDP ist nur erforderlich, wenn QUIC für HTTP/3 verwendet wird.

Update-Hinweise

Allgemeine Informationen

> **HINWEIS:** Weitere Informationen zu Updates auf Version 14 oder höher finden Sie unter **Update auf Version 14**.

Reihenfolge bei der Aktualisierung

1. Aktualisieren Sie die Intranetrolle. Dies kann einige Zeit in Anspruch nehmen. Unter Umständen ist eine temporäre Erhöhung des zugewiesenen RAM-Speichers hilfreich.
2. Aktualisieren Sie die Gatewayrolle(n). Falls Sie mehrere Gatewayrollen einsetzen, aktualisieren Sie diese nacheinander.
3. Aktualisieren Sie das Web Portal.

Falls Gatewayrolle parallel und Intranetrolle auf demselben Rechner installiert sind

- Sie müssen in den meisten Fällen einer Aktualisierung vor und nach der Installation manuelle Schritte durchführen, da sonst der reibungslose Betrieb von NoSpamProxy nicht mehr gewährleistet ist.

> **HINWEIS:** Beachten Sie hierzu die Hinweise unter **Upgrade-Pfade**.

- Kontrollieren Sie nach der Durchführung einer Programmaktualisierung in jedem Fall die Konfiguration von NoSpamProxy. Kontrollieren Sie im Speziellen auch die Lizenz, die auf Übersichtsseite des NoSpamProxy Command Center angezeigt ist.

Offline-Installation

Informationen zur Installation ohne Zugang zum Internet Sie unter **Offline-Installation**.

Informationen zur Installation ohne Zugang zum Internet Sie unter **Offline-Installation**.

Lizenzen

Falls Sie Fragen zu Ihrer Lizenz haben, kontaktieren Sie bitte unser Support-Team unter **info@netatwork.de**.

Für eine schnellstmögliche Bearbeitung Ihrer Anfrage übermitteln Sie uns bitte die folgenden Informationen:

- Die eingesetzte Version von NoSpamProxy
  Die Versionsnummer finden Sie in der Übersicht des NoSpamProxy Command Center in der rechten oberen Ecke.

- Ihre bestehende Kundennummer
  Die Kundennummer finden Sie der Übersichtsseite von NoSpamProxy unter **Lizenz verwalten** oder in Ihrer Lizenzdatei unter **<field name="ContactNumber">C12345</field>**.

Proxyeinstellungen

Die Proxyeinstellungen werden in einer Konfigurationsdatei vorgenommen. Diese Einstellungen werden bei jedem Update überschrieben und müssen im Anschluss erneut angepasst werden. Kopieren Sie sich daher im Vorfeld die entsprechenden Konfigurationsdateien in ein Backup-Verzeichnis, um sie danach wieder verwenden zu können.

HINWEIS: Bei Updates, beispielsweise von Version 13.1 auf Version 13.2, können die Dateien weiterverwendet werden. Bei Updates von Version 13.2 auf Version 14 oder weiteren Updates auf höhere Versionen als der Version 14 müssen die Änderungen auf Basis der neuen Dateien durchgeführt werden.

Templateanpassungen

Wenn Sie ein Update von NoSpamProxy 10.x oder kleiner auf eine neuere Version durchführen, müssen Sie die Templatedateien von NoSpamProxy noch manuell sichern. Diese werden zur Version 10.x bei jedem Update überschrieben und müssen im Vorfeld gesichert werden. Nach dem Update können Sie die Dateien wieder in das

originäre Verzeichnis zurückkopieren. Mit der Version 11.x ist ein Template-Designer in NoSpamProxy integriert. Ab diesem Zeitpunkt ist dieser Schritt nicht mehr notwendig, es sei denn, Sie haben die Texte in den Templates angepasst.

> **HINWEIS:** Bei Updates, beispielsweise von Version 13.1 auf Version 13.2, können die Dateien weiterverwendet werden. Bei Updates von Version 13.2 auf Version 14 oder weiteren Updates auf höhere Versionen als der Version 14 müssen die Änderungen auf Basis der neuen Dateien durchgeführt werden.

Upgrade-Pfade

Je nachdem, von welcher vorherigen Version Sie auf die aktuelle Version von NoSpamProxy aktualisieren, müssen unterschiedliche Schritte durchgeführt werden. Sie benötigen keine neue Lizenzdatei, sofern die Softwarewartung noch gültig ist.

Update von Version 13.2 auf Version 14

Beachten Sie bei Updates auf Version 14 die Hinweise unter **Änderungen und Empfehlungen ab Version 14**.

Update von Version 13.1 auf Version 13.2

Beim Upgrade von der Version 13.1 auf die Version 13.2 bleiben alle Einstellungen und Benutzerinformationen erhalten.

Update von Version 13 auf Version 13.1

Beim Upgrade von der Version 13 auf die Version 13.1 bleiben alle Einstellungen und Benutzerinformationen erhalten.

Upgrades von Version 12.2 auf Version 13

Beim Upgrade von der Version 12.2 auf die Version 13 bleiben alle Einstellungen und Benutzerinformationen erhalten. Stellen Sie sicher, dass das .NET Framework in der Version 4.7.2 installiert ist und die SQL Server Version mindestens 2008 R2, besser 2012 oder neuer entspricht Mit Version 13.0 haben wir die Einbindung der Lizenz von Lizenz-Datei auf Lizenz-Schlüssel umgestellt. Hierzu beachten Sie bitte den Knowledge-Base-Artikel Neue Lizenz installieren.

Upgrades von Version 12.1 auf Version 12.2

Beim Upgrade von der Version 12.1 auf die Version 12.2 bleiben alle Einstellungen und Benutzerinformationen erhalten.

Upgrades von Version 12 auf Version 12.1

Level-of-Trust Hash-Werte werden ab Version 11.1 als SHA-2 anstatt von MD5 geschrieben. Ab der darauf folgenden Version (Version 12.0) soll die Unterstützung zum Auslesen von MD5 wegfallen. Das Upgrade von einer Version vor 11.1 auf eine Version nach 11.1 muss über die Version 11.1 durchgeführt werden und die Version 11.1 muss eine Woche laufen damit alle benötigten Hash-Trusts auf SHA-2 umgeschrieben werden.

Ansonsten bleiben beim Upgrade von der Version 12 auf die Version 12.1 alle Einstellungen und Benutzerinformationen erhalten.

Upgrades von Version 11.1 auf Version 12

Die Version 12 von NoSpamProxy erfordert mindestens einen SQL Server 2008R2 oder neuer. Aus Performance-Gründen wird empfohlen, auf den SQL Server 2016 zu wechseln. Beim Update von der Version 11.1 auf die Version 12 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Upgrades von Version 11 auf Version 11.1

Mit der Version 11.1 wird als SQL Server die Version 2008 vorausgesetzt. Aktualisieren Sie bitte Ihren SQL Server 2005 auf mindestens die Version 2008, bevor Sie das NoSpamProxy Update starten. Beim Upgrade von der Version 11 auf die Version 11.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Upgrades von Version 10.1 auf Version 11

Beim Upgrade von der Version 10.1 auf die Version 11 bleiben während des Upgrades alle Einstellungen und Benutzerinformationen erhalten. Für die Benutzung des NoSpamProxy Disclaimers wird die Gruppe NoSpamProxy Disclaimer Administrators hinzugefügt. Fügen Sie bitte alle Benutzer, die die Vorlagen und Regeln der Disclaimer verwalten sollen, dieser Benutzergruppe hinzu.

Upgrades von Version 10 auf Version 10.1

Beim Upgrade von der Version 10 auf die Version 10.1 bleiben während des Upgrades alle Einstellungen und Benutzerinformationen erhalten. Upgrades von älteren Versionen Für Informationen zu Upgrades von älteren Versionen steht Ihnen unsere Knowledge Base zur Verfügung.

Änderungen und Empfehlungen ab Version 14

> **WARNUNG:** Stellen Sie sicher, dass Sie vor dem Update auf die Version 14 die Version 13.2.21327.1706 installiert haben. Ein Update von einer anderen Version kann zu Problemen führen. Siehe **Software-Archiv**.

Änderungen bei Updates

Veränderte Namen der NoSpamProxy-Dienste

Die NoSpamProxy-Dienste haben neue Namen. Unter Umständen müssen Sie Anpassungen im Monitoring vornehmen. Die folgenden Namen werden ab Version 14 verwendet (die bisherigen Namen stehen in Klammern):

- **NoSpamProxyCoreAntispamEngine**
- **NoSpamProxyGatewayRole** (NetatworkMailGatewayGatewayRole)
- **NoSpamProxyIdentityService** (-)
- **NoSpamProxyIntranetRole** (NetatworkMailGatewayIntranetRole)
- **NoSpamProxyLargeFileSynchronization** (NetatworkMailGatewayFileSynchronizationService)
- **NoSpamProxyManagementService** (NetatworkMailGatewayManagementService)

- **NoSpamProxyMessageTrackingService** (-)
- **NoSpamProxyPrivilegedService** (NetatworkMailGatewayPrivilegedService)
- **NoSpamProxyWebApp** (NoSpamProxyIntranetRoleWebApp)

Veränderte Namen der NoSpamProxy-Prozesse

Die NoSpamProxy-Prozesse haben neue Namen. Nehmen Sie gegebenenfalls Anpassungen des Monitorings, der Windows Firewall sowie bestehender lokaler Virenscanner vor. Die folgenden Namen werden ab Version 14 verwendet (die bisherigen Namen stehen in Klammern):

- **NoSpamProxy.CoreAntispamEngine**
- **NoSpamProxy.IntranetRole** (NetatworkMailGatewayIntranetRole)
- **NoSpamProxyFileSynchronizationService** (NoSpamProxyFileSynchronizationService)
- **NoSpamProxy.GatewayRole** (NetatworkMailGatewayGatewayRole)
- **NoSpamProxy.ManagementService** (NetatworkMailGatewayManagementService)
- **NoSpamProxy.MimeDetection** (Netatwork.NoSpamProxy.Mime.Detection.External)
- **NoSpamProxy.PrivilegedService** (NetatworkMailGatewayPrivilegedService)
- **NoSpamProxy.WebAppHostingService** (NoSpamProxy.WebAppHostingService)

Zahlreiche Änderungen bezüglich der Datenbankstruktur

Die Veränderungen der Datenbankstruktur machen die Anpassung bestehender PowerShell-Skripte sowie SIEM-Systeme (beispielsweise Splunk) notwendig.

Aktion CSA Whitelist ist jetzt Aktion CSA Certified IP List

Die Aktion **CSA Whitelist** ist nun ein Filter und heißt **CSA Certified IP List**.

Die NoSpamProxy-Managementkonsole heißt jetzt NoSpamProxy Command Center

Die NoSpamProxy-Managementkonsole/NoSpamProxy Management Console wurde in NoSpamProxy Command Center umbenannt und ist kein MMC-Snap-in mehr. Etwaige Konfigurationen (etwa wenn die MMC bisher remote installiert wurde) gehen beim Upgrade verloren und müssen in der neuen Anwendung neu konfiguriert werden.

Neuer Ordner für das NoSpamProxy Command Center

Das NoSpamProxy Command Center erstellt einen Ordner sowie Dateien im Benutzerprofil unter **AppData\Roaming\NoSpamProxy**. Hier wird die Konfiguration des NoSpamProxy Command Center gespeichert.

Neue Netzwerkadresse zum Herunterladen von AV-Mustern

Es wird eine neue Netzwerkadresse zum Herunterladen von AV-Mustern verwendet: https://av-patterns.nospamproxy.com/

Änderungen bei Neuinstallation

Veränderter Installationspfad

Der Installationspfad lautet bei Neuinstallationen **C:\Programme\NoSpamProxy** (vormals C:\Program Files\Net at Work Mail Gateway).

> **HINWEIS:** Bei Updates bleibt der bisherige Pfad unverändert.

Veränderte Datenbanknamen

Die Namen der verwendeten Datenbanken lauten bei Neuinstallationen wie folgt (die bisherigen Namen stehen in Klammern):

- **NoSpamProxyGatewayRole** (NoSpamProxyDB)
- **NoSpamProxyIntranetRole** (NoSpamProxyAddressSynchronization)
- **NoSpamProxyWebPortal** (enQsigPortal)

> **HINWEIS:** Bei Updates werden die bisherigen Namen beibehalten.

NoSpamProxy Web App

Während des Setups wird die NoSpamProxy Web App als Teil der Intranetrolle mitinstalliert.

Empfehlungen

- Wir empfehlen das Hinzufügen des Filters **32Guards** zu allen ein- und ausgehenden Regeln.
- Wir empfehlen das Hinzufügen der Aktion **32Guards** zu allen ein- und ausgehenden Regeln.

Hinweise

HINWEIS: Bei Updates auf die Version 14 ist es möglich, dass die Fehlermeldung **Failed to compile the template 'C:\ProgramData\Net at Work Mail Gateway\Gateway\Templates\HddStressLevel.cshtml'** angezeigt wird. Sie können diese Fehlermeldung ignorieren.

HINWEIS: Bei Updates auf die Version 14 müssen Sie die Verbindung zwischen NoSpamProxy Command Center und Intranetrolle neu konfigurieren, falls sich diese auf unterschiedlichen Rechnern befinden.

HINWEIS:
Wenn in Version 13.2 ein Microsoft-365-Server als E-Mail-Server des Unternehmens konfiguriert ist, wird nach dem Update ein eingehender Sendekonnektor mit Kosten von 50 angelegt. Dieser Konnektor kann nicht entfernt werden. Bei hybriden Szenarien kann sich dies auf das E-Mail-Routing auswirken, da ein normaler Konnektor höhere Kosten verursacht.

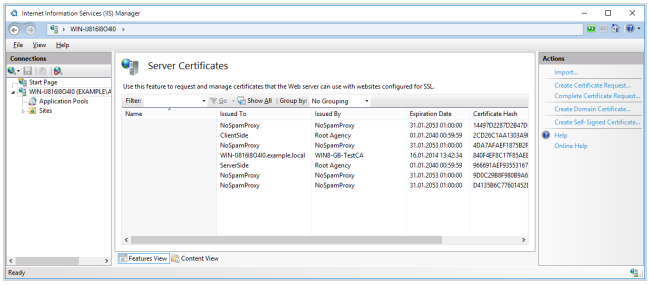
Um Probleme zu umgehen,

- ändern Sie die Kosten des normalen Konnektors **vor dem Update** auf einen Wert unter 50 oder
- passen Sie die Kosten des neu angelegten Konnektors **nach dem Update** umgehend an. Beachten Sie, dass der E-Mail-Verkehr möglicherweise unterbrochen wird.

Hinweise zur Installation des Web Portals

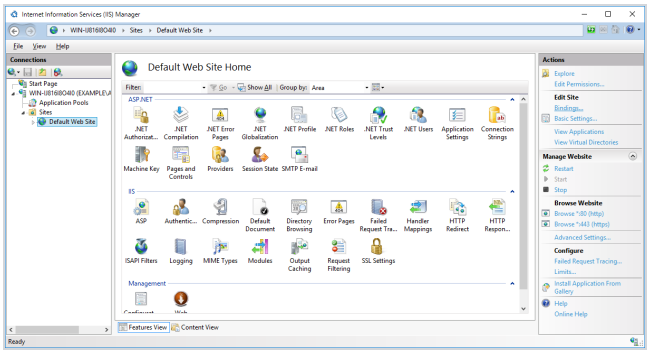
Installation eines SSL-Zertifikats im IIS

1. Starten Sie den **Information Services (IIS) Manager**.
2. Doppelklicken Sie **Server Certificates**. Es öffnet sich die Liste der Server-Zertifikate. Kontrollieren Sie, ob Ihr eigenes Zertifikat für den SSL-Zugang angezeigt wird. Die Server-Zertifikate müssen im Zertifikatsspeicher des lokalen Computer-Kontos hinterlegt sein und liegen unter **Persönliche Zertifikate/Personal**. Alle für SSL nutzbaren Zertifikate werden in der Liste **Server Certificates** des IIS-Managers aufgeführt.

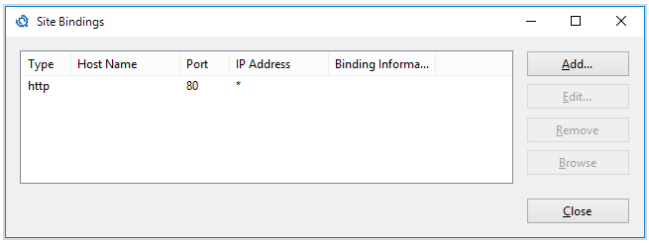


HINWEIS: Stellen Sie sicher, dass das verwendete SSL-Zertifikat unter anderem den exakten FQDN enthält, den Sie für den Aufruf des Web Portals verwenden. Wenn Sie das Web Portal zum Beispiel unter Verwendung der URL **https://portal.example.com/ enqsig** betreiben wollen, muss der Name **portal.example.com** als Name im SSL-Zertifikat auftauchen. Des Weiteren muss sichergestellt sein, dass der Aussteller dieses Zertifikats auf dem Server der Intranetrolle als vertrauenswürdige Stammzertifizierungsstelle eingetragen ist. Die Liste der vertrauenswürdigen Stammzertifizierungsstellen können sie im Zertifikatsspeicher des lokalen Computerkontos einsehen. Öffnen Sie auf dem Server der Intranetrolle den Internet Explorer und geben die URL des Webportals ein, in unserem Beispiel **https://portal.example.com/enqsig**. Die Seite muss sich ohne Fehlermeldungen öffnen. Wenn das der Fall ist, kann die Verbindung zum Webportal in der Intranetrolle ebenfalls erfolgreich hinzugefügt werden.

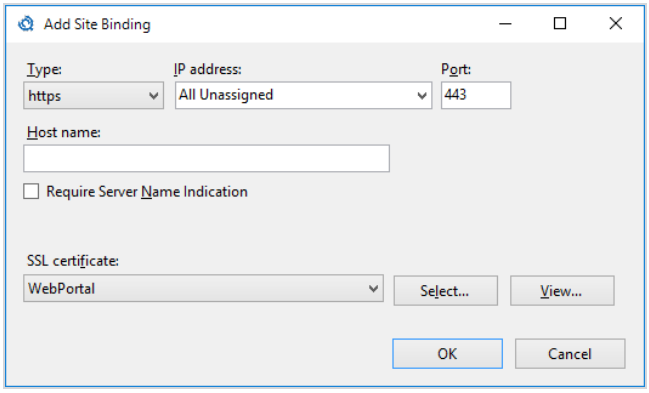
3. Wählen Sie unter **Sites** die Webseite, in die das Webportal installiert wurde. Bei einer Standardinstallation heißt sie Default Web Site.



4. Rechtsklicken Sie **Edit Bindings...** oder unter **Actions** die Option **Bindings...**.
5. Klicken Sie **Add...**.

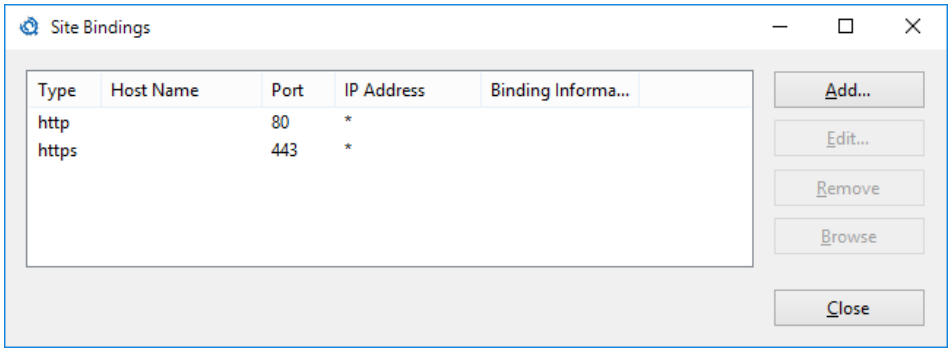


6. Wählen Sie gegebenenfalls eine bestimmte IP-Adresse, den Port 443 und das zuvor kontrollierte SSL-Zertifikat.



Nach Abschluss des Dialogs erscheint die neue Bindung in der Liste aller Bindungen

der Website.

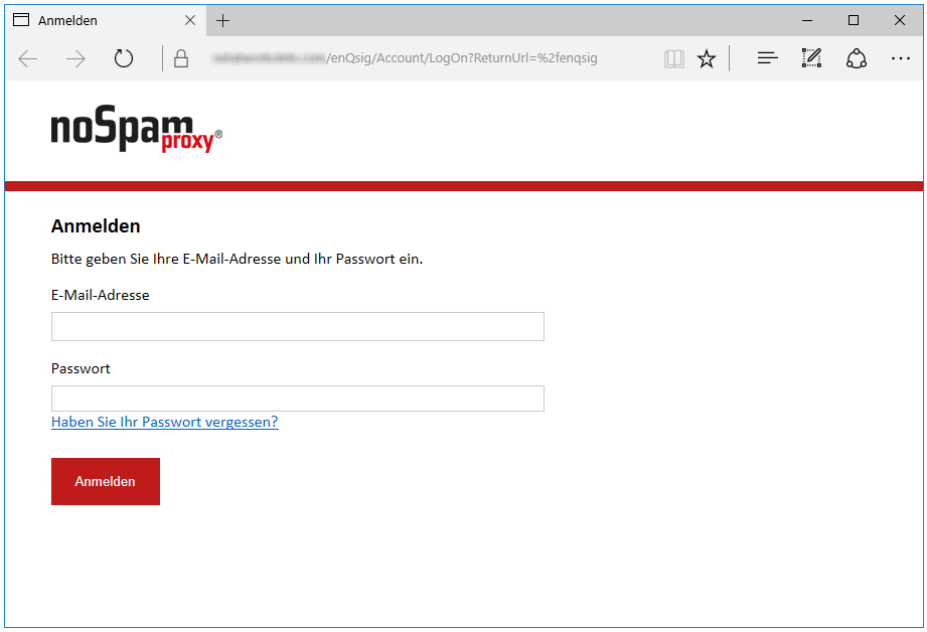


Nach der Installation

Aufrufen des Webportals

Nach Abschluss der Installation können Sie die Webseite des Webportals über die bei der Installation angegebene Adresse aufrufen. Bei einer Standardinstallation ist diese **https://<Rechnername>/enqsig**.

Sollte die Seite nicht aufrufbar sein, überprüfen Sie bitte die Konfiguration des Internet Information Servers. Schauen Sie danach in das Kapitel Fehlerbehandlung. Bei erfolgreicher Installation erscheint die Anmeldeseite des Webportals.



Verbinden des Webportals mit der Intranetrolle

1. Öffnen Sie die Verwaltungsoberfläche von NoSpamProxy.
2. Gehen Sie zu **Konfiguration > NoSpamProxy-Komponenten > Webportal**.
3. Markieren Sie das entsprechende Webportal und klicken Sie **Bearbeiten**.
4. Konfigurieren Sie die Verbindung.

Upgrades

Allgemeine Informationen

Wenn Sie ein Update von einer vorherigen Version des Web Portals durchführen, beachten Sie die folgenden Hinweise.

- Sie müssen in den meisten Fällen einer Aktualisierung vor und nach der Installation manuelle Schritte durchführen, da sonst der reibungslose Betrieb des Webportals nicht mehr gewährleistet ist. Beachten Sie dazu die Hinweise unter Upgrade-Pfade. Die Abschnitte sind kumulativ, das heißt, dass Sie nacheinander die Abschnitte von Ihrer derzeit installierten Version bis zur aktuellen Version beachten müssen.
- Kontrollieren Sie nach der Durchführung einer Programmaktualisierung in jedem Fall die Konfiguration Ihres Webportals.

Updates von Version 13.1 auf Version 13.2

Beim Update von der Version 13.1 auf die Version 13.2 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 13 auf Version 13.1

Beim Update von der Version 13 auf die Version 13.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 12.2 auf Version 13

Beim Update von der Version 12.2 auf die Version 13 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 12.1 auf Version 12.2

Beim Update von der Version 12.1 auf die Version 12.2 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 12 auf Version 12.1

Beim Update von der Version 11.1 auf die Version 12 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 11.1 auf Version 12

Beim Update von der Version 11.1 auf die Version 12 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 11 auf Version 11.1

Mit der Version 11.1 wird als SQL Server die Version 2008 vorausgesetzt. Aktualisieren Sie bitte Ihren SQL Server 2005 auf mindestens die Version 2008, bevor Sie das NoSpamProxy Update starten. Beim Update von der Version 11 auf die Version 11.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 10.1 auf Version 11

Beim Update von der Version 10.1 auf die Version 11 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 10 auf Version 10.1

Beim Update von der Version 10 auf die Version 10.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Fehlerbehandlung

Anmeldeseite nicht erreichbar - Fehler 500.21

Falls die Anmeldeseite nicht angezeigt wird, sondern stattdessen der HTTP Fehler 500.2,1 ist wahrscheinlich Microsoft .NET Framework 4.8 im IIS nicht richtig installiert oder registriert.

> **HINWEIS:** Bevor Sie das Microsoft .NET Framework 4.8 auf Ihrem Internet Server neu registrieren, überprüfen Sie bitte, ob das Framework mit eventuellen anderen Internetseiten, die über diesen Server bereitgestellt werden, kompatibel ist. Sichern Sie Ihr System und speziell die IIS-Konfiguration, bevor Sie fortfahren.

> **HINWEIS:** Falls Sie NoSpamProxy und Microsoft Exchange auf demselben Server installiert haben, stellen Sie vor Installation oder Aktualisierung des Microsoft .NET-Frameworks sicher, dass die jeweilige Version des Frameworks von Exchange unterstützt wird. Eine Übersicht der unterstützten Versionen bietet die **Exchange-Server-Unterstützbarkeitsmatrix**.

- Führen Sie eine erneute Registrierung des ASP.NET-Frameworks mit dem folgenden Befehl durch:

```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_
regiis.exe -i
```

Anzeige des Zertifikatsspeichers des lokalen Computers

Um die Zertifikate des lokalen Computers anzuzeigen, gehen Sie folgendermaßen vor:

1. Starten Sie eine neue MMC-Konsole (**Start > Ausführen > mmc.exe**).
2. Gehen Sie zu **Datei/File** und klicken Sie **Snap-In hinzufügen/entfernen/Add/Remove Snap-in**.
3. Wählen Sie das **Zertifikate/Certificates** Snap-In aus und klicken Sie **Hinzufügen/Add**. Es erscheint der Konfigurationsassistent für das Snap-In **Zertifikate**.
4. Gehen Sie zu **Computer Konto/Computer account**, und danach zu **Lokaler Computer/Local computer**.
5. Klicken Sie **Beenden/Finish**.
6. Klicken Sie **OK**.
7. Klicken Sie **Zertifikate (Lokaler Computer)/Certificates (Local Computer)**, um die Zertifikatsspeicher für den Computer anzuzeigen.

Hilfe und Unterstützung

Knowledge Base

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

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