



## Installation Manual

Version 14

## Legal information

All rights reserved. This document and the applications described therein are copyrighted products of Net at Work GmbH, Paderborn, Federal Republic of Germany. This document is subject to change without notice. The information contained in this document does not constitute an assumption of warranty or liability on the part of Net at Work GmbH. The partial or complete reproduction is only permitted with the written permission of Net at Work GmbH.

Copyright © 2023 Net at Work GmbH

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

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® and Azure® are registered trademarks of Microsoft Corporation. NoSpamProxy® and 32Guards® are registered trademarks of Net at Work GmbH. All other trademarks used belong to the respective manufacturers or owners.

**THIS DOCUMENT WAS LAST EDITED ON NOVEMBER 27, 2023.**

# Content

<b>System requirements</b> .....	<b>1</b>
<b>Infrastructure recommendations</b> .....	<b>9</b>
<b>Installing NoSpamProxy</b> .....	<b>11</b>
Offline installation .....	11
<b>Component selection</b> .....	<b>14</b>
<b>Database configuration</b> .....	<b>16</b>
<b>After the installation</b> .....	<b>17</b>
<b>Installing NoSpamProxy on a cloud service</b> .....	<b>26</b>
<b>Offline installation</b> .....	<b>32</b>
<b>Port allocation</b> .....	<b>33</b>
<b>Update recommendations</b> .....	<b>35</b>
<b>Changes and recommendations as of version 14</b> .....	<b>41</b>
<b>Notes on the installation of the Web Portal</b> .....	<b>47</b>
<b>Help and support</b> .....	<b>57</b>

# System requirements

## **|** General requirements

### **Hardware**

- Dedicated email server (cloud-based or on-premises)
- 4GB RAM Main memory
- 2 CPU cores (virtualized or physical)
- Sufficient storage space. The size required depends on the number of emails received and on the modules used. Contact our support team for assistance with planning.

### **Communication**

- Communication via the SMTP protocol for inbound and outbound emails. NoSpamProxy Encryption also supports the receipt of messages via the POP3 protocol.
- Port redirection or relay system. NoSpamProxy accepts the emails on port 25 instead of your previous email server. If the email server and NoSpamProxy are installed on the same system, the previous email server port must be redirected.



**NOTE:** NoSpamProxy **cannot** be operated in the combination **Domain Controller + Exchange + NoSpamProxy** on a single system, because the operation of Exchange on a domain controller is prohibited.



**NOTE:** NoSpamProxy can be installed on a system in parallel with Exchange. However, this combination is not recommended, since problems are often encountered during operation due to double port assignments:

- Port 6060/6061 TCP (internal communication between the NoSpamProxy roles)
- Port 25 (SMTP, also used by Exchange)
- Port 443 (SSL, is required for the Web Portal, but can be changed)
- Port 465 TCP (POP3, no support for NoSpamProxy Server Protection)

## Troubleshooting



**TIP:** We recommend using Telnet Client or PuTTY on all servers (to test network connectivity).

## NoSpamProxy



**NOTE:** For the gateway role and the intranet role, you need a Microsoft SQL Server. You can use **either** Microsoft SQL Express **or** Microsoft Server Standard/Enterprise.



**NOTE:** If you use Microsoft SQL Server Express and update to version 14 or higher of NoSpamProxy Server, the utilisation of the database used must not exceed 70 percent (7 GB).



**NOTE:** If you have installed NoSpamProxy and Microsoft Exchange on the same server, before installing or upgrading the Microsoft .NET framework, make sure that the appropriate version of the framework is supported by Exchange. For an overview of supported versions, see the **Exchange Server Supportability Matrix**.

**NOTE:**

If the NoSpamProxy Command Center is used on a Windows Server 2012 R2, it can happen that the latest messages are not displayed on the start page. This is because the operating system cannot open a secure connection to the source of the messages.

For this, the following two TLS ciphers must be activated in the operating system:

- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Then restart the operating system.

For more information, see the [Microsoft documentation](#).

- Windows Server 2012 R2 or later (Windows Server 2012 R2 is discontinued as of December 31, 2023)
- Microsoft SQL Server Standard/Enterprise 2012 Service Pack 4 or later (discontinued as of December 31, 2023) **or** Microsoft SQL Express 2019 (on Windows Server 2016 or newer) or Microsoft SQL Express 2017 (on Windows Server up to and including 2012 R2)
- Microsoft .NET Framework 4.8
- Microsoft Visual Studio 2010 Tools for Office Runtime

## Gateway Role

- Working DNS resolution. This is used by NoSpamProxy Protection for the resolution of real-time blocklists and spam URL blocklists. NoSpamProxy Encryption requires DNS resolution for checking certificates (access to 'Certificate Revocation Lists' and 'OCSP').
- HTTP and HTTPS and LDAP access to the Internet. NoSpamProxy Protection requires access for one of the real-time blocklists, the Core Antispam Engine and the Integrated Malware Scanner. NoSpamProxy Encryption uses HTTP and HTTPS as well as LDAP to check certificates (access to 'Certificate Revocation Lists' and 'OCSP').
- If you are using a firewall, the ports provided for NoSpamProxy must be released (usually port 25).
- TCP connection via port 6060 and HTTPS connection via port 6061 from the interface to the Gateway Role. These ports are required for the initial connection between Gateway Roles and the Intranet Role. After all Gateway Roles are connected, communication to them is carried out solely via the Intranet Role.
- Optional: Any file-based on-access virus scanner
- Access the URL [nimbus.bitdefender.net](http://nimbus.bitdefender.net).



**NOTE:** When you share ports, share them on both Windows Firewall and your perimeter firewall.

## Intranet Role

- TCP connection via port 6060 and HTTPS connection via port 6061 from the interface to the Gateway Role.
- TCP connection via port 6060 and HTTPS connection via port 6061 from the Intranet Role to the Gateway Role.
- Optional: TCP connection to the domain controller via LDAP or Global Catalog
- Optional: TCP connection to the Web Portal via HTTPS.

## NoSpamProxy Command Center

- TCP connection via port 6060 and HTTPS connection via port 6061 from the interface to the Gateway Role.

## ■ Outlook Add-in

- Outlook 2010 with Service Pack 2 or later
- Microsoft Visual Studio 2010 Tools for Office Runtime
- Microsoft .NET Framework 4.8
- Access to the URL [nimbus.bitdefender.net](http://nimbus.bitdefender.net).



**NOTE:** Make sure that all third-party applications you use that connect to NoSpamProxy are covered by the respective manufacturer support. If this is not the case, the NoSpamProxy support team cannot provide support services.



**NOTE:** If you have installed NoSpamProxy and Microsoft Exchange on the same server, before installing or upgrading the Microsoft .NET framework, make sure that the appropriate version of the framework is supported by Exchange. For an overview of supported versions, see the [Exchange Server Supportability Matrix](#).

## Web Portal

- Windows Server 2012 R2 or later (Windows Server 2012 R2 is discontinued as of 31.12.2023)
- Microsoft .NET Framework 4.8
- Microsoft SQL Server Standard/Enterprise 2012 Service Pack 4 or later (discontinued as of December 31, 2023) **or** Microsoft SQL Express 2019 (on Windows Server 2016 or newer) or Microsoft SQL Express 2017 (on Windows Server up to and including 2012 R2)



**NOTE:** If you have installed NoSpamProxy and Microsoft Exchange on the same server, before installing or upgrading the Microsoft .NET framework, make sure that the appropriate version of the framework is supported by Exchange. For an overview of supported versions, see the [Exchange Server Supportability Matrix](#).

## Preparations

Depending on the planned installation environment, different preparations are necessary.

- **Open ports for the firewall**| If you use a firewall, the port intended for the NoSpamProxy Web Portal must be open. Usually this is port 443.
- **IIS on a Gateway Role**| If the IIS are installed on the same system as one of the Gateway Roles, disable SSL loopback checking. The procedure is described in the [Microsoft Knowledge Base](#).
  - Use method 1 to set up an exception for the connection to this address.
  - Method 2 is not recommended as it would disable an essential security feature of your server.
- **Web Portal in the DMZ/on computers outside the domain**| If the Web Portal is installed on a computer in the DMZ or on a computer outside the domain, please disable the UAC remote restrictions. The procedure is described in the [Microsoft Knowledge Base](#).

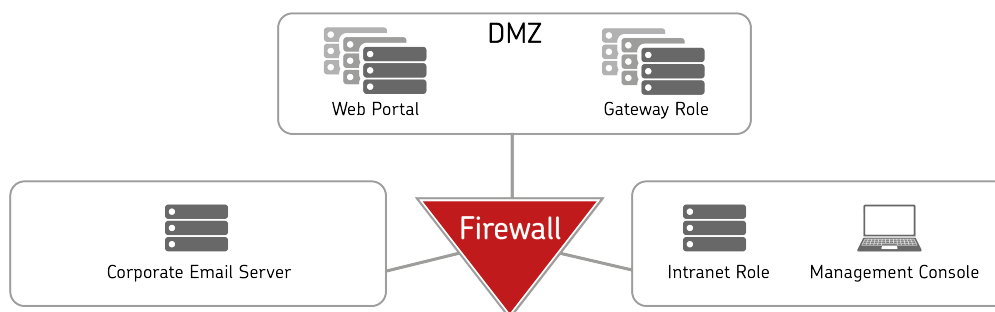
# Infrastructure recommendations

## Installation of the roles on different servers

We recommend that you install the components involved on different servers. This has two decisive advantages:

- Enabling high availability of your email infrastructure.
- You thus increase the security of your email infrastructure, as you can locate the Gateway Roles and web portals in a demilitarised zone (DMZ).

A distribution of the components could look as follows:



**NOTE:** In larger environments with high email volumes, you have the option of installing several servers with gateway roles in the DMZ. This way you can build a highly available system.



**TIP:** Detailed information on the communication between the components can be found under **Port allocation**.

## **I** Installation on a single server

You can install all components involved on one server. This can be useful for small environments.



**WARNING:** The installation of all components on a single server may have a negative effect on the availability and security of your email infrastructure.

# Installing NoSpamProxy

## I Before installation

- Close all Windows programs before starting the installation.
- Consider email addresses for the following use cases (only for new installations):
  - **Notifications to external recipients**| The address that NoSpamProxy uses as the sender address to send emails externally (for example, non-delivery reports or PDF encryption).
  - **Notifications to internal recipients**| The address that NoSpamProxy uses as the sender address to send emails to internally (for example, delay notifications or download confirmations).
  - **Notifications to internal administrators**| The address used to receive administrative notifications (for example, problems running NoSpamProxy or Large Files shares).

## I Offline installation

For information on installation without access to the Internet, see **Offline installation.**

## Starting the installation

- Click the setup file of NoSpamProxy. The wizard guides you through the installation.

## Installation path



**WARNING:** Using a custom installation path may compromise the protection of your IT environment from unauthorised access and malware. We strongly recommend that you use the default installation path.

## Installation types

The setup differs depending on whether you want to perform a new installation, a change or an upgrade:

Installation type	Definition	Properties of the setup
New installation	NoSpamProxy is currently not installed.	During installation, you have the option of selecting individual components for installation. You also need to set up the database, the database server and the installation folder.
Changing the installation	A NoSpamProxy installation in the same version as that of the setup is currently	During installation, you have the option to keep, install or remove individual components. You can also adjust the settings for the database, the database server and the installation folder.

Installation type	Definition	Properties of the setup
	installed.	
Update	A NoSpamProxy installation in a lower version than that of the setup is currently installed.	You update your NoSpamProxy installation. The existing settings are adopted.

# Component selection

Here you determine which role(s) will be installed on the respective computer.



**TIP:** Information on the NoSpamProxy infrastructure can be found at [Infrastructure recommendations](#).

## I About the components of NoSpamProxy

### Intranet Role

The Intranet Role contains the entire configuration of NoSpamProxy and manages the cryptographic keys. This role also synchronizes user data from the Active Directory or another directory service, such as Lotus Domino. The Intranet Role is installed only once. As the name suggests, the Intranet Role is typically installed on the Intranet of your company..

### Gateway Role

The Gateway Role is the actual core of NoSpamProxy. NoSpamProxy accepts the emails on port 25, checks them for spam and rejects them if necessary.

NoSpamProxy Encryption checks emails to local recipients for valid signatures and decrypts them. Emails to external recipients are signed and encrypted, depending on the configuration. It also provides an interface to De-Mail, Deutschland-Online-Infrastruktur and POP3 mailboxes.

## Web Portal

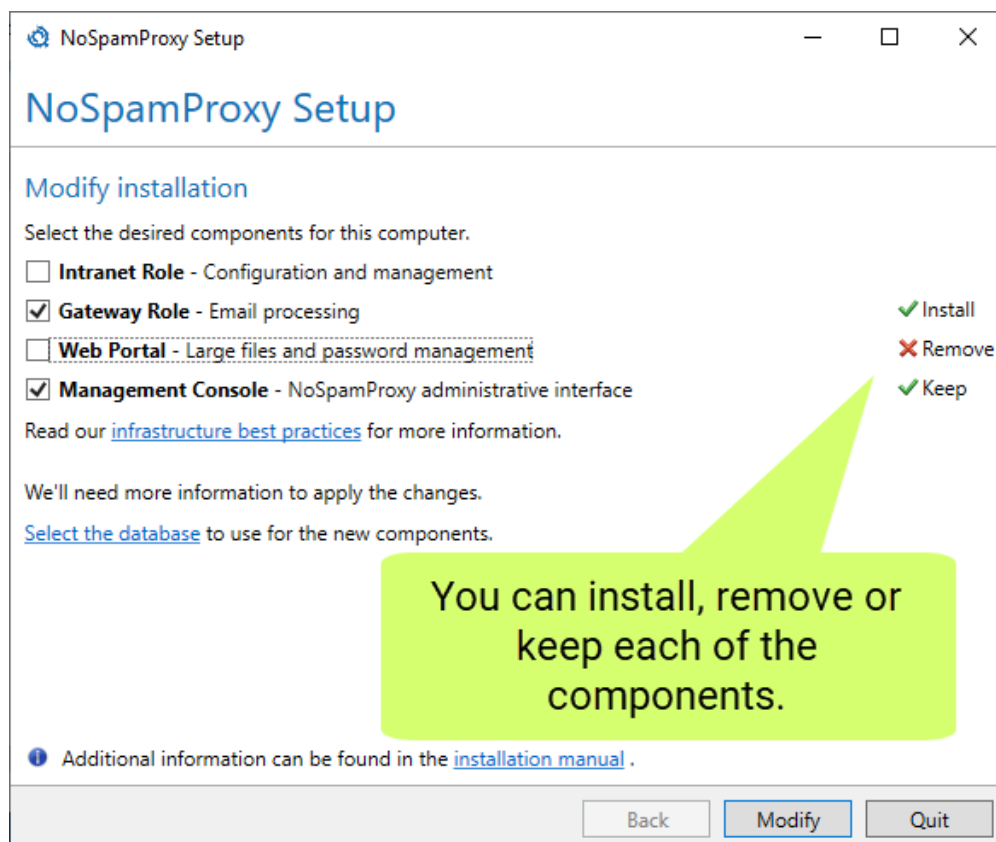
The Web Portal allows users to store passwords for PDF mail and to write replies to PDF mails. See [Notes on the installation of the Web Portal](#).

## NoSpamProxy Command Center

The NoSpamProxy Command Center is the user interface of NoSpamProxy. The NCC is used for the central management and administration of NoSpamProxy.

## NoSpamProxy Web App

During setup, the NoSpamProxy Web App is installed as part of the Intranet Role. The Web App offers further functions via a web-based interface, such as additional search options for message tracking. .



# Database configuration

## I Selecting the database

You need a Microsoft SQL Server to use NoSpamProxy. You can use **either** Microsoft SQL Express **or** Microsoft Server Standard/Enterprise. See **System requirements**.



**NOTE:** If you use Microsoft SQL Server Express and update to version 14 or higher of NoSpamProxy Server, the utilisation of the database used must not exceed 70 percent (7 GB).

## I Login credentials

We require two types of credentials:

**Information for setting up the database**| This information is only required during installation to initially set up the database.

**Information for access during operation**| This information is needed so that NoSpamProxy can access the database during operation.



**NOTE:** Click **Recheck access** to check the database configuration after you have made changes.

# After the installation

After completing the installation, you will find an entry for the NoSpamProxy Command Center in the start menu, if you have installed it.

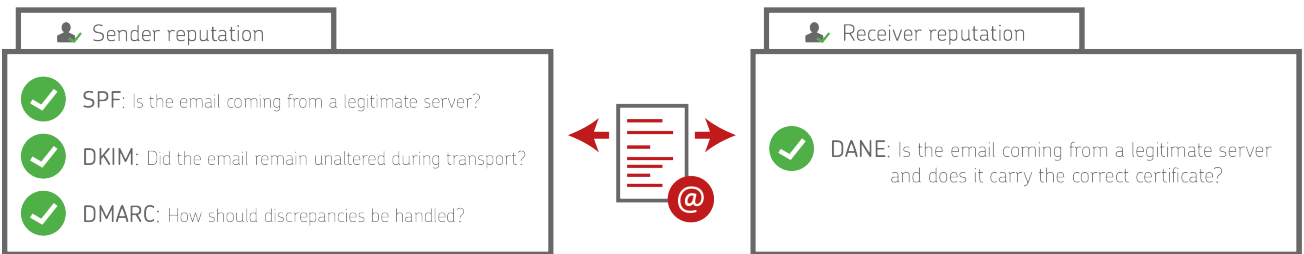
If you have installed all roles on the same server, a link to the configuration wizard appears on the overview page of the configuration interface. You can use this wizard to import your license and complete the configuration of NoSpamProxy.

## I Setting up the DNS configuration

Automatic sender identification enables the receiving server of an email to clearly determine whether it actually originates from the specified sender. In addition, the server can determine whether the submitting server is authorised to deliver emails on behalf of the sending domain. This is made possible by the use of special methods for sender identification, which are becoming more and more widespread as standard tools for email security. The individual methods are described under the abbreviations

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

and build on each other. With DANE (DNS-based Authentication of Named Entities), a procedure for validating the recipient is added.



The corresponding information on SPF, DKIM, DMARC and DANE must be published in the DNS configuration of the respective company domain and thus made available to the external communication partners. In this way, the communication partner is given the opportunity to establish beyond doubt whether the email actually was actually sent from the sender displayed. In addition, the reputational risk for the corporate domains also decreases.

## I NoSpamProxy on a domain controller

After installing NoSpamProxy on a domain controller, you will find the four user groups

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

under **Active Directory > Users and Computers**.

## Establishing the connection to the Intranet Role

The connection of the NoSpamProxy Command Center to the Intranet Role is set to **localhost** after installation.

If the NCC is installed on a different computer than the computer of the Intranet Role, you must adjust the connection.

Proceed as follows:

1. Perform one of the following two steps:
  - Click **NoSpamProxy** and select **Action > Change server** from the menu.
  - Right-click **NoSpamProxy** and select Change server from the context menu.
2. Enter the name of the server (for example **mail.example.com**) and the port (usually **6060**).
3. Click **Save and Close**.

For the change to take effect, you must close and restart the NoSpamProxy Command Center.



**NOTE:** If the NoSpamProxy is operated in a DMZ and you want to control the service remotely from the LAN via the NoSpamProxy Command Center, you only need to enable TCP port 6060 on the firewall and port 6061 for HTTPS. This connection is encrypted on a certificate-based basis. For further information, see [Port allocation](#).

## Configuring the certificate for the Web App

A certificate is required so that users can use the NoSpamProxy Web App and backend services securely.



**NOTE:** After installation, a self-signed certificate is already stored that enables a connection to the Web App. We advise against the use of this certificate and recommend the use of a previously imported certificate to optimise security.

1. Go to **Configuration > NoSpamProxy Components > NoSpamProxy Web App**.
2. Click **Modify**.
3. Under **DNS name**, enter the host name under which the Web App can be reached.
4. Enter the port used and click **Next**.



**NOTE:** Port 6061 is used by default. If you want to establish an HTTPS connection, use port 443.

5. Configure the certificate you want to use to secure the NoSpamProxy Web App:
  - **Private certificate** NoSpamProxy creates both a private certificate and a root certificate. You must install the root certificate on all computers from which you want to connect to the Web App.

- **Existing certificate** You are using an existing certificate that you have previously purchased from a certificate authority and deposited in NoSpamProxy.

6. Click **Finish and restart**.

## **|** Configuring installed on-access virus scanners

To solve (recurring) problems with the interaction of installed on-access virus scanners, configure your virus scanner so that the **directories are**

- 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

be excluded from the scan on all systems with the Gateway Role or Web Portal installed.



**NOTE:** Note that the path is a hidden directory.

For servers with Web Portal installed, the following **folder** (default path for storing files for the Web Portal) must be excluded:

- C:\Program Files\NoSpamProxy\Web Portal

Otherwise, with some virus scanners, access to the Web Portal may be severely delayed and communication problems may occur.

In addition, an exception for the **processes**

- amserver.exe and
- NoSpamProxy.CoreAntispamEngine.exe

should be set if the on-access virus scanner allows this.



**TIP:**

If you do not find the path described above, it is most likely an older NoSpamProxy installation that has already been updated several times. In this case, please first check the file

**C:\ProgramData\Net at Work Mail**

**Gateway\Configuration\Gateway Role.config** and look for the entry **<storageLocation path=**.

This path is currently used by the Gateway Role.

If you have enabled file-based virus scanning in the rules, also ensure that your scanner is configured to completely delete or quarantine infected files and archives. If the scanner is configured to **Clean up**, NoSpamProxy often cannot detect that these have been modified by the installed scanner. Thus, the "file-based virus scan" then fails despite successful detection by NoSpamProxy. This occurs particularly with archives.

## I Deposit of a TLS certificate for inbound connections

If a separate TLS identity is to be used in the receive connector, this must first be stored in the computer certificate store on all systems with NoSpamProxy components. Subsequently, the following service accounts must be granted read permissions on the private key:

- NT Service\NoSpamProxyGatewayRole
- NT Service\NoSpamProxyManagementService
- NT Service\NoSpamProxyPrivilegedService
- NT Service\NoSpamProxyIntranetRole

## I Configuring the SSL Certificate for the Web Portal

To deposit a certificate to secure the Web Portal, it must first be added to the computer certificate store. The certificate may be

- a wildcard certificate,
- a SAN certificate or
- trade a single certificate.

The certificate must then be selected for HTTPS in the bindings area of the default website.

## I Configuring the Large Files directory

In order to enable the full functionality of the Web Portal, especially for the Large Files functionality, the service accounts mentioned below must be equipped with the corresponding rights on the directory configured for Large Files:

- IS AppPool\enQsigPortal - **Write**
- NT Service\NetatworkMailGatewayFileSynchronizationService - **Modify**

## I Setting up the multiple assignment of service ports

If you want to use one port for multiple web services, you must set a *Host Header*. A host header is also referred to as *hostname*. This is used to distinguish between different services that are operated via a common port or a common IP address. For example, it is possible to operate the Web Portal and the Web App via port 443 (or another port).

Setting a host header is only possible with the help of the PowerShell cmdlet `Set-NspWebApiConfiguration`. Below you will find a description:

### Procedure

Enter the following command in the command line:

```
Set-NspWebApiConfiguration -Port <ThePortUsed> -DnsName <TheDNSName> -  
UseHostHeader true -ShowCertificateSelectorUI
```

Setting the value `true` for the parameter `UseHostHeader` configures the use of the host header. In this example, the use of the parameter `ShowCertificateSelectorUI` also determines that a Windows dialogue is displayed, with the help of which you can specify the thumbprint of the certificate.



**NOTE:** After executing the cmdlet, you must restart the NoSpamProxy Command Center.

# Installing NoSpamProxy on a cloud service

## Integrating the TCP proxy



**NOTE:** You must have a valid software maintenance contract to use the TCP Proxy.

It is possible that for cloud-based systems, e.g. Microsoft Azure, port 25 is blocked by the provider. However, port 25 is required for sending emails, and port 25 being blocked prevents NoSpamProxy from operating on such a system.

We offer a solution in the form of our *TCP proxy*. This system can be activated in NoSpamProxy as described below. Each outgoing connection is routed to a routable IPv4 address on the TCP level through the TCP proxy for NoSpamProxy. The emails will be sent from the server via port 443 to the TCP proxy and from there via port 25 to the recipient system.

1. Stop the Gateway Role via the NoSpamProxy console or the Windows services.
2. Open a text editor using administrative rights on the system where the Gateway Role is installed.
3. Open the configuration file "**Gateway Role.config**" from the directory **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

4. Search the file for `<smtpServicePointConfiguration>` and change/add the value

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

as attributes . If `<smtpServicePointConfiguration` is not present, search for `<netatwork.nospamproxy.proxyconfiguration` and add

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

directly under this value.

5. Save the file and close the editor.
6. Place the **Root CA certificate** in the Microsoft certificate store in the computer account under **Trusted Root Certification Authorities > Certificates** on the server with the Gateway Role.
7. In the NoSpamProxy Command Center under **Configuration > NoSpamProxy components > Gateway Roles** edit the appropriate gateway role and change the value for **SMTP Server Name** to the value `outboundproxy.nospamproxy.com`.
8. Restart the Gateway Role.

9. Open the **Gateway Role.config** file again and check whether the value was retained at startup.

## I Adjusting the SPF entry

- If the TCP proxy is implemented, it acts as the sending system. Thus, the TCP proxy must also be included in your SPF record. We strongly recommend adding the following entry to your SPF record:

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

## I Gegebenenfalls: Anpassen von Microsoft 365

Falls Sie aus Azure heraus E-Mails an eine eigene Microsoft-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 Microsoft 365 die TLS-Zertifikate gegen die HELO-Domain geprüft werden, ist es nur mit deutlich erhöhtem Aufwand möglich, dies entsprechend umzusetzen. We therefore recommend validation by name.

## I If necessary: Adjust the firewall

- If you specifically block outgoing connections, you should adjust the exception for the TCP proxy so that connections to the **IP network 193.37.132.0/24** are allowed.

## I Setting up a static IP address

If you want to run NoSpamProxy or parts of it in a virtual machine in a Microsoft Azure environment, you must have an IP address that is retained even after the machine is restarted. To achieve this, you must set up a static IP address (reserved IP address). Otherwise, it is possible that a different IP address will be assigned after the machine is restarted.



**NOTE:** You make this setting on the Microsoft Azure virtual machine where NoSpamProxy is installed.

1. Open the web [page portal.azure.com](https://portal.azure.com).
2. Under **Home > Virtual Computers**, click the virtual computer where NoSpamProxy is installed.
3. Go to **Network > Network interface > IP configurations** and select the configuration relevant for NoSpamProxy.
4. Enable the **Public IP address** option and then click **Create new**.
5. Enter a name and select the **Static** option.
6. Click **OK**.

The IP address is now displayed under the specified name.



**NOTE:** Also note the instructions on the corresponding [page of the Microsoft Azure documentation](#).

## I Customizing the Reverse DNS Entry for the NoSpamProxy Server

1. Go to [portal.nospamproxy.com](https://portal.nospamproxy.com).
2. Go to **Dashboard > Resource Groups > [TheResourceGroupTheVirtualComputerBelongsTo] > [YourVirtualComputer] > Properties**.
3. Enter a name for the public IP address under **DNS name label**.
4. Start the Azure Shell.
5. Enter the following command, replacing the placeholders:

```
az network public-ip update --resource-group  
[ResourceGroup] --name [IPAddressName] --reverse-fqdn  
[FullDNSName] --dns-name [DNSName]
```



**NOTE:** Also note the instructions on the corresponding page of the Microsoft Azure documentation.

# Offline installation

If you want to run the setup file on a computer that has no or only limited access to the Internet, proceed as follows:

1. Switch to a computer that can access the Internet. This can also be a computer with a client operating system.
2. Download the setup file to this computer or place the file on this computer.
3. Open the command line and enter the following command:

```
NameOfTheSetupFile.exe /layout
```

4. Specify the download path.
5. After the download is complete, copy the folder with the downloaded files to the computer on which you want to install NoSpamProxy.
6. Run the Bundle.exe file.

# Port allocation

The components of NoSpamProxy communicate using the following ports:

## Intranet Role

Inbound	Outbound
NoSpamProxy Command Center: 6060 TCP, 6061 TCP	LDAP server: 389/3268 LDAP/GC, 636/3269 LDAPS/GC Web Portal: 443 HTTPS (UDP und TCP) Gateway Role: 6060 TCP, 6061 TCP Internet: 443 HTTPS (TCP)

## Gateway Role

Inbound	Outbound
Intranet Role: 6060 TCP, 6061 TCP Internal email server: 25 SMTP External email server: 25 SMTP Core Antispam Engine: 8093	DNS server: 53 DNS digiSeal server: 2001 TCP Internal email server: 25 SMTP External email server: 25 SMTP Web Portal: 443 HTTPS (UDP und TCP) POP3 retrieval (if required): 465 TCP

Inbound	Outbound
	Internet: 443 HTTPS (TCP) Internet: 80 HTTP (TCP) Core Antispam Engine: 8093

## Web Portal

Inbound	Outbound
Intranet Role: 443 HTTPS (UDP und TCP)	Internet: 443 HTTPS (TCP)

## NoSpamProxy Command Center

Inbound	Outbound
n/a	Intranet Role: 6060 TCP, 6061 TCP



**NOTE:** Port 443 via UDP is only required if QUIC is used for HTTP/3.

# Update recommendations

## General Information



**NOTE:** For more information on updates to version 14 or higher, please visit [Update auf Version 14](#).

### Update sequence

1. Update the Intranet Role. This may take some time. Under certain circumstances, a temporary increase in the allocated RAM memory is helpful.
2. Update the Gateway Role(s). If you use several Gateway Roles, update them one after the other.
3. Update the Web Portal.

### If the Gateway Role and Intranet Role are installed on the same computer

- In most cases of an update, you must perform manual steps before and after the installation, otherwise the smooth operation of NoSpamProxy is no longer guaranteed.



**NOTE:** Please refer to the notes under [Upgrade paths](#).

- After performing a program update, always check the configuration of NoSpamProxy. In particular, check the licence displayed on the overview page of the NoSpamProxy Command Center.

## Offline installation

For information on installation without access to the Internet, see [Offline installation](#).

For information on installation without access to the Internet, see [Offline installation](#).

## I Licenses

If you have any questions about your licence, please contact our support team at [info@netatwork.de](mailto:info@netatwork.de).

For the fastest possible processing of your request, please send us the following information:

- The used version of NoSpamProxy  
You can find the version number in the overview of the NoSpamProxy Command Center in the upper right corner.
- Your existing customer number  
You can find the customer number on the overview page of NoSpamProxy under Manage License or in your license file under `<field name="ContactNumber">C12345</field>` .

## I Proxy settings

The proxy settings are made in a configuration file. These settings are overwritten with every update and must be adjusted again afterwards. Therefore, copy the corresponding configuration files to a backup directory in advance in order to be able to use them again afterwards.



**NOTE:** In the case of updates, for example from version 13.1 to version 13.2, the files can continue to be used. For updates from version 13.2 to version 14 or further updates to versions higher than version 14, the changes must be made on the basis of the new files.

## I Template adaptations

If you are updating from NoSpamProxy 10.x or lower to a newer version, you must still back up the template files of NoSpamProxy manually. These are overwritten with every update to version 10.x and must be saved in advance. After the update you can copy the files back into the original directory. With version 11.x a template designer is integrated in NoSpamProxy. This step will no longer be necessary unless you have adjusted the texts in the templates.



**NOTE:** In the case of updates, for example from version 13.1 to version 13.2, the files can continue to be used. For updates from version 13.2 to version 14 or further updates to versions higher than version 14, the changes must be made on the basis of the new files.

## I Upgrade paths

Depending on which previous version you upgrade from to the current version of NoSpamProxy, different steps must be performed. You do not need a new license file if the software maintenance is still valid.

### Update from version 13.2 to version 14

When updating to version 14, please refer to the notes under **Changes and recommendations as of version 14.**

### Update from version 13.1 to version 13.2

When upgrading from version 13.1 to version 13.2, all settings and user information are retained.

### Update from version 13 to version 13.1

When upgrading from version 13 to version 13.1, all settings and user information are retained.

## **Update from version 12.2 to version 13**

When upgrading from version 12.2 to version 13, all settings and user information are retained. Make sure that the .NET Framework version 4.7.2 is installed and that the SQL Server version is at least 2008 R2, better 2012 or newer. With version 13.0 we have changed the license integration from license file to license key. Please refer to the Knowledge Base article [Installing a new license](#).

## **Update from version 12.1 to version 12.2**

When upgrading from version 12.1 to version 12.2, all settings and user information are retained.

## **Update from version 12 to version 12.1**

Level-of-Trust Hash values are written as SHA-2 instead of MD5 starting with version 11.1. Starting with the following version (version 12.0) the support for reading MD5 will be dropped. The upgrade from a version before 11.1 to a version after 11.1 has to be done via version 11.1 and version 11.1 has to run for one week so that all required hash trusts are converted to SHA-2.

Otherwise, all settings and user information will be retained when upgrading from version 12 to version 12.1.

## **Update from version 11.1 to version 12**

Version 12 of NoSpamProxy requires at least a SQL Server 2008R2 or later. For performance reasons, it is recommended to switch to SQL Server 2016. When updating from version 11.1 to version 12, all settings and user information are

retained during the update.

### **Update from version 11 to version 11.1**

With version 11.1, the SQL Server version 2008 is required. Please update your SQL Server 2005 to at least version 2008 before you start the NoSpamProxy Update.

When upgrading from version 11 to version 11.1, all settings and user information are retained during the update.

### **Update from version 10.1 to version 11**

When upgrading from version 10.1 to version 11, all settings and user information are retained during the upgrade. The NoSpamProxy Disclaimer Administrators group is added for the use of the NoSpamProxy Disclaimer. Please add all users who should manage the templates and rules of the disclaimers to this user group.

### **Update from version 10 to version 10.1**

When upgrading from version 10 to version 10.1, all settings and user information are retained during the upgrade. Upgrades from older versions For information on upgrades from older versions, please refer to our Knowledge Base.

# Changes and recommendations as of version 14



**WARNING:** Make sure you have installed version 13.2.21327.1706 before updating to version 14. Updating from another version may cause problems. See [Software-Archiv](#).

## Changes when updating

### Changed names of the NoSpamProxy services

The NoSpamProxy services have new names. You may have to make adjustments in the monitoring. The following names are used from version 14 (the previous names are in brackets):

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

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

## Changed names of the NoSpamProxy processes

The NoSpamProxy processes have new names. If necessary, adjust the monitoring, the Windows firewall and existing local virus scanners. The following names are used from version 14 (the previous names are in brackets):

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

## Numerous changes regarding the database structure

The changes to the database structure make it necessary to adapt existing PowerShell scripts as well as SIEM systems (for example Splunk).

## **Action CSA Whitelist is now Action CSA Certified IP List**

The action **CSA Whitelist** is now a filter and is called **CSA Certified IP List**.

## **The NoSpamProxy management console is now called NoSpamProxy Command Center**

The NoSpamProxy Management Console/NoSpamProxy Management Console has been renamed NoSpamProxy Command Center and is no longer an MMC snap-in. Any configurations, e.g. if the MMC was previously installed remotely, are lost during the upgrade and must be reconfigured in the new application.

## **New folder for the NoSpamProxy Command Center**

The NoSpamProxy Command Center creates a folder and files in the user profile at **AppData\Roaming\NoSpamProxy**. The configuration of the NoSpamProxy Command Center is saved here.

## **New network address for downloading AV patterns**

A new network address is used to download AV patterns: <https://av-patterns.nospamproxy.com/>

## Changes during new installations

### Changed installation path

The installation path for new installations is **C:\Program Files\NoSpamProxy** (formerly C:\Program Files\Net at Work Mail Gateway).



**NOTE:** When updating, the previous path remains unchanged.

### Changed database names

The names of the databases used are as follows for new installations (the previous names are in brackets):

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



**NOTE:** When updating, the previous names are retained.

### NoSpamProxy Web App

During setup, the NoSpamProxy Web App is installed as part of the Intranet Role.

## Recommendations

- We recommend adding the filter **32Guards** to all inbound and outbound rules.
- We recommend adding the action **32Guards** to all inbound and outbound rules.

## Notes



**NOTE:** When updating to version 14, it is possible that the error message **Failed to compile the template 'C:\ProgramData\Net at Work Mail Gateway\Gateway\Templates\HddStressLevel.cshtml'** is displayed. You can ignore this error message.



**NOTE:** When updating to version 14, you must reconfigure the connection between the NoSpamProxy Command Center and the Intranet Role if they are located on different computers.



**NOTE:**

If a Microsoft 365 server is configured as the corporate email server in version 13.2, an inbound send connector with a cost of 50 is created after the update. This connector cannot be removed. In hybrid scenarios, this can have an impact on email routing, as a normal connector incurs higher costs.

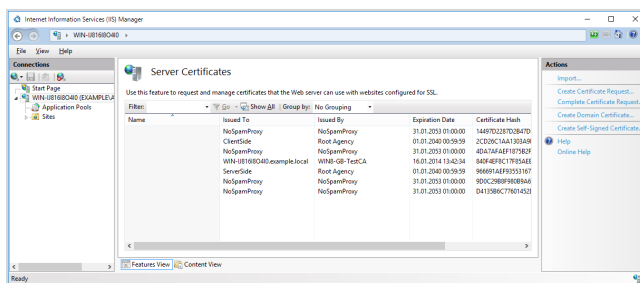
To avoid problems,

- change the cost of the normal connector **before the update** to a value below 50 or
- immediately adjust the costs of the newly created connector **after the update**. Note that email traffic may be interrupted.

# Notes on the installation of the Web Portal

## ■ Installing an SSL certificate in IIS

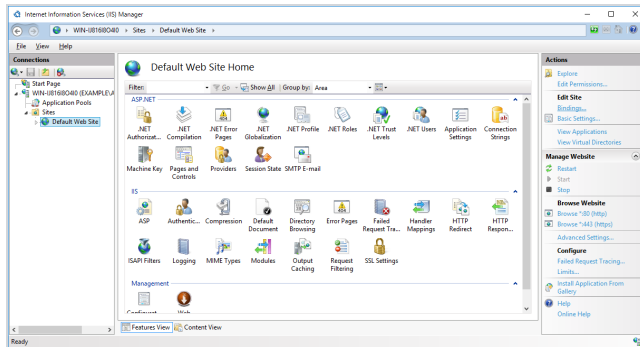
1. Start the **Information Services (IIS) Manager**.
2. Double-click **Server Certificates**. The list of server certificates opens. Check whether your own certificate for SSL access is displayed. The server certificates must be stored in the certificate store of the local computer account and are located under **Personal**. All certificates that can be used for SSL are listed in the **Server Certificates** list in the IIS Manager.





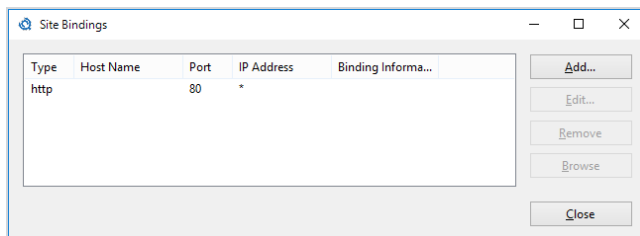
**NOTE:** Make sure that the SSL certificate you use contains, among other things, the exact FQDN that you use to call the web portal. For example, if you want to operate the web portal using the URL **https://portal.example.com/enqsig**, the name **portal.example.com** must appear as the name in the SSL certificate. Furthermore, it must be ensured that the issuer of this certificate is registered on the server of the Intranet Role as a trusted root certification authority. You can view the list of trusted root certification authorities in the certificate store of your local computer account. On the server of the Intranet Role, open Internet Explorer and enter the URL of the Web Portal, in our example **https://portal.example.com/enqsig**. The page must open without error messages. If this is the case, the connection to the Web Portal in the Intranet Role can also be added successfully.

3. Under **Sites**, select the website where the web portal has been installed. For a standard installation it is called Default Web Site.

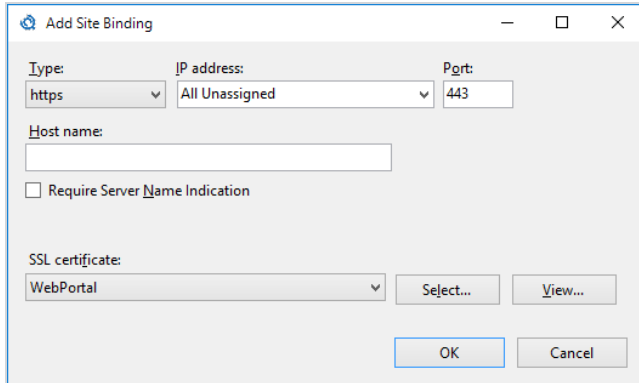


4. Right click **Edit Bindings...** or under **Actions** select **Bindings....**

5. Click **Add....**



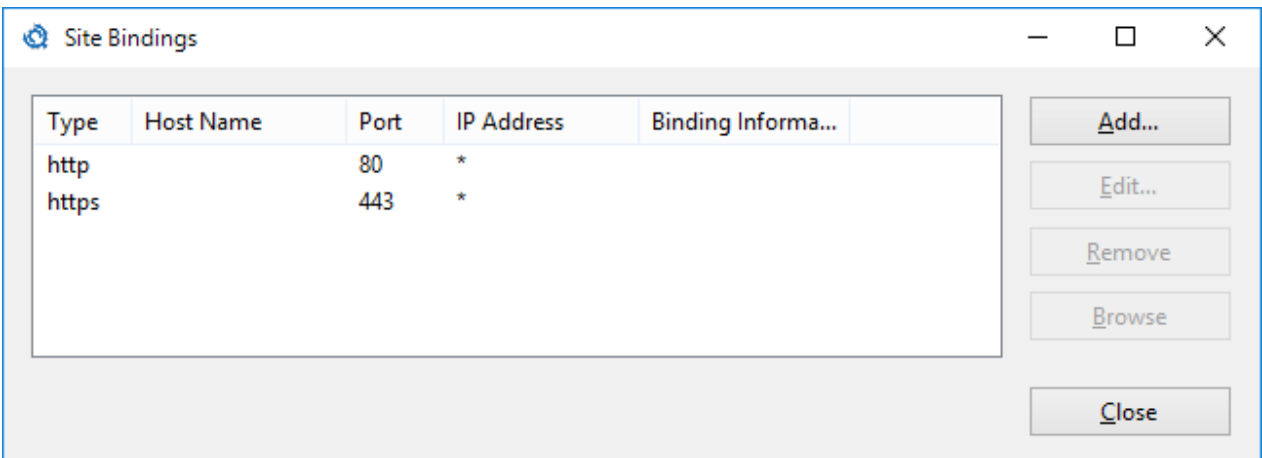
6. If necessary, select a specific IP address, port 443 and the previously controlled SSL certificate.



The 'Add Site Binding' dialog box is shown. It contains the following fields and controls:

- Type:** A dropdown menu with 'https' selected.
- IP address:** A dropdown menu with 'All Unassigned' selected.
- Port:** A text box containing '443'.
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- SSL certificate:** A dropdown menu with 'WebPortal' selected.
- Select...** and **View...** buttons next to the SSL certificate dropdown.
- OK** and **Cancel** buttons at the bottom.

When the dialog is completed, the new binding will appear in the list of all bindings on the website.



The 'Site Bindings' dialog box is shown, displaying a list of bindings. The list has the following columns: Type, Host Name, Port, IP Address, and Binding Informa... (truncated). The list contains two entries:

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

On the right side of the dialog, there are five buttons: **Add...**, **Edit...**, **Remove**, **Browse**, and **Close**.

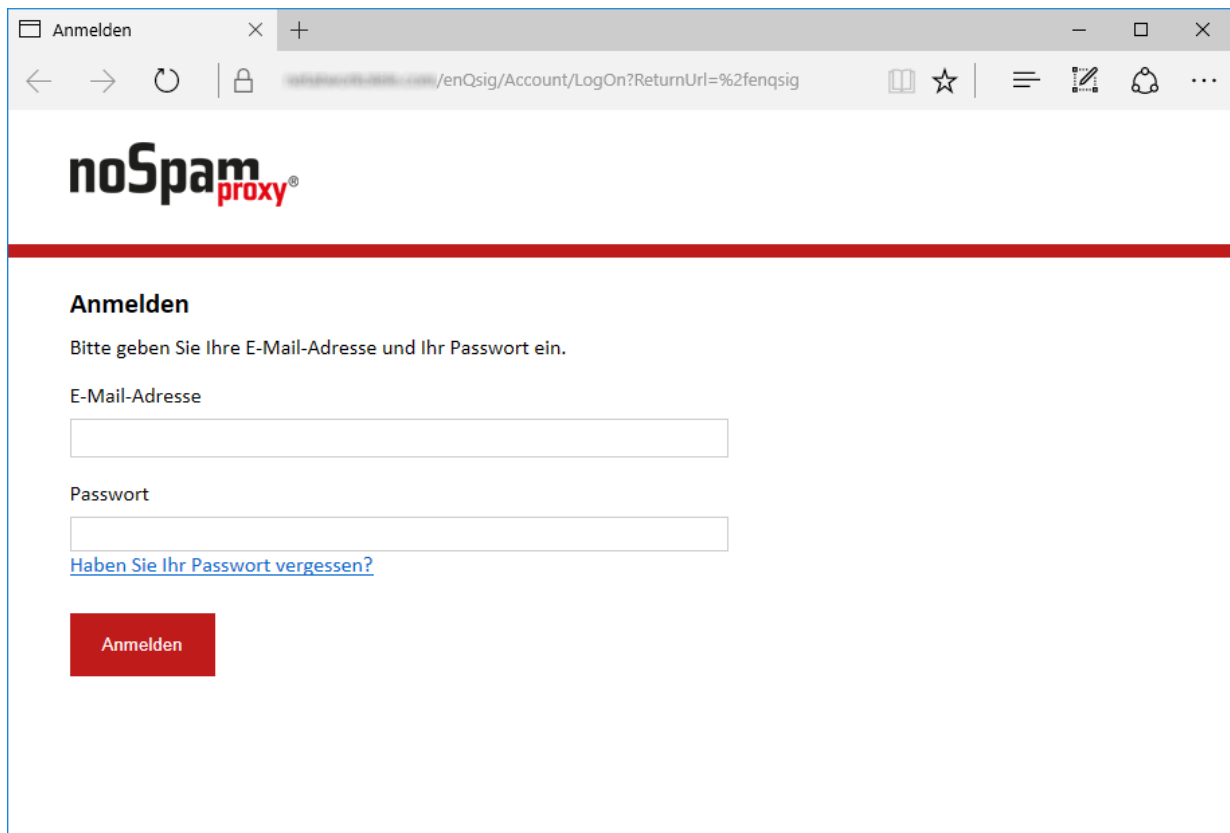
## I After the installation

### Accessing the Web Portal

Once the installation is complete, you can access the website of the Web Portal at the address specified during installation. For a standard installation, this is

**https://<computer name>/enqsig.**

If the page cannot be accessed, please check the configuration of the Internet Information Server. Afterwards, please refer to the chapter on error handling. If the installation was successful, the login page of the Web Portal appears.



The screenshot shows a web browser window with the title 'Anmelden'. The address bar displays the URL 'https://<computer name>/enqsig/Account/LogOn?ReturnUrl=%2fenqsig'. The page features the 'noSpam proxy' logo at the top. Below the logo, the heading 'Anmelden' is followed by the instruction 'Bitte geben Sie Ihre E-Mail-Adresse und Ihr Passwort ein.' There are two input fields: 'E-Mail-Adresse' and 'Passwort'. A blue link 'Haben Sie Ihr Passwort vergessen?' is located below the password field. A red 'Anmelden' button is positioned at the bottom of the form.

## Connecting the Web Portal to the Intranet Role

1. Open the NoSpamProxy Management Console.
2. Go to **Configuration > NoSpamProxy components > Web Portal**.
3. Select the corresponding Web Portal and click **Edit**.
4. Configure the connection.

## I Upgrades

### General Information

If you are updating from a previous version of the Web Portal, please note the following.

- In most cases of an update you will have to perform manual steps before and after the installation, otherwise the smooth operation of the Web Portal is no longer guaranteed. Please refer to the notes under Upgrade paths. The sections are cumulative, which means that you must follow the sections from your currently installed version to the current version in sequence.
- In any case, check the configuration of your Web Portal after you have carried out a program update.

### Updates from version 13.1 to version 13.2

When updating from version 13.1 to version 13.2, all settings and user information are retained during the update.

### **Updates from version 13 to version 13.1**

When updating from version 13 to version 13.1, all settings and user information are retained during the update.

### **Updates from version 12.2 to version 13**

When updating from version 12.2 to version 13, all settings and user information are retained during the update.

### **Updates from version 12.1 to version 12.2**

When updating from version 12.1 to version 12.2, all settings and user information are retained during the update.

### **Updates from version 12 to version 12.1**

When updating from version 11.1 to version 12, all settings and user information are retained during the update.

### **Updates from version 11.1 to version 12**

When updating from version 11.1 to version 12, all settings and user information are retained during the update.

## **Updates from version 11 to version 11.1**

With version 11.1, the SQL Server version 2008 is required. Please update your SQL Server 2005 to at least version 2008 before you start the NoSpamProxy Update.

When updating from version 11 to version 11.1, all settings and user information are retained during the update.

## **Updates from version 10.1 to version 11**

When updating from version 10.1 to version 11, all settings and user information are retained during the update.

## **Updates from version 10 to version 10.1**

When updating from version 10 to version 10.1, all settings and user information are retained during the update.

## **| Error handling**

### **| Login page not accessible - Error 500.21**

If the logon page does not appear, but instead the HTTP error 500.2.1 is displayed, it is likely that Microsoft .NET Framework 4.8 is not properly installed or registered in IIS.



**NOTE:** Before you re-register the Microsoft .NET Framework 4.8 on your Internet server, please check that the framework is compatible with any other Internet sites that may be hosted by this server. Back up your system and especially the IIS configuration before you continue.



**NOTE:** If you have installed NoSpamProxy and Microsoft Exchange on the same server, before installing or upgrading the Microsoft .NET framework, make sure that the appropriate version of the framework is supported by Exchange. For an overview of supported versions, see the [Exchange Server Supportability Matrix](#).

- Re-register the ASP.NET framework with the following command:

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

## I Displaying the certificate store of the local computer

To view the certificates of the local computer, follow these steps:

1. Start a new MMC console (**Start > Run > mmc.exe**).
2. Go to **File** and click **Add/Remove Snap-in**.
3. Select the **Certificates** snap-in and click **Add**. The Configuration Wizard for the **Certificate** snap-in appears.
4. Go to **Computer account**, and then to **Local computer**.
5. Click **Finish**.
6. Click **OK**.
7. Click **Certificates (Local Computer)** to view the certificate stores for the computer.

# Help and support

---

## Knowledge Base

---

The **Knowledge Base** contains further technical information on various problems.

## Website

---

The **NoSpamProxy website** contains manuals, white papers, brochures and other information about NoSpamProxy.

## NoSpamProxy Forum

---

The **NoSpamProxy forum** gives you the opportunity to exchange information with other NoSpamProxy users, get tips and tricks and share them with others.

## Blog

---

The **blog** offers technical support, tips on new product versions, suggestions for changes to your configuration, warnings about compatibility problems and much more. The latest news from the blog is also displayed on the start page of the NoSpamProxy Command Center.

## YouTube

---

On our **YouTube** channel you will find tutorials, how-tos and other product information that will make working with NoSpamProxy easier.

## NoSpamProxy Support

---

You can reach our support team

- by phone at **+49 5251304-636**
- by email at **support@nospamproxy.de**.

