

noSpam[®] proxy SERVER

Manual

Protection

Version 15

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 DECEMBER 11, 2024.

Content

The user interface	1
Actions on the overview page	1
Further settings	3
Monitoring	6
Message tracking	8
Enabling message tracking	8
Filtering search results	9
View details on processing an email	10
Exporting or importing records	15
Report misclassification	15
Notes	16
Message tracking (Web App)	17
Overview	17
Filtering emails	18
Viewing email details	18
Email queues	26
Searching for specific queues	26
Start or pause delivery over selected domains	27
Creating a disabled queue	27
Emails on hold	29
Searching for specific emails on hold	29
In which cases are emails put on hold?	30
Related steps	30
Locked attachments	31

Status types	32
Large Files	37
Related steps	37
Filter options during the search	38
Reports	39
Reports	39
De-Mail	41
Event log	43
Filtering entries	43
Identities	45
Corporate domains	46
Managing corporate domains	47
Editing cryptographic keys	48
Setting up administrative addresses	50
Corporate users	54
Adding corporate users	56
Automating the user import	57
Setting up address rewriting	66
Configuring default settings for users	67
Adding additional user fields	68
Partners	71
Default partner settings	72
Adding partner domains	74
Editing partner domains	75
Adding user entries to partner domains	77

Email authentication	79
DomainKeys Identified Mail (DKIM)	79
Configuration	90
Setting up email routing	92
Adding corporate email servers	92
Creating inbound connectors	97
Creating outbound send connectors	99
Creating receive connectors	105
Invalid requests for SMTP receive connectors	106
Queued delivery	108
Setting up header-based routing	110
Creating rules	111
General Information	111
Steps in creating rules	113
Related topics	118
NoSpamProxy components	121
Intranet Role	122
Gateway Role	123
Web Portal	132
Databases	141
How to change the WebPort for NoSpamProxy	159
Connected systems	162
DNS Servers	163
Archive connectors	164
De-Mail via Mentana-Claimsoft	167

CSA Certified IP List	168
User notifications	170
Inspection report	170
Email notifications	172
How to customise NoSpamProxy notifications	173
Procedure after updates	173
Using different designs for sender domains	180
Presettings	189
Branding	190
Word matching	191
Realtime block lists	193
Advanced settings	195
Sensitive data protection	196
Monitoring	197
Subject flags	200
Level of trust configuration	205
SMTP protocol settings	212
SSL/TLS configuration	218
Troubleshooting	221
Log settings	224
Blocked IP addresses	226
Fixing permissions	227
Market communication with AS4	228
Step 1: Activating the AS4 module	229
Step 3: Creating the required Windows group	231

Step 4: Configuring the key management service	232
Configuring the service address	232
(Optional) Adding an HSM	233
(Optional) Configuring a token	234
Frequently asked questions	235
Step 5: Configuring your market partner account	237
Adding your market partner account	237
Creating a certificate request for AS4 communication	239
Importing certificates	240
Changing settings	241
Step 6: Activating market partner communication	242
Requesting outbound AS4	242
Confirm inbound AS4	243
Testing AS4 connectivity	244
AS4 Message tracking	246
Adding market partners manually	251
Editing the key storage	253
Configuring the storage location for EDIFACT documents	254
Annex	255
Filters in NoSpamProxy	256
Filters available in NoSpamProxy	259
Actions in NoSpamProxy	282
Actions available in NoSpamProxy	283
Basic concepts	303

Sender reputation	303
32Guards	304
Flow Guard	307
Content filters	308
Level of Trust	310
Rules	315
Spam Confidence Level (SCL)	317
URL Safeguard	322
Help and support	327

The user interface

NoSpamProxy is managed via the NoSpamProxy Command Center. It is divided as follows:

- **Monitoring**| This area provides an overview of the receipt and delivery of emails. Additionally, you can view the event log of all connected roles.
- **Identities**| This area is used for basic configuration of NoSpamProxy. You define send and receive connectors for emails, your rules and notifications, and the connections to components.
- **Configuration**| This area is used for basic configuration of NoSpamProxy. You define send and receive connectors for emails, your rules and notifications, and the connections to components.
- **Troubleshooting**| You use this area for diagnostics. You create log files of the individual NoSpamProxy components or have settings corrected automatically.

▮ Actions on the overview page

The available actions are displayed in the lower left corner.

Refresh

Click here to update the data displayed on the overview page.

Configuration wizard

The configuration wizard guides you through all the essential steps of the NoSpamProxy configuration:

Licence| Install a license or change the existing license. If you have not yet created any rules, you can have the appropriate standard rules created depending on your licensed functions.

Connection to the Gateway Role| If no Gateway Role has been connected yet, you can connect your Gateway Role here. After adding the role, set the DNS name for the server identity of this Gateway Role.

Corporate domains| Configuration of the corporate domains. If the gateway has not yet entered any corporate domains when you run the wizard, this step adds the primary domain of the license to the list of corporate domains.

Local email servers| Configuration of the local email servers.

Inbound email delivery| Configure the delivery of email to local email servers.

Outbound send connectors| Configure the delivery of emails to external email servers.

Administrative addresses| Configure the administrative email addresses.

Sensitive data protection| Set a password to protect sensitive data.

When the wizard is complete, perform the following steps:

- Check the configuration of the receive connectors.
- Import your own personal cryptographic keys to use NoSpamProxy Encryption with S/MIME or PGP keys under certificate or PGP key management. See [Zertifikate und PGP-Schlüssel](#).

Carrying out these steps ensures the function of NoSpamProxy.

Change server

Here you can select a server to access via NCC.

Language selection

Here you can change the display language.

I Further settings

Open Disclaimer website

Click here to edit templates and rules for your disclaimers.

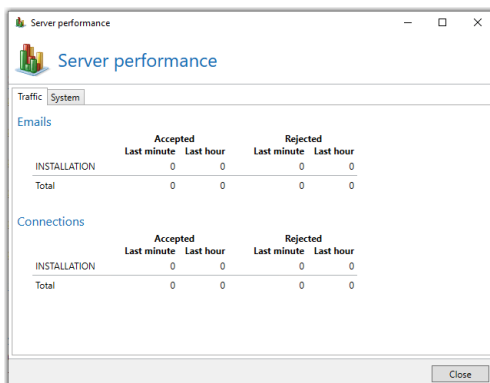
Open documentation

Opens the NoSpamProxy documentation.

View server performance

This action gives you a quick overview of the current processing of emails and the resources currently available.

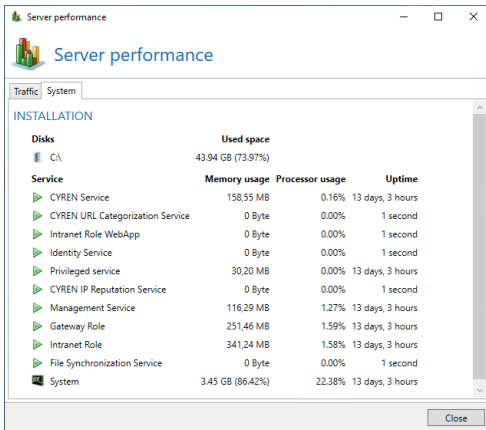
Traffic| This tab shows a moving average of the processed emails of the last minute or hour. The page is updated automatically and also shows you whether NoSpamProxy is currently receiving emails.



The screenshot shows a window titled 'Server performance' with a 'Traffic' tab selected. It displays two tables: 'Emails' and 'Connections'. Both tables show statistics for 'Accepted' and 'Rejected' emails/connections over the last minute and last hour. The data is as follows:

	Accepted		Rejected	
	Last minute	Last hour	Last minute	Last hour
INSTALLATION	0	0	0	0
Total	0	0	0	0

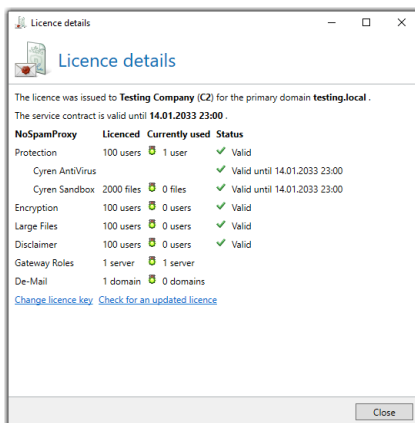
System| This tab shows the installed services, their status and the resources used for each system with Intranet or Gateway Roles.



In addition to this view, the performance indicators are also available on the server.

Manage license

This action opens the dialog for the currently used license. It shows you all relevant data of your license and warns you if problems with the license occur.



Here you can see your C-number, domain and all licensed functions and their validity period.

Change licence key Load another licence file and use it in NoSpamProxy as long as the expiry date of the software maintenance is at least as far or further in the future as the licence currently in use.

Check for an updated licence Check for changes to the active licence.

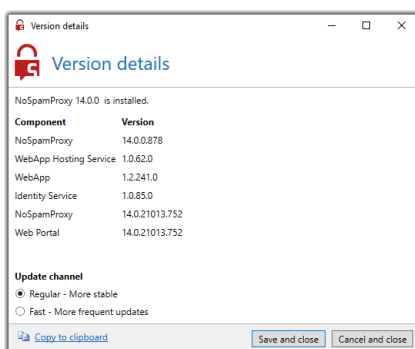
Selecting the update channel

- Click on the version number displayed to view details of the version of your NoSpamProxy instance and to change the release channel.

Updates for NoSpamProxy are offered via two update channels:

Regular Channel The regular channel is the default setting and offers updates that have been tested for a long time and achieve the highest stability for NoSpamProxy.

Fast Channel The Fast Channel offers updates earlier, these have also passed all automatic tests and have also been successfully installed, but have completed shorter test cycles in real environments.



NOTE: If you switch from the fast update channel to the regular update channel, you will only receive updates again when the version offered for updating has a higher version number than the one already installed. This may take some time.

Monitoring

This area provides you with all information about inbound and outbound emails. It also contains status information regarding system and email traffic.

Angehaltene E-Mails Under certain conditions, emails can be put on hold. This means that until further notice, the email will neither be delivered nor rejected, but will wait for certain conditions to be met.

Message tracking	8
Enabling message tracking	8
Filtering search results	9
View details on processing an email	10
Exporting or importing records	15
Report misclassification	15
Notes	16
Message tracking (Web App)	17
Overview	17
Filtering emails	18
Viewing email details	18
Email queues	26
Searching for specific queues	26
Start or pause delivery over selected domains	27
Creating a disabled queue	27
Emails on hold	29
Searching for specific emails on hold	29

In which cases are emails put on hold?	30
Related steps	30
Locked attachments	31
Status types	32
Large Files	37
Related steps	37
Filter options during the search	38
Reports	39
Reports	39
De-Mail	41
Event log	43
Filtering entries	43

Message tracking

This area displays detailed information about the processing of emails. You can see which emails were blocked or let through, as well as trace the procedure of NoSpamProxy and the functioning of the rules.



TIP: The NoSpamProxy Web App offers additional search options for message tracking. See [Message tracking \(Web App\)](#).

Enabling message tracking

1. Go to **Configuration > Advanced settings > Monitoring**.
2. Click **Modify**.
3. On the **Message tracking tab**, select the **Gather message tracks** option.
4. Configure the following options:
 - **Store summaries** | The period of time for which you can trace emails. The message summary information only allows you to see in the message tracking overview whether and when the email you are looking for has arrived and whether it has been accepted or rejected.
 - **Store details** | The retention time for the associated message details. In the details you will find the ratings of each filter, information about the origin of the email and the duration of the analysis, as well as other useful information. Since this information makes up the majority of message tracking, it is possible to keep it for a shorter period of time than the summary information.

- **URL Safeguard**| The period of time for which the visits of the targets of URLs are stored.
 - **Store statistics**| The period for which you can create reports. To be able to create a meaningful report, we recommend a minimum retention period of 12 months.
5. On the **Emails on hold** tab, configure the retention period for emails that are waiting for an encryption key.
 6. Click **Save and close**.

| Filtering search results

You can use the following search criteria individually or in combination to filter the results.

Dispatch period| By selecting under Periods, frequently required searches can be selected quickly.



NOTE: A time period must be specified in any case. By default, the start time is set to the current system time - 1 hour and the end time is set to the current day at 23:59.

- **Sender and recipient address**| The email addresses of the communication partners. It can be filtered for local and external addresses. The search can be performed for exact hits or for components of addresses. The search for exact hits is much faster.
- **Subject**| The content of the subject line.
- **Message ID**| The internal identifier of the email.

- **Delivery results**| The status of the delivery.
- **SCL value**| The calculated spam confidence level.
- **Rule**| The name of the rule by which the message was processed.



TIP: When entering text, you can always enter the entire text to be searched for or just parts of it.

The search results are sorted by date in ascending order.

View details on processing an email

The details contain information on the delivery status as well as the signing or encryption of an email.

1. Right-click the record whose details you want to view.
2. Click on **Details**.

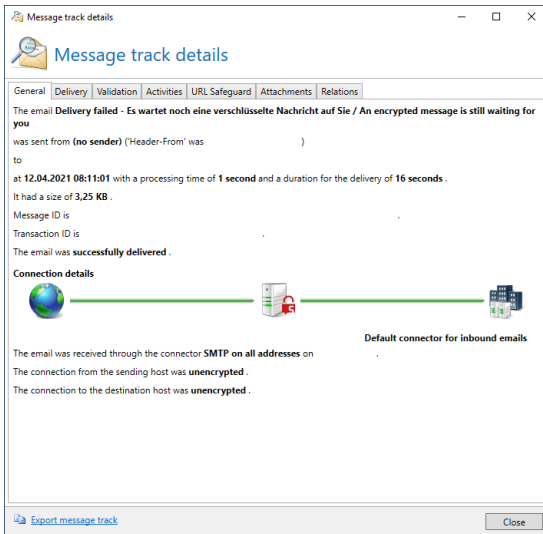
or

- Double-click the record.

Here you can view all processing steps and details that are available for the corresponding data record from the start to the close of the connection.

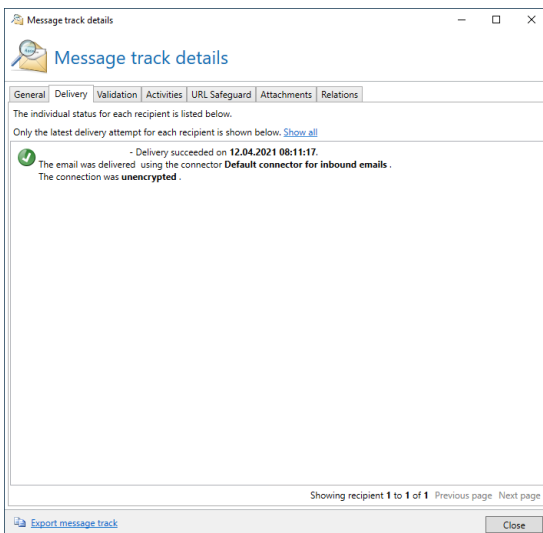
General

The **General** tab contains, for example, information on the connection, the delivery status and the connectors used.



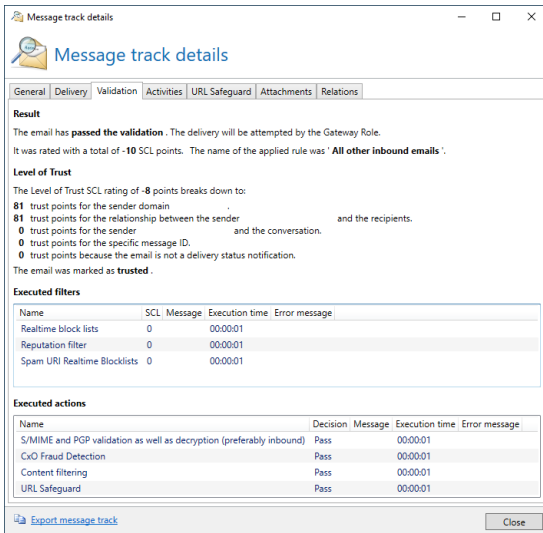
Delivery

The **Delivery** tab contains a list of delivery attempts as well as information on connectors and encryption.



Validation

The **Validation** tab shows, among other things, details about the validation of the email, the calculation of the Spam Confidence Level for the Level of Trust assessment, and the filters and actions performed on the email.



The screenshot shows the 'Message track details' window with the 'Validation' tab selected. The window title is 'Message track details'. The tabs are: General, Delivery, Validation, Activities, URL Safeguard, Attachments, Relations. The 'Validation' tab is active.

Result
The email has **passed the validation**. The delivery will be attempted by the Gateway Role.
It was rated with a total of **-10** SCL points. The name of the applied rule was '**All other inbound emails**'.

Level of Trust
The Level of Trust SCL rating of **-8** points breaks down to:
81 trust points for the sender domain
81 trust points for the relationship between the sender and the recipients.
0 trust points for the sender and the conversation.
0 trust points for the specific message ID.
0 trust points because the email is not a delivery status notification.
The email was marked as **trusted**.

Executed filters

Name	SCL	Message	Execution time	Error message
Realttime block lists	0		00:00:01	
Reputation filter	0		00:00:01	
Spam URI Realttime Blocklists	0		00:00:01	

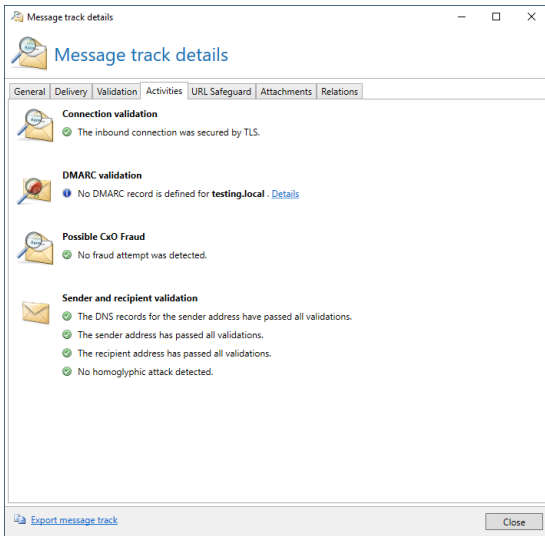
Executed actions

Name	Decision	Message	Execution time	Error message
S/MIME and PGP validation as well as decryption (preferably inbound)	Pass		00:00:01	
CxO Fraud Detection	Pass		00:00:01	
Content filtering	Pass		00:00:01	
URL Safeguard	Pass		00:00:01	

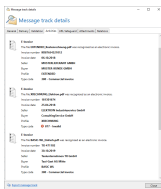
Export message track Close

Activities

The **Activities** tab contains information on activities that have been carried out on the respective email.

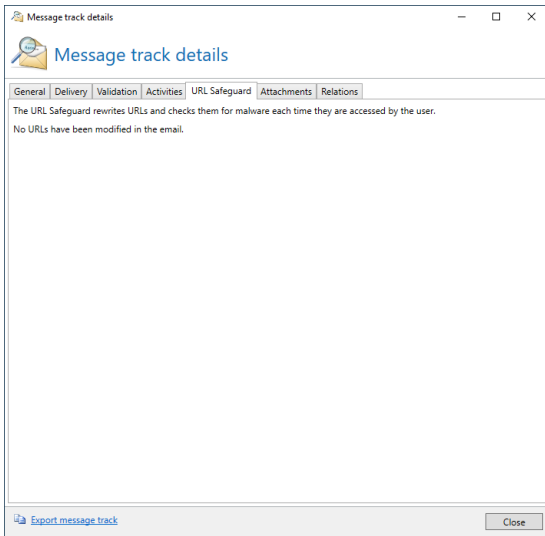


It also provides information on e-invoices received or sent.



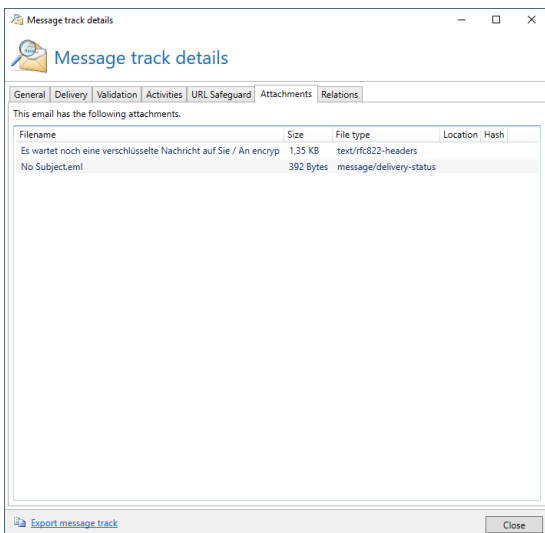
URL Safeguard

The **URL Safeguard** tab contains information on URLs that have been rewritten by URL Safeguard.



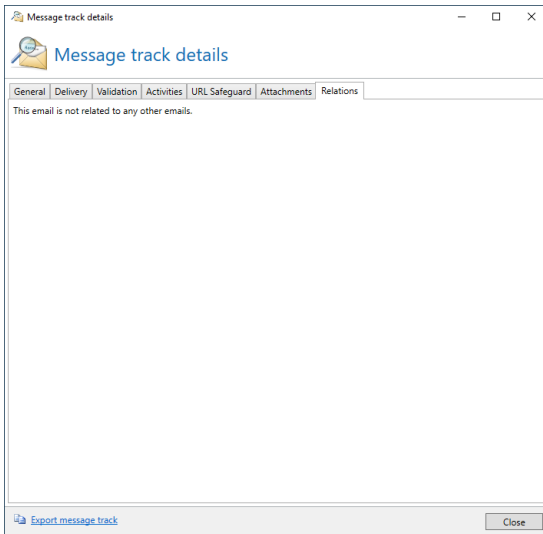
Attachments

The **Attachments** tab contains information about the email attachments, such as size, file type and hashes.



Relations

The **Relations** tab shows emails that are related to the respective email.



Exporting or importing records

You can save the message tracking records as a CSV file on your local hard drive or view saved records in full detail. This function is useful if you need assistance in analysing a data set.

- To export, click **Export all message tracks** in the lower left corner of the details dialog.
- To view, click **Load message track file** in the list of all records found.

Report misclassification

For information on reporting misclassifications, see [Melden von False Negatives und False Positives](#).

Notes



NOTE: Please consider the data protection regulations existing in your company when configuring this section.



NOTE: In order not to let the database size of the message tracking and reports grow uncontrolled, the Intranet Role cleans up the database on a regular basis. All elements that have exceeded a specified age are deleted from the database.



NOTE: If you want to discard all message tracking records and statistical data, please select the option **Disable message tracking completely** under the **Advanced Settings** of the Gateway Role. In this case no data will be collected. For example, if you only want to record statistical data, select the option Message tracking records are deleted immediately to delete all message tracking records at 2 a.m.



NOTE: If you receive several tens of thousands of emails or spam emails per day, the database size limit may be exceeded with an Express Edition SQL Server. With so many emails, shorter retention periods of message tracking records should be chosen or a SQL Server database should be installed without this limitation.

Message tracking (Web App)

The Web App offers further functions via a web-based interface, for example additional search options for message tracking.

Overview

Under **Monitoring > Message Tracking** you will find general information as well as information on the message flow and on signing and encryption.

Icons used



The email was transmitted encrypted.



The email was transmitted partially encrypted.



The email was signed.



The email was partially signed.



The signature is damaged.



The encryption is damaged.



The email was received from the Internet.



The email was sent from a corporate email server.



TIP: A list of the icons can also be found under **Legend** in the message tracking overview.

Rearranging columns

To change the order of the displayed columns, drag the respective column and drop it in the desired place.

Filtering emails

Adding conditions

1. Click **Add condition** in the upper left corner of the message tracking.

Addresses	Connection	Message	Validation	Security
Any address	Direction	Subject	Rule	Signed
'MAIL FROM' address	Sender IP address	Attachment	Status	Encrypted
'Header-From' address	Gateway Role	URL	SCL	
Recipient addresses	Transaction ID	Message ID		
	Delivery duration	Put on hold		
	Processing duration			

2. Select and configure one or more conditions.
3. Click **Search** to execute the query.

To remove a condition, click **Remove Condition next** to the respective condition.


Saving searches

To avoid having to recreate a search you have configured each time, you can save it as a preset. You can then select them from the **Saved searches** drop-down menu.

- After configuring the query, click **Add current search** under **Saved searches** to save it.


Creating default searches

Default searches are executed each time the message tracking is opened.

- From the **Saved Searches** drop-down menu, mark the desired search with  to save it as a default search.

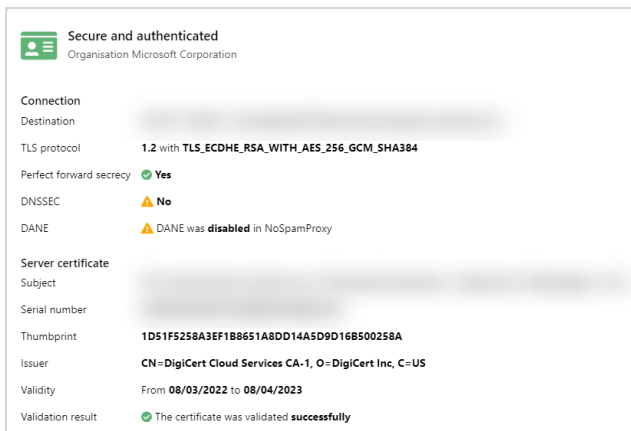
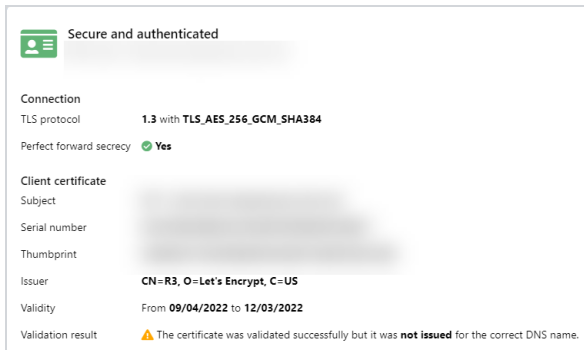
Viewing email details

- Click the email whose details you want to view. The detailed view of the respective email opens.

Monitoring ■ In the **Details** pane on the General tab, click the  icon to open the Details 18 pane in a new tab.

- Click **Download Message Tracking Record** to save the record as a json file

- By clicking on the send address you can display both the MAIL FROM and the Header-From address (if they are different).
- By clicking on the recipient address you can display all recipients.
- By clicking on the name of the TLS server certificate, you can view details of the connection encryption:



Action by the administrator may be required for certain emails. In this case, click **Action required** to view more information and options:

Emails on hold| The email has been stopped for at least one recipient. See [**Angehalten E-Mails**](#).

Locked attachments| At least one attachment requires approval by the administrator.



TIP: Information on the individual status types can be found under [Status types](#).

Delivery tab

Here you will find information about the individual delivery attempts.

The individual status of each recipient is listed below.

Delivery attempt: Latest	Reset filter	1 of 1	
Recipient address	Status	Date	Details
	Successfully delivered	11/16/2022 11:36:28 AM	Delivered to mail via Office 365

[Download message track](#) [Close](#)

- If not all delivery attempts are initially displayed, click **Show all** to display all delivery attempts.

Validation tab

Here you will find information about validation, applied filters and executed actions.



NOTE: Entries in the **Executed Filters** and **Executed Actions** lists are sorted by **Error message (descending) > SCL (descending) > Name (ascending)**.

Major update from Message center

General Delivery **Validation** Activities URL Safeguard Attachments Relations

Result
The email has **passed the validation**. The delivery will be attempted by the Gateway Role.
It was rated with a total of **0** SCL points. The name of the applied rule was **All other inbound emails**.

Level of Trust
The Level of Trust system changed the rating by **0** SCL Points. [Details](#)

Executed filters

Name	SCL	Message	Execution time	Error message
32Guards	0		00:00:01	
CSA Certified IP List	0		00:00:01	
Cyren AntiSpam	0		00:00:01	
Cyren IP Reputation	0		00:00:01	
Real-time blocklists	0		00:00:01	
Reputation filter	0		00:00:06	
Spam URI Realtime Blocklists	0		00:00:01	

Executed actions

Name	Decision	Message	Execution time	Error message
Content filtering	Pass		00:00:01	
32Guards	Pass		00:00:01	
CxO Fraud Detection	Pass		00:00:01	
Greylisting	Pass		00:00:01	
Malware scanner	Pass		00:00:01	
URL Safeguard	Pass		00:00:01	
S/MIME and PGP validation as well as decryption (preferably inbound)	Pass		00:00:01	

[Download message track](#) Close

Validation results and information on Level of Trust

Filters applied to this email

Actions executed based on the filter results

Activities tab

Here you will find information about how the email was processed on the server. These are, for example, details on the applied encryption, reputation checks, and the use of Content Disarm and Reconstruction or PDF Mail. This tab also contains information about the consequences of the results of certain checks.

General Delivery Validation Activities URL Safeguard Attachments Relations

- Connection validation**
 - ✓ The inbound connection was secured by TLS.
- Greylisting**
 - ✓ Greylisting was not applicable for this email.
- DMARC validation**
 - ✓ The message passed DMARC validation. It has been sent from **microsoft.com** . [Details](#)
- Possible CxO Fraud**
 - ✓ No fraud attempt was detected.
- Cyren IP address reputation**
 - ✓ There are no known risks associated with the sender address [redacted]. The Cyren reference ID is [redacted].
- DNS validation**
 - ✓ The IP address [redacted] resolved to hostname [redacted].
 - ✓ The hostname [redacted] associated with the IP address [redacted] is valid.
 - ✓ The hostname [redacted] associated with the IP address [redacted] does resolve back to the IP address.
 - ✓ 'MAIL FROM' domain does resolve to the IP address [redacted].
- Sender and recipient validation**
 - ✓ The DNS records for the sender address passed all validation.
 - ✓ No homographic attack detected.
- Malware scan**

[Download message track](#) Close

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

General Delivery Validation Activities URL Safeguard Attachments Relations

- Possible CxO Fraud**
 - ✓ No fraud attempt was detected.
- E-Invoice**

The file **EXTENDED_Kostenrechnung.pdf** was recognised as an electronic invoice.

Invoice number **KR87654321012**
 Invoice date **10/06/2018**
 Seller **MUSTERLIEFERANT GMBH**
 Buyer **MUSTER-KUNDE GMBH**
 Profile **EXTENDED**
 Type code **380 - Commercial invoice**
- E-Invoice**

The file **XRECHNUNG_Elektron.pdf** was recognised as an electronic invoice.

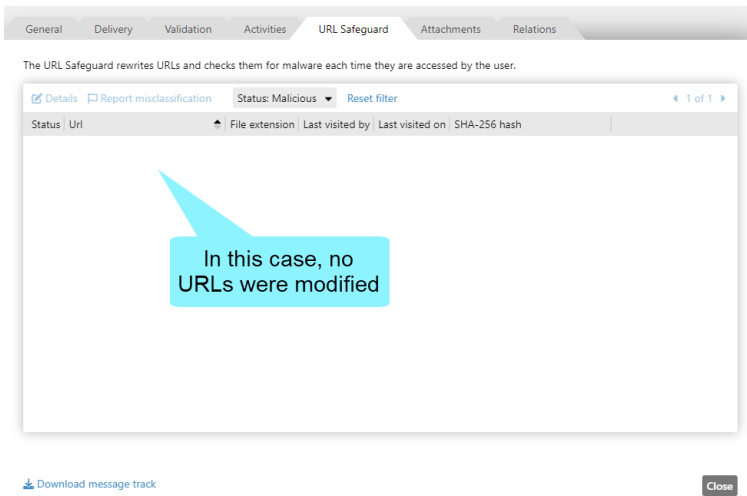
Invoice number **181301674**
 Invoice date **04/25/2018**
 Seller **ELEKTRON Industrieservice GmbH**
 Buyer **ConsultingService GmbH**
 Profile **XRECHNUNG**
 Type code **877 - Invalid**
- E-Invoice**

The file **BASIC-WL_Einfach.pdf** was recognised as an electronic invoice.

[Download message track](#) Close

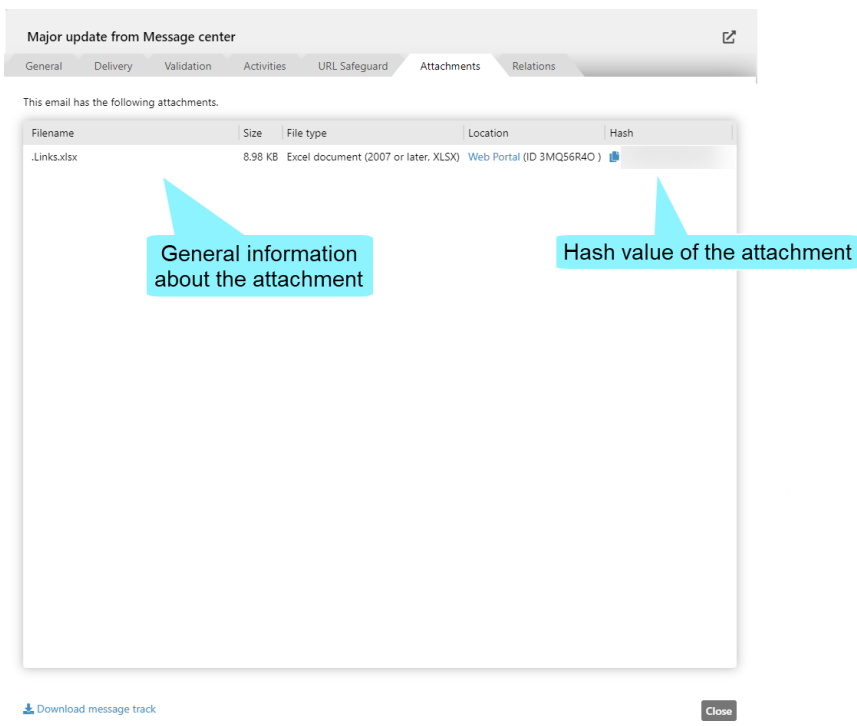
URL Safeguard tab

Here you can find information about URLs contained in the email or attachments that have been rewritten or blocked by the URL Safeguard.



Attachments tab

Here you can find information about attachments contained in the email.



The status of attachments that have been saved on the Web Portal is indicated by the following icons:

- 🔒 | The release of this attachment has been requested.
- ⚠️ | The malware scan for this attachment has failed.
- 🔄 | An automatic approval is set up for this attachment.
- 🗑️ | This attachment has already been deleted.
- 🔒 | This attachment is locked.

For information on locked attachments, see [Locked attachments](#).

Relations tab

Here you will find links to other message tracking records that are related to this record.

Major update from Message center

General Delivery Validation Activities URL Safeguard Attachments **Relations**

This email is related to these emails.

Type	Status	Date received	MAIL FROM	Recipients	Subject
Initiator	Put on hold	05/19/2022 1:23:44 PM	admin@netspam.email	nsp-preview-1@nsp-preview-1.de	test

Type of relation

Click the subject of the email to open the respective details in a new tab

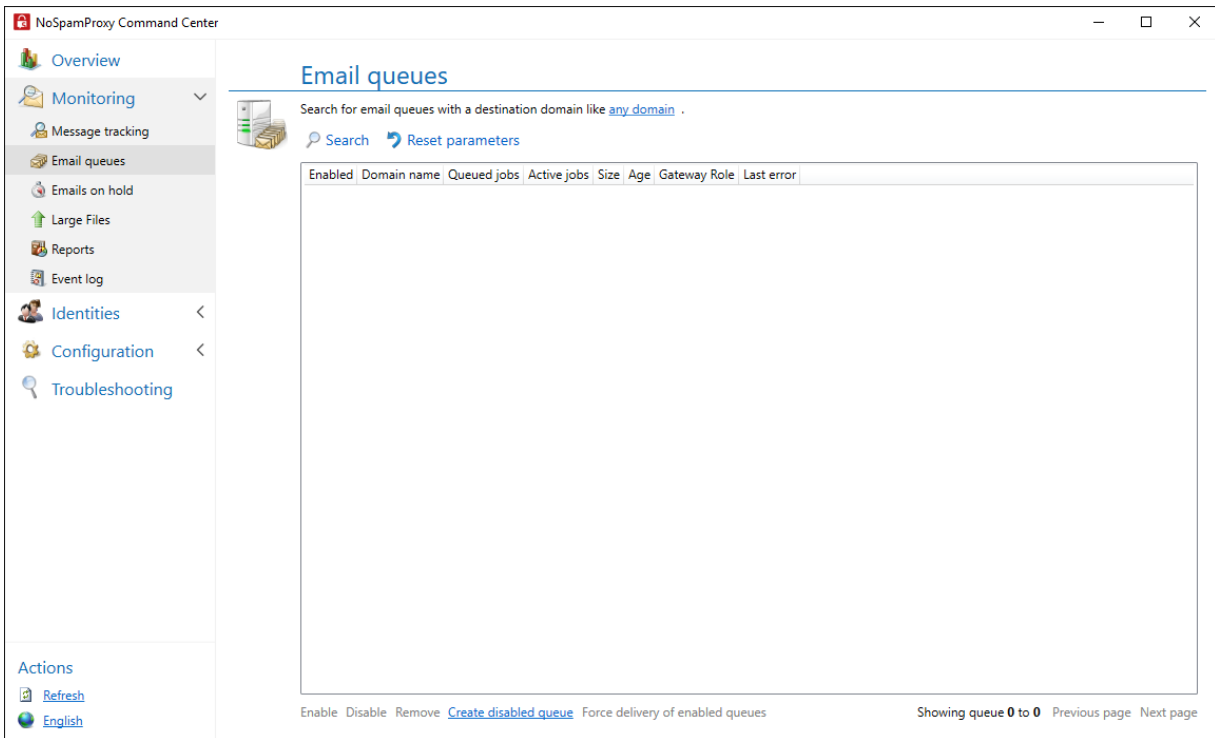
[Download message track](#)

Close

Email queues

Emails to external addresses are assigned to queues according to your domain. There is one queue per domain.

Under **Email queues** all active email queues are displayed. Here you can see at a glance to which domains you still need to send emails. You also have the option of stopping the transfer to one or more specific domains.



Searching for specific queues

1. Enter the search term in the search field.
2. Click **Search**.

All queues that match the search term are displayed.

The individual columns contain detailed information:

Enabled| Shows whether emails are currently being delivered for this domain.

Domain name| Corresponds to the name of the target domain.

Queued jobs| The number of emails.

Active jobs| Shows the currently open SMTP connections to the target domain. This is especially interesting for bulk emailing, where multiple emails are sent to the same domain.

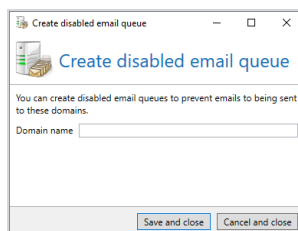
| Start or pause delivery over selected domains

- Click **Activate selected queues** or **Deactivate selected queues** to start or pause email delivery over a specific domain.

| Creating a disabled queue

You can create a disabled queue to prevent the connection to a specific domain in advance.

1. Select **Create disabled queue..**



2. Under **Domain name for queue**, specify the domain name, for example, **example.com**.
3. Save the setting to create the disabled queue.

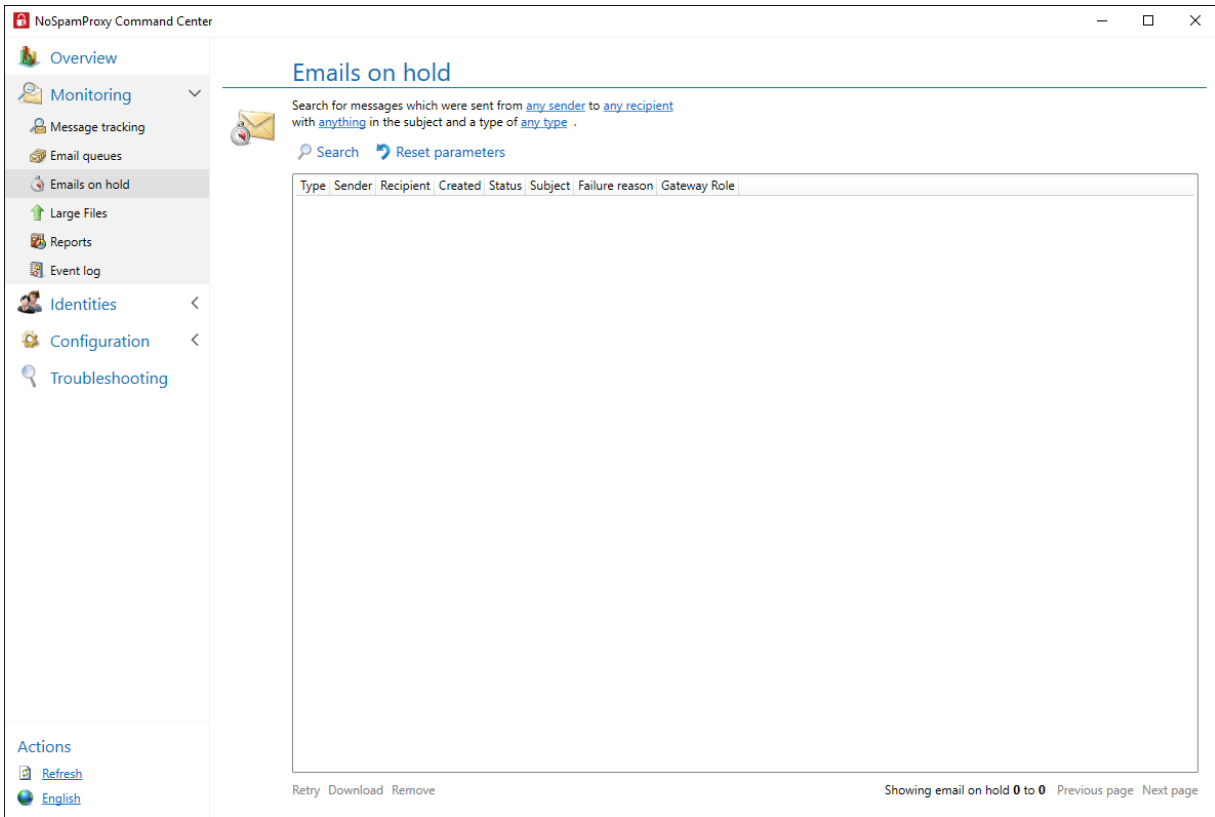
All emails sent to **example.com** are now paused in the NoSpamProxy queues until you reactivate the queue.



TIP: A queue can also be deleted. When deleting, you can decide whether or not a non-delivery report (NDR) is sent.

Emails on hold

Under certain conditions, emails can be put on hold, which means that until further notice the respective email is neither delivered nor rejected, but waits for certain conditions to be met. Email are put on hold in case of missing cryptographic keys, incidents involving file attachments and incidents involving the qualified signature or De-Mail.



Searching for specific emails on hold

When searching for emails on hold, the filter criteria

- Direction,
- sender and recipient address,
- subject line and the
- status

of the email are available.



TIP: For the addresses and subject line, only parts of the text to be searched must be entered.

In which cases are emails put on hold?

- For users of NoSpamProxy Large Files, files that failed to upload are displayed in the list.

Related steps

- **Reprocessing emails**| You can trigger a reprocessing of emails by clicking **Retry**. If incidents occur again, the affected emails are entered into the list again.
- **Saving emails locally**| You can save complete emails with all associated documents locally by marking the respective incident and then clicking **Download**.
- **Deleting emails**| You can delete emails on hold. You can choose whether or not the sender is notified about this.

Locked attachments

Attachments that have been locked are stored on the Web Portal. On the **Attachments** tab in the details view of the respective email, you have the following options:

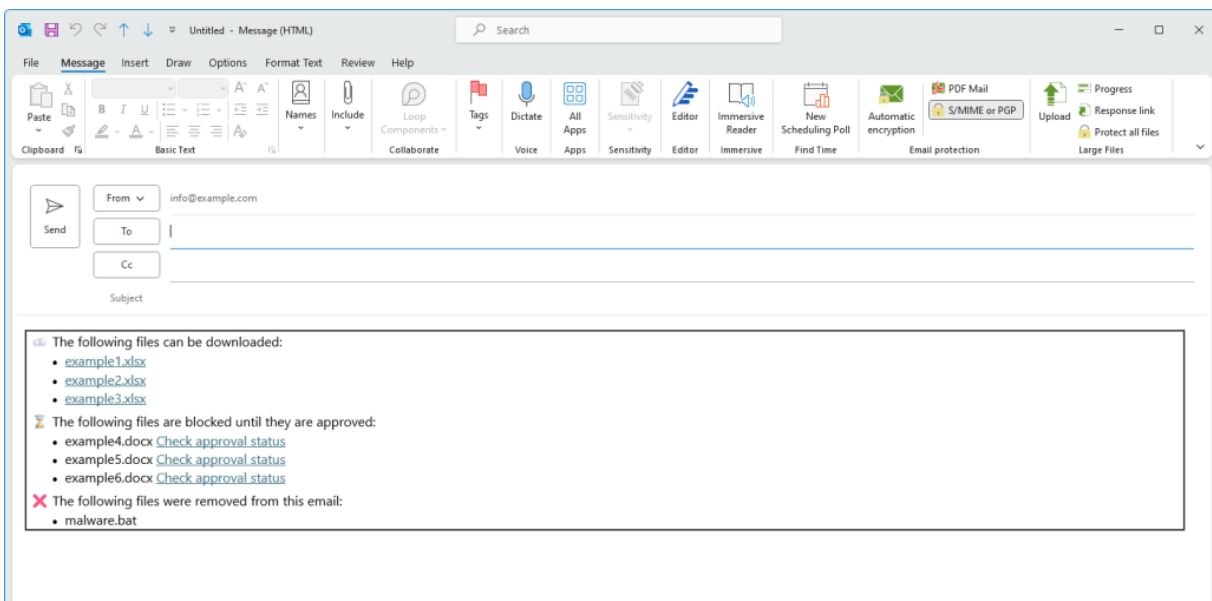
- Click **Large Files** for more information on the attachment, to download the attachment or to run a malware scan.
- Click **Approve attachments** to approve the respective attachments.
- Click **Discard attachments** to delete the respective attachments.



TIP: For an overview of all emails that contain files that require manual approval, add the condition **Attachment requires approval** in the message tracking.

Email hints

Links to Web Portal files are added as notes in the respective emails.



■ Status types

In the following, the individual status types are explained by means of examples.



NOTE: This information is for basic understanding and does not necessarily cover every case.

- **Successful**| The email was successfully transmitted to the recipient.
- **Delivery failed**| An outbound email was rejected by the receiving system. In the "Delivery" tab, you can track the feedback from the receiving system.
- **Temporarily rejected**| The delivering email server receives a response and will make another delivery attempt after the configured interval.
 - **Greylisting**| An inbound email has received at least 2 SCL points for violating our filters.
 - **Recipient does not match the rule of the first recipient**| An outbound email is sent to different recipients and a certificate for encryption is not available for each recipient.
 - **32Guards**| A recently righted host is temporarily rejected for a short period of time to determine its reputation.
 - **Service not reachable**| The Integrated Malware Scanner is usually configured as the only selected **Malware scanner** but is not reachable.
- **Permanently rejected**| The email was rated with at least 4 SCL points due to violation of our filters or rejected by [Actions in NoSpamProxy](#).
- **Delivery pending**| The email is still being delivered and will be noted shortly with a different status depending on the result. Details can be found on the tab **Delivery**.

- **Multiple delivery states**| An email was sent to several recipients and noted with different results. Details can be found in the respective entry on the tab **Delivery**.
- **Accepted but not delivered**| The email is received but cannot be processed.
 - **Outbound content filtering**| The stored content filter prohibits the attachment of the e-mail.
 - **Encryption**| A rule with mandatory encryption is used; this was not possible for the recipient.
 - **The sender has established a connection but has not transmitted an email body**| In this case, NoSpamProxy only sees the email envelope with sender and recipient, but cannot process the email. Often such a connection is created to validate an email address of a previously outgoing email and is intended to serve as an anti-spam measure. The process is known as **callback verification**.
 - **De-Mail**| An attempt is made to deliver an email for which there is no configuration in NoSpamProxy to a De-Mail recipient.
- **Duplicate**| An email was delivered twice to NoSpamProxy. The loop (email loop) is prevented and the email is not delivered.
 - An inbound email is delivered by NoSpamProxy to the configured email server. However, this email does not end up in the recipient's mailbox, but the email server sends it back to NoSpamProxy again a few seconds after receiving the email.
 - An inbound email was sent twice with the same message ID from the same or different submitting systems. Each email must have a unique mail ID.

- An outbound email to Office 365 is fetched back into the own tenant. In this case, the own Office 365 connector is the problem.



Office 365 operates on the principle that there are multiple access points for emails. If you configure a connector, it is transmitted to the systems responsible for your client.

If a communication partner receives emails via the same system as you, your connector (inbound) naturally also applies.

Please note that Office 365 has two types of connectors: **Partner organisation to Office 365** and **Organisation email server to Office 365**. The crucial difference here is that the partner connector only becomes active if one of your own domains is specified as the email recipient. The connector **Organisation email server to Office 365** takes effect when your domain appears as the sender and then retrieves the email back to your tenant.

From NoSpamProxy's point of view, the email is correctly delivered to the system specified in the MX. From Microsoft's side, however, the difference to the expected behaviour is that your client receives the email due to the previously mentioned connector instead of the actual recipient client and then wants to deliver it back to NoSpamProxy according to the rules. The email was then delivered from NoSpamProxy's point of view, but incorrectly classified in Office 365.

There are several solutions here. All of them aim to distinguish between emails from you and emails coming to you. You can achieve this either by re-creating the inbound connector in Office 365 (**partner organisation to Office 365**) or by switching to

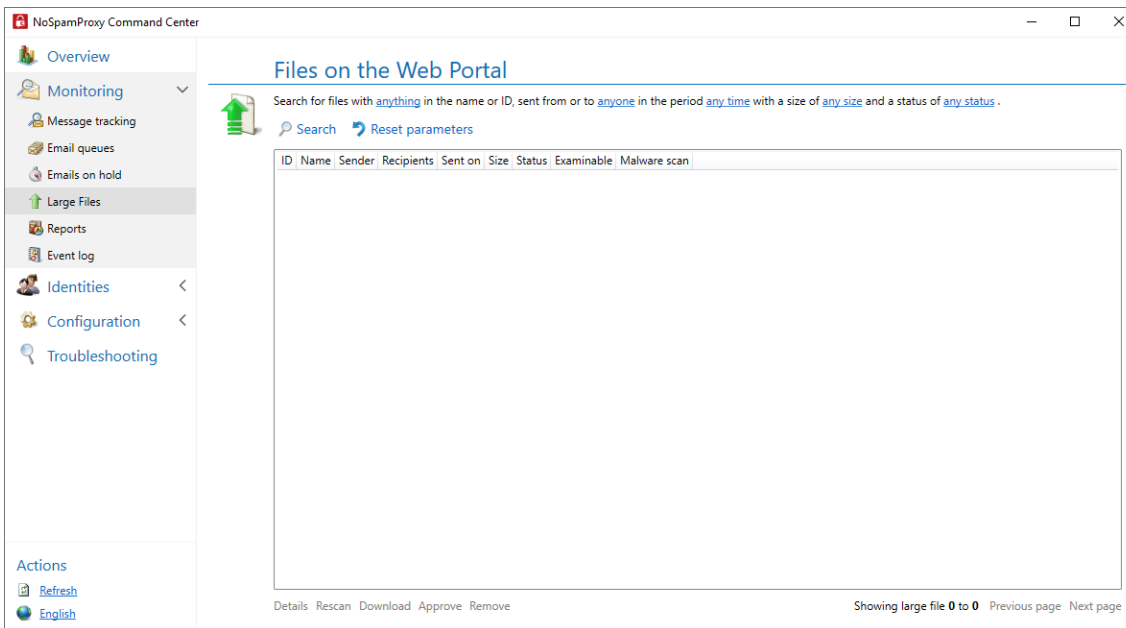


different TLS identities for inbound and outbound send connectors in NoSpamProxy. We recommend here not to transmit a TLS identity in the outbound send connector.

- **Put on hold**| Further actions are necessary for the email to be delivered successfully.
 - **Content filter**| The email is stopped to process the attached files and then delivered with a second message track as a successful email. The action performed can be tracked in the Message Track on the **Activities** tab. You can track the successor of the email in the Message Track on the tab **Relations**.
 - **PDF mail**| The outbound email is converted into a PDF document and encrypted because there is no S/MIME certificate for the recipient. The recipient must assign a password on the Web Portal; until then, the email remains in this status.
 - **Service not reachable**| The Integrated Malware Scanner cannot reach files that are to be uploaded to the Web Portal.

Large Files

Here you get an overview of all files currently stored on the Web Portal.



Related steps

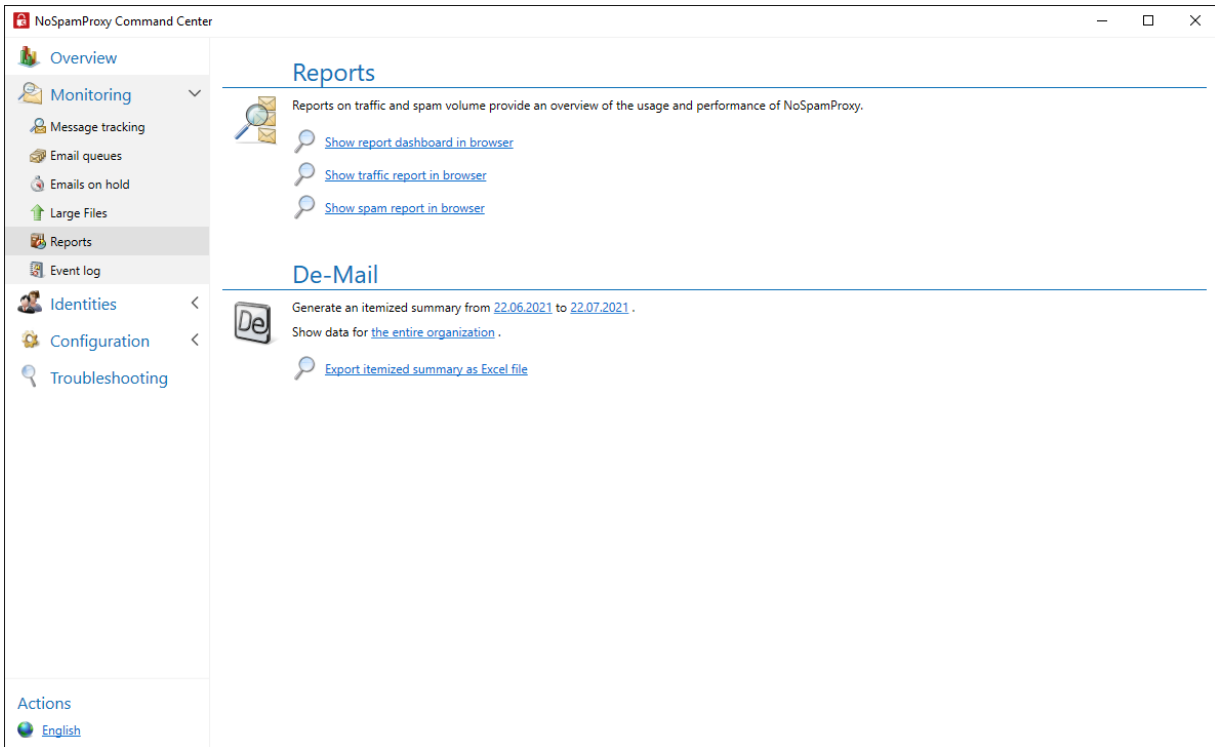
- Deleting files that are no longer needed.
- Sharing files for download that require the approval of an administrator.
- Downloading files not yet released by the administrator to check their contents (if they are marked as **examinable** in the list)
- Scanning files for malware via **Rescan**. If malware is found, the file is deleted and the recipient is informed of the result. The **Malware scan** column shows the time of the last scan.

Filter options during the search

- **File name**| Specify the full or partial file name.
- **ID**| The email ID of the respective email.
- **Sender or recipient address**| Specify a full or partial email address. In the overview, only the first recipient address is displayed for the recipient addresses, but all addresses are searched for.
- **Periods**| The period can be limited. If you want it to remain open, clear the check boxes before **From** and **To**. By selecting under Periods, frequently required searches can be selected quickly.
- **File size**| Restrict the file size using the sliders. Deactivate the restriction by the check boxes in front of the sliders.
- **Status**| Select all files or files with certain properties, such as **Waiting for approval**, **Never downloaded** or **Malware scan failed**. You can also search for files that have not yet been approved or where errors occurred during the malware scan. Click **Details** to view additional recipients and any problems that may have occurred during the malware scan.

Reports

The NoSpamProxy reports give you an overview of your email traffic history and how the volume of spam has changed over the months, as well as information on the email addresses and domains that received the most spam.



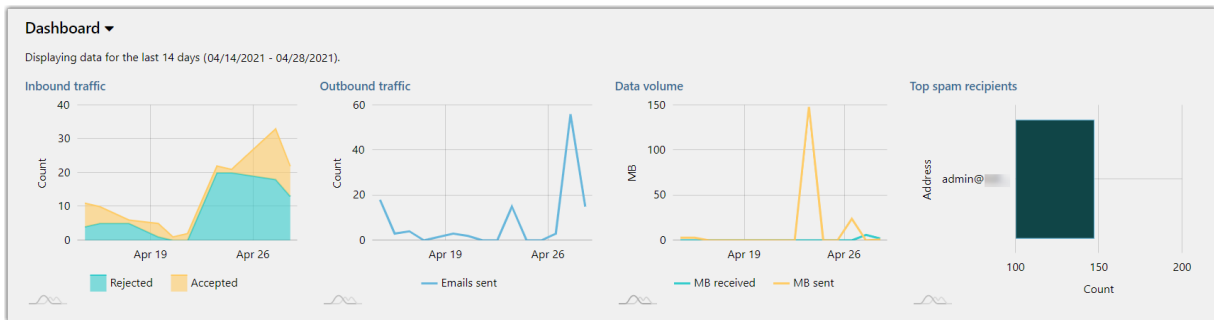
Reports

The reporting in NoSpamProxy Cloud now offers a quick overview of inbound and outbound email traffic as well as the top spam recipients.



TIP: You can hover over a date in all views to see exact details.

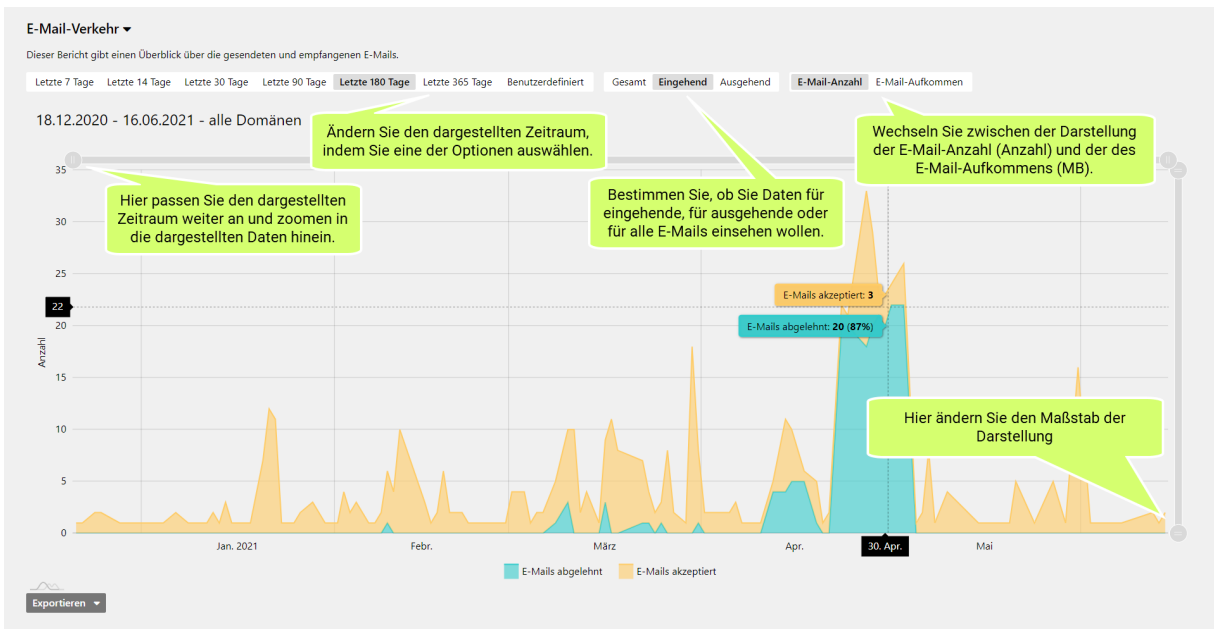
Dashboard



The dashboard shows you four quick overviews of

- inbound emails
- outbound emails
- the data volume (MB) and
- the top spam recipients.

Email traffic



The detailed views on email traffic provide you with detailed overviews on the selected period and direction of the email flow. Adapt the individual charts to your needs by, for example, changing the time period displayed or displaying only data for incoming emails.

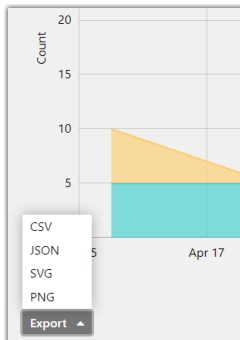
Top spam recipients

This view shows you the recipients who have received the most spam in the selected period.

Exporting charts

You can also export charts as files in CSV, JSON, SVG or PNG formats.

1. In the desired chart, open the drop-down menu in the lower left corner.
2. Select the format in which you want to export the chart.



De-Mail

With the De-Mail report you can generate an individual connection overview for sent De-Mails as an Excel report.

Proceed as follows:

1. Select whether you want to create an overview for the entire organization or for a specific domain.
2. If necessary, restrict the time period for the overview.
3. Click on **Export as Excel file**.
4. In the following dialog, select where you want to save the Excel file.
5. Click **Save**.

Event log

The server events relevant for NoSpamProxy are available here.

Ereignisanzeige

Suche nach [alle Einträge](#) für [alle Rollen](#) .

Suchen [Parameter zurücksetzen](#)

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

Zeige Ereignis 1 bis 50 Vorherige Seite [Nächste Seite](#)

Details

Markierte Einträge in die Zwischenablage kopieren

Filtering entries

The following properties can be used to limit the results:

- Roles and services

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

[Alle auswählen](#) [Alle löschen](#)

- Type of events displayed: errors, information and warnings.

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



TIP: To look at previous entries, you can browse through the results of the search using **Back** and **Next**. To view the details of an entry, select it with the mouse. The details are displayed in the lower part of the page.

Identities

This section gives you access to all external and internal companies and persons as well as to their email addresses.

Corporate domains	46
Managing corporate domains	47
Editing cryptographic keys	48
Setting up administrative addresses	50
Corporate users	54
Adding corporate users	56
Automating the user import	57
Setting up address rewriting	66
Configuring default settings for users	67
Adding additional user fields	68
Partners	71
Default partner settings	72
Adding partner domains	74
Editing partner domains	75
Adding user entries to partner domains	77
Email authentication	79
DomainKeys Identified Mail (DKIM)	79

Corporate domains

Corporate domains are the domains for which you want to receive emails. The list of corporate domains can also be used in the [Creating rules](#). Connections to domains that are not included in the list will be regarded as relay abuse by NoSpamProxy.



NOTE: You must add all local domains to the list of corporate domains. Otherwise, all local emails will be rejected.

The screenshot shows the NoSpamProxy Command Center interface. The left sidebar contains navigation options: Overview, Monitoring, Identities (expanded), Corporate domains (selected), Corporate users, Partners, Certificates, PGP keys, Public key servers, Key enrolment, Email authentication, Additional user fields, Configuration, and Troubleshooting. The main content area is titled "Corporate domains" and includes a table of configured domains.

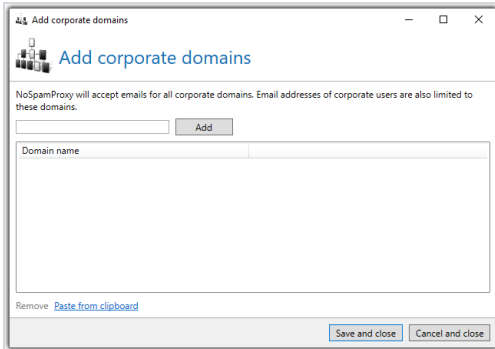
Domain name	Administrative addresses	Associated certificates	Associated PGP keys	DKIM key
example.com	Use default domain settings	John Doe Max Mustermann	"Max Mustermann" <max.mustermann@example.com> ✓ Valid "John Doe" <john.doe@example.com>	example on example.com
example.local	Use default domain settings			example on example.com

Below the table, there are links for [Add](#), [Modify](#), and [Remove](#). A section titled "Default domain settings" explains that these settings are used if no more specific settings are configured on a domain. It lists that notifications to corporate users are sent from `example@example.com`, notifications to external recipients are sent from `example@example.com`, and administrative alerts are sent to `admin@example.com`. A [Modify](#) link is provided at the bottom.

Managing corporate domains

Adding corporate domains

1. Go to **Identities > Corporate domains**.
2. Click **Add**.



3. Enter the name of the domain you want to add.
4. Click **Add**.

Removing corporate domains

1. Go to **Identities > Corporate users > Corporate users**.
2. Select the domain you want to remove.
3. Click **Remove**.

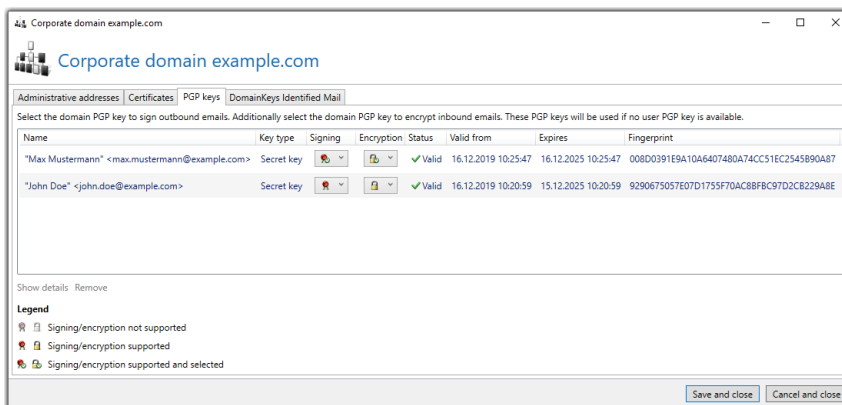


NOTE: When you delete local domains, all email addresses in that domain are also deleted from corporate users. If the users do not have any email addresses after this deletion, the users will also be deleted.

Editing cryptographic keys



NOTE: The management of domain certificates and domain PGP keys in the company domains as well as the management of certificates and PGP keys in the email addresses of the Corporate users is done almost identically. The following description of key selection applies to both applications.



Requesting cryptographic keys

1. Go to **Identities > Corporate domains**.
2. Double-click the domain whose cryptographic keys you want to edit or highlight the domain and click **Edit**.
3. Switch to the **Certificates** or **PGP keys** tab.
4. Determine
 - under **Signing**, which of the cryptographic keys is to be used for signing emails and

- under **Encryption**, which of the cryptographic keys is to be used for encrypting emails.

5. Click **Save and Close**.



NOTE: NoSpamProxy only offers you the options for each cryptographic key that the respective key supports. Please note that only one key can be selected for encryption or signature at a time. If you select a different key at a later date, the first selected key will no longer be used for encryption.

Show details

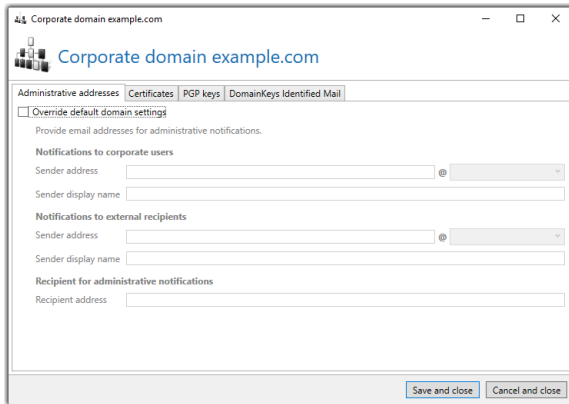
- Click **Show details** to view all properties of the key.

Deleting cryptographic keys

- Click **Remove** to delete the respective cryptographic key.

Setting up administrative addresses

Domain-specific addresses



NoSpamProxy requires valid sender addresses for the email notifications it sends and an address to which administrative alerts are sent. To configure domain-specific addresses, proceed as follows:

1. Go to **Identities > Corporate users > Corporate users**.
2. Double-click the domain you want to edit.
3. Select **Overwrite default domain settings** to use the settings made here in place of the default domain settings.
4. Enter the respective addresses.
5. Click **Save and close**.

Cross-domain addresses

Here you define administrative addresses that are used for sending email notifications and receiving administrative alerts if no specific settings are configured for the domain. Proceed as follows:

Default domain settings

Default domain settings

Provide email addresses for administrative notifications. These settings are used when no domain specific settings are configured.

Notifications to corporate users

Sender address: example @ example.com

Sender display name: Max Mustermann

Notifications to external recipients

Sender address: example @ example.com

Sender display name: Max Mustermann

Recipient for administrative notifications

Recipient address: admin@example.com

Save and close Cancel and close

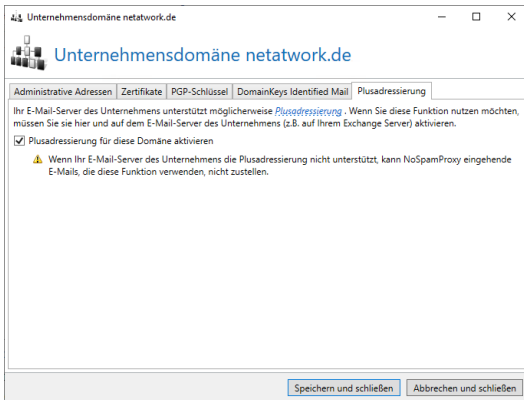
1. Go to **Identities > Corporate users > Corporate users**.
2. Click **Default domain settings**.
3. Enter the respective addresses.
4. Click **Save and close**.



TIP: If a domain requires an address that differs from the default address, you can configure this address for the respective domain.

Plus Addressing

Plus addressing (also known as sub-addressing) is a method of supporting dynamic, discardable email addresses for mailboxes. If activated, NoSpamProxy assigns, for example, the company user with the email address `john.doe@example.com` to the email address `john.doe+newsletter@example.com`.



WARNING: If your corporate email server does not support plus addressing, NoSpamProxy will not be able to deliver inbound emails that use this feature.



Plus addresses (also called sub addresses) are **not** counted in the context of licensing, provided plus addressing is activated for the respective domain. This applies both to the licensing of modules and to the licensing of services. Only the underlying email addresses of users for whom plus addresses exist are counted.



NOTE: If you want to use this function, you must activate it here **and** on the company's email server, e.g. your Exchange server.

1. Go to **Identities > Corporate domains**.
2. Double-click the domain you want to edit or highlight it and click **Modify**.
3. Go to the **Plus addressing** tab.

4. Check the box **Enable plus addressing for this domain**.
5. Click **Save and close**.



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

Corporate users

As with Corporate domains, NoSpamProxy can check the individual recipients and reject emails to non-existent recipients immediately. To do this it is necessary that NoSpamProxy knows all internal recipients. If you use an Active Directory, you can easily import the corporate users.

The list of corporate users is used when you filter for **Local addresses** instead of **Corporate domains** in the rules.



NOTE: In order for NoSpamProxy to use the list of corporate users, the scope in the corresponding rules for inbound email traffic on the **Message flow** tab must be changed from **to a corporate domain** to **a corporate email address**. Only now does NoSpamProxy use the list of corporate users to determine valid email addresses.

Corporate users

Corporate users represent the members of your organization.
 Search for users with [anything](#) in the name, their details or email addresses and a status of [any status](#).

[Search](#) [Reset parameters](#)

Enabled	Type	Display name	Email addresses	Inbound content filtering	Outbound content filtering	Flow Guard
✓	Manual user	John Doe	john.doe@example.com	Use parent settings	Use parent settings	Default user settings
✓	Manual user	Max Mustermann	max.mustermann@example.com	Use parent settings	Use parent settings	Default user settings

[Add](#) [Modify](#) [Remove](#) [Request cryptographic keys for selected users](#) [Automatic user import](#) Showing address 1 to 2 [Previous page](#) [Next page](#)

Default user settings
 These settings are used if no more specific settings are configured on a user.
 Allow **any** attachment on inbound emails.
 Allow **any** attachment on outbound emails.
 Users can send emails to **unlimited** recipients per 60 minutes and to **unlimited** recipients per 24 hours.
[Modify](#)

Actions
[Refresh](#)
[English](#)

Types of users

The list of corporate users can contain two different types of users:

- **Manually entered users** | You can manage all properties of manually entered users in NoSpamProxy. These users can be changed and deleted at will.
- **Replicated users** | Replicated users are imported from a directory service such as Active Directory. The properties of these users must be changed in the original source, because in replicated users only a read-only view of most properties is available in NoSpamProxy. All changes will be applied when the user imports are executed again. In replicated users, you can change the activity status of the entire user as well as the activity status of individual email addresses.

Related steps

- **Adding corporate users**| All users that are to be managed by NoSpamProxy must first be added. See [Adding corporate users](#).
- **Importing users automatically**| You can automate the import of user data through **Automatic user import**. See [Automating the user import](#).
- **Setting up address rewriting**| Address rewriting changes the email address of a corporate user to another email address. See [Setting up address rewriting](#).
- **Setting specific content filters as default**| See [Configuring default settings for users](#).

Adding corporate users

To add a corporate user, do the following:

1. Go to **Identities > Corporate users > Corporate users** and click **Add**.
2. Enter the name of the new user and (optional) details.
3. Enter all the user's email addresses by typing the local part of the email address and selecting the domain from the drop-down menu.



NOTE: The first address entered will be used as the primary address. You can change this in the list of email addresses by selecting **Set as primary address**. The primary address is used for other functions, such as De-Mail.



NOTE: For more information about editing certificates linked a user's e-mail address, see [Kryptographische Schlüssel für Domänen verwenden](#).

4. (Optional) Set up Address rewriting for the email address.
5. Select the content filter to be assigned to the user or use the [Configuring default settings for users](#).
Note that content filters configured for partners are also applied. For emails received from the Internet, the content filters of the partner and each local recipient are combined. The most restrictive settings are then applied.
Outbound settings are processed using the outbound email policy.
6. Use the Flow Guard settings to determine how many emails the user can send.
7. Determine whether the name of this user should be used for the [CxO Fraud Detection](#)
8. Select the languages for email notifications and email hints.
9. (Optional) Edit the additional user fields available for this user.
10. Determine which De-Mail functions should be available for this user.
11. Click **Finish**.

| Automating the user import

You can automate the import of user data by setting up multiple user imports in the Intranet Role. This enables you to keep the corporate users in the NoSpamProxy Gateway Role differentiated and up-to-date.

As source, either

- an on-premises Active Directory,
- an Azure Active Directory,
- a generic LDAP source,
- or a text file

can be used.



NOTE: Not all Active Directory attributes are synchronised with NoSpamProxy in all scenarios. The same behaviour occurs with the additional user fields. If the automatic user import is configured to use the "Global catalogue", only a few attributes are provided by the Active Directory. To access missing attributes, you must switch the import to use the default domain controller or a specific server. For more information, see the [Microsoft documentation](#).

New user import via on-premises Active Directory

1. Go to **Identities > Corporate users > Corporate users**.
2. Click **Automatic user import** and click **Add**.
3. Select **Active Directory** as the type of user import.
4. Under **General**, specify a unique name, the update cycle and the status of the user import.

5. Select the type of server and the user who is allowed to access it.



TIP: The Active Directory search selects the users to be imported. Here you can filter for specific containers, e.g. `OU=sales, OU=user, DC=domain, DC=DE`. In most cases, you will want to import all the users' email addresses. You can also restrict the import to the primary address by selecting the option on this page.



NOTE: If you want to enter a specific domain controller, you can enter an IP address or a server name. When the integrated Windows Authentication is selected, NoSpamProxy uses the network service if it is installed on a domain controller. Otherwise, the computer account is used for authentication.

6. (Optional) Specify an additional LDAP filter.
7. Select whether you want to encrypt the connection using TLS.
8. Select the type of authentication and enter the login data.
9. Select the scope and which addresses are to be imported (all or only primary addresses).
10. Under **Groups**, specify which functions each local user who has been imported may use. The functions depend on his group membership.
11. Click **Finish**.

New user import via Azure Active Directory

1. Go to **Identities > Corporate users > Corporate users**.
2. Click **Automatic user import** and click **Add**.
3. Select **Azure Active Directory** as the user import type.
4. Under **General**, specify a unique name, the update cycle and the status of the user import.
5. Provide a certificate for the AAD app registration by entering the following in PowerShell:

```
$newCertificate = New-SelfSignedCertificate -Subject "nospamproxy-userimport.example.com" -HashAlgorithm "SHA256" -KeyLength 4096 -KeySpec KeyExchange -NotAfter $((Get-Date).AddYears(30)) -KeyExportPolicy NonExportable
```
6. Give the Intranet Role read authorisation for the private key.
7. Use the certificate to create a new app registration in the AAD and assign the following permissions: **Microsoft Graph permission: Group.Read.All, User.Read, User.Read.All**
8. Switch to the NCC and enter your client name, the client ID and the certificate.
9. Under **Groups**, specify which functions each local user who has been imported may use. The functions depend on his group membership.
10. (Optional) Under **Additional user fields**, assign values from the directory to the additional user fields.
11. Click **Finish**.



NOTE: To set up automatic user import via Azure Active Directory in NoSpamProxy, NoSpamProxy must be registered as an app in the Azure portal. See [Registrieren von NoSpamProxy in Microsoft Azure](#).



NOTE: NoSpamProxy does not support public folders, as these are also no longer supported by Azure Active Directory.

New user import via generic LDAP

1. Go to **Identities > Corporate users > Corporate users**.
2. Click **Automatic user import** and click **Add**.
3. Select **Generic LDAP** as the type of user import.
4. Under **General**, specify a unique name, the update cycle and the status of the user import.
5. Enter the server and port and select the type of authentication.
6. Enter the Search Root and the class name under which the groups can be found.



TIP: You can restrict the search to users with certain properties by applying a filter. You can also restrict the LDAP search in the directory to certain containers.

7. Under **LDAP address fields**, specify additional LDAP fields to search for email addresses. This is necessary if your system does not store the email addresses in the default fields **mail** or **otherMailBox**.
8. Under **Groups**, specify which functions each local user who has been imported may use. The functions depend on the respective group membership.
9. Click **Finish**.



TIP: The **additional user fields** of a user can be filled with values directly by the user import. See **DISCLAIMER** to learn how to configure additional user fields within an automatic user import.

New user import via text file

1. Go to **Identities > Corporate users > Corporate users**.
2. Click **Automatic user import** and click **Add**.
3. Select **Text file** as the type of user import.
4. Under **General**, specify a unique name, the update cycle and the status of the user import.
5. Specify the path to the file that contains the user addresses.
6. Under **Content filtering**, select the policies for inbound and outbound emails.
7. Click **Finish**.



NOTE: The text file does not require a special format. All email addresses are found and imported regardless of format.



NOTE: If you have a license for NoSpamProxy Large Files or NoSpamProxy Protection, you can also select a content filter for all users to be imported here. The content filters are configured under

New group in user import



NOTE: To enable functions for user groups, an Active Directory connection or LDAP connection must be configured.



NOTE: The scope of Active Directory groups must be of the type **Universal**. For more information, see the [Microsoft documentation](#).

Proceed as follows:

1. Search for the group you want to authorize and select it.



NOTE: If you have licensed NoSpamProxy Large Files or NoSpamProxy Protection, you can select the ones used for each group.

2. Select the content filter settings for inbound and outbound emails.
3. Set the hourly and daily limits for the Flow Guard.
4. Select whether you want to use all members of the group for CxO Fraud Detection.

5. Specify which De-Mail functions are made available to the members of this group.



NOTE: All users who want to use De-Mail need a De-Mail address. You can have these created using the address management according to a replacement pattern or manually using an address rewriting. A warning is displayed in the event log for users who do not have a valid De-Mail address. If the members of the group are not allowed to send De-Mails, this dialog cannot be used.

6. (If De-Mail is available) Select whether the address rewriting is to be created automatically according to the stored pattern or manually via the address rewriting node.



NOTE: If you want to have the address descriptions created automatically, you can either have individual entries created or use the group mailbox functionality. For individual entries, a unique De-Mail address is generated for each user for his primary email address. To do this, you define a template in the dialog according to which the address is to be created.

7. (If De-Mail is available) Use one of the predefined replacement templates and customise it if you do not want to create the replacement entry completely manually. Alternatively the group mailbox functionality can be used.
8. Click **Finish**.



WARNING: Email addresses are only imported if the domain is also stored in the corporate domains of NoSpamProxy. All others are not imported.

Available replacement entries are available for the individual entries in the automatic creation of address rewritings:

First name %g| When using '%g', the first name of the user is used. For example, for the user 'Jane Doe' the first name 'Jane' is inserted.

First letter of first name %1g| When using '%1g', the first letter of the user's first name is used. You can also use other numbers instead of '1' to use several letters of the surname. For example, for the user 'Jane Doe' the part 'Ja' of the first name is inserted when using '%2g'.

Last name %s| When using '%s', the last name of the user is used. For example, for the user 'Jane Doe' the surname 'Doe' is inserted.

First letter of last name %1s| When using '%1s', the first letter of the user's last name is used. You can also use other numbers instead of '1' to use several letters of the surname. For example, for the user 'Jane Doe', when using '%3s', the 'Doe' part of the surname is inserted.

Local part %p| When using '%p', the local part of the primary email address is used. For example, for the address 'jane.doe@example.com' the local part 'jane.doe' is inserted.

Domain without TLD %c| When using '%c', the domain of the primary email address is used without the top-level domain such as '.de', '.net', '.com' etc. For example, for the domain 'example.com' the domain name 'example' is inserted.

Setting up address rewriting



The address rewriting rewrites the email address of a company user to a different email address. This allows corporate users to contact external email recipients through email addresses other than their own. The email will appear to have been sent from the rewritten address.

For emails to local addresses, the system verifies whether the recipient is an entry from the external addresses of the address rewriting. The address is then sent to the local address of the entry.

Other use cases are so-called group mailboxes. In this case, different local email addresses are rewritten to one address. e.g. `info@example.com`.

Proceed as follows:

1. Go to **Identities > Corporate users > Corporate users**.
2. Double-click the user for whom you want to set up address rewriting or select the user and click **Modify**.
3. Switch to the **Email addresses** tab.
4. Double-click the email address you want to rewrite or highlight it and click **Modify**.
5. Switch to the **Address rewriting** tab and click **Add**.
6. Enter the following:
 - an external address that is used for sending.
 - the behaviour when receiving emails for the external address.

7. Click **Next**.
8. Specify the scope for which the external address is used.
9. Click **Finish**.

■ Configuring default settings for users

Here you define which global settings are applied for users if no settings are configured for individual users.

1. Go to **Identities > Corporate users > Default user settings**.
2. Click **Modify**.
3. Select the desired behaviour of the content filter for inbound emails (Inbound filter) and outbound emails (Outbound filter).



NOTE: Note that content filters configured for partners are also applied. For emails received from the Internet, the content filters of the partner and each individual local recipient are combined. The most restrictive settings are then applied. Outbound settings are processed using the outbound email policy.

4. Select the desired behaviour of the Flow Guard.
5. Select the languages for email notifications and email hints.



NOTE: Email notifications are displayed in all languages.

6. Click **Save and close**.

Adding additional user fields



This feature is available if you have purchased a corresponding licence.

You can add additional fields to the data of your company users. You can then insert these fields as placeholders in your disclaimer templates. When attaching the disclaimer to emails, these placeholders will then be replaced by the inserted values.

Additional user fields

You can specify additional fields for your corporate users. These fields can be used in the Disclaimers as placeholder. You can map values to these fields on manually created users or via the automatic user import.

Name	Default value	Field type
City		Standard
Company		Standard
Country		Standard
Department		Standard
Email		Standard
FaxNumber		Standard
GivenName		Standard
MobilePhone		Standard
State		Standard
Street		Standard
Surname		Standard
Telephone		Standard
Title		Standard
ZipCode		Standard

[Add](#) [Modify](#) [Remove](#) [Create default fields](#)

1. Go to **Identities > Additional user fields > Additional user fields**.
2. Click **Add**.
3. Enter a name for the field.

4. (Optional) Enter a default value. This value is used if no value is set on the user itself.



TIP:

For most applications, it is recommended to select **Create default fields**. This creates frequently used fields. When the fields are created, the user fields are automatically assigned to Active Directory fields. You can adjust this assignment manually later.

Default values are used if the user is not assigned their own values. In the field for the telephone number, for example, the number of the head office can be entered, in the field for the email address the email address of the head office.

See [Automating the user import](#).



NOTE:


- Placeholders based on custom user fields are represented in the template editor with an asterisk (*), for example **[*CustomUserField]**. Exceptions are placeholders in templates created with NoSpamProxy version 13.2 or smaller.
- Placeholders based on custom user fields are not localised.

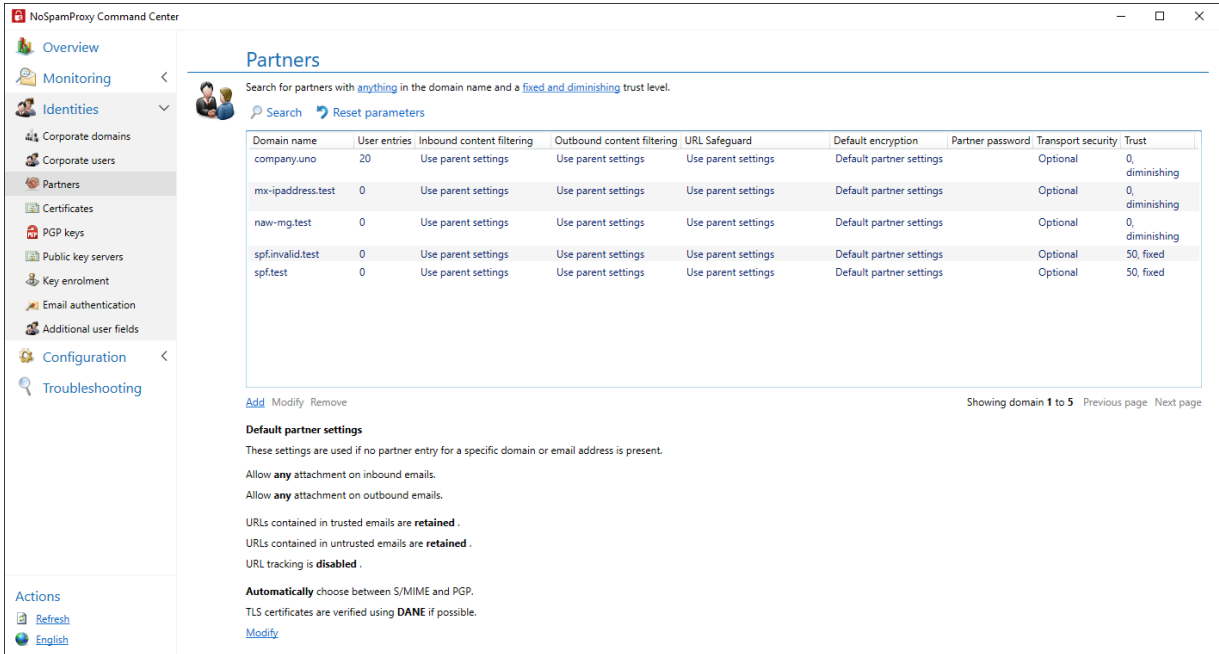


NOTE: For manually created users, you can edit the fields defined here directly on the user object. If you import your users from a remote system, you can use an automatic user import to define how these fields are filled. If required, you can specify a default value. This value is used if no value is set on the user itself. See [Automating the user import](#).

Partners

Partners are external communication partners with whom you exchange emails. Settings for partners can be made on the respective partners, the associated partner domain or the respective email address of the partner. The list of partners is grouped according to the respective domains.

 **NOTE:** The settings on an email address take precedence over the settings on a domain. Likewise, the settings on a domain have priority over the settings for all partners.



The screenshot shows the 'Partners' page in the NoSpamProxy Command Center. The left sidebar contains navigation options: Overview, Monitoring, Identities (with sub-items: Corporate domains, Corporate users, Partners, Certificates, PGP keys, Public key servers, Key enrolment, Email authentication, Additional user fields), Configuration, and Troubleshooting. The main content area is titled 'Partners' and includes a search bar and a 'Reset parameters' button. Below this is a table listing partner domains and their settings.

Domain name	User entries	Inbound content filtering	Outbound content filtering	URL Safeguard	Default encryption	Partner password	Transport security	Trust
company.uno	20	Use parent settings	Use parent settings	Use parent settings	Default partner settings	Optional	0, diminishing	
mx-ipaddress.test	0	Use parent settings	Use parent settings	Use parent settings	Default partner settings	Optional	0, diminishing	
naw-mg.test	0	Use parent settings	Use parent settings	Use parent settings	Default partner settings	Optional	0, diminishing	
spf.invalid.test	0	Use parent settings	Use parent settings	Use parent settings	Default partner settings	Optional	50, fixed	
spf.test	0	Use parent settings	Use parent settings	Use parent settings	Default partner settings	Optional	50, fixed	

Below the table, there are links for 'Add', 'Modify', and 'Remove'. A status indicator shows 'Showing domain 1 to 5'. The 'Default partner settings' section explains that these settings are used if no partner entry is present for a specific domain or email address. It lists several rules: allowing any attachment on inbound and outbound emails; retaining URLs in trusted emails and disabling URL tracking; and automatically choosing between S/MIME and PGP, with TLS certificates verified using DANE if possible. A 'Modify' link is provided at the bottom.



Automatic removal of partners

Partners are automatically removed when the Level of Trust value of the respective domain has dropped to 0 **and** the partner does not have any other properties that prevent this, such as stored users, passwords or certificates.

Related steps

Determining the default behaviour | You configure the basic behaviour for trusted and untrusted emails under [Default partner settings](#).

Adding a new partner domain | To create a domain for a partner, create it in NoSpamProxy. See [Adding partner domains](#).

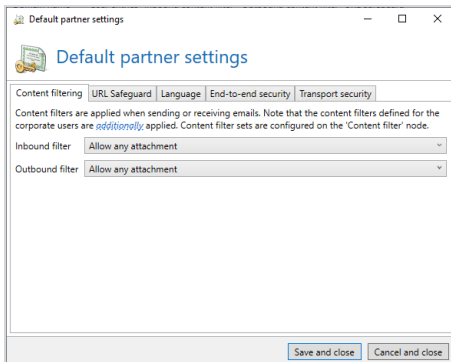
Adding users | Add new users of a domain to the corresponding domain as a user entry. See [Adding user entries to partner domains](#).

Default partner settings

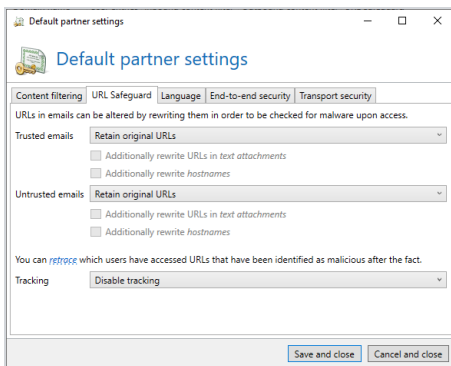
Under **Identities > Partners > Default partner settings** you configure settings that are applied when there are no partner entries for a domain or email address.

- Click **Modify** to open the **Default partner settings** dialog.

Content filtering | Select a policy for email attachments on both inbound and outbound emails. Content filters are configured under **Content filters**.

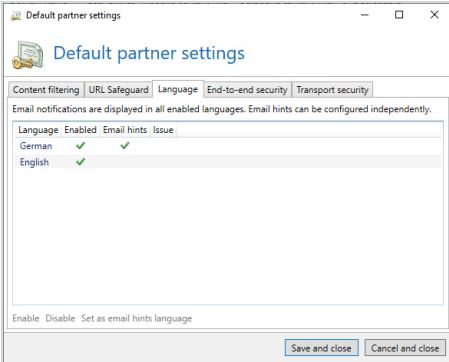


URL Safeguard | Configure the basic behaviour of URL Safeguard for trusted and untrusted emails. Also determine whether the URL tracking should be switched on or off.

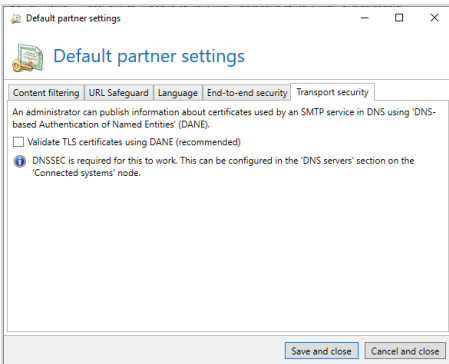


TIP: URL tracking allows you to see which users accessed URLs that turned out to be malicious **after the fact**. Details can then be found on the **URL Safeguard** tab of the respective message track. See [URL Tracking](#).

Language | Select the languages for email notifications and email hints.



Transport Security | Configure the use of a DNSSEC-enabled DNS server.



NOTE: By using DNS-based Authentication of Named Entities (DANE), the TLS certificates of the transport encryption are checked, so that only certificates that the recipient of the email has classified as trustworthy are accepted. In order to secure TLS certificates via DANE, you must configure a DNSSEC-compatible Connected systems under DNS Servers.

Adding partner domains

Each partner domain contains settings for Content filters, the necessary transport security and the trust between the domains.

1. Go to **Identities > Partners > Partners** and click **Add**.
2. Enter the name of the partner domain.
3. Select the settings for content filters for inbound and outbound emails.
4. Select the settings for the URL Safeguard.



Details on the configuration options can be found under [URL Safeguard](#).

5. Select the languages for email notifications and email hints.
6. Choose the transport security for this domain. The transport security determines whether the communication to the servers of the partner domain must be encrypted and which certificates are trusted, if necessary.



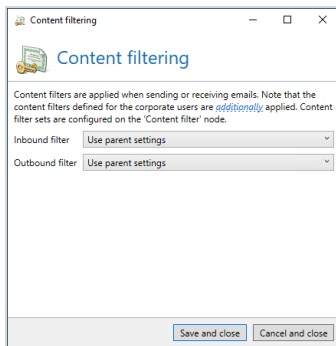
NOTE: You can also store additional certificates here that can be used for transport encryption to the target server. To deactivate transport security, untick all check boxes.

7. Specify the trust in this domain. The trust in a domain becomes stronger through emails sent to the domain and approaches 0 again over time without further email communication. You can also set the trust to a fixed value. See [Level of Trust](#).
8. Click **Finish**.

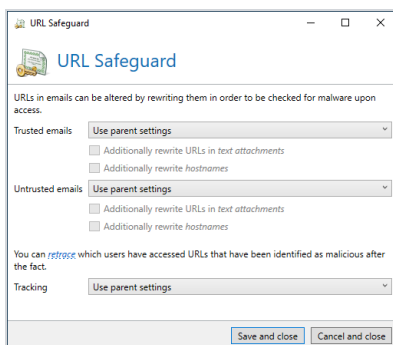
| Editing partner domains

1. Go to **Identities > Partners > Partners**.
2. Double-click the domain you want to edit and stay on the **Domain entry** tab.

3. Select the settings for **Content filters** for inbound and outbound emails.



4. Under **URL Safeguard**, configure the basic behaviour of the URL Safeguard for trusted and untrusted emails. Also determine whether the URL tracking should be switched on or off. You can find our recommended settings at **Recommended partner settings for the URL Safeguard**.



TIP: URL tracking allows you to see which users accessed URLs that turned out to be malicious **after the fact**. Details can then be found on the **URL Safeguard** tab of the respective message track. See [URL Tracking](#).

5. Select the languages for email notifications and email hints.

6. Specify the trust in this domain. Trust in a domain is strengthened by emails sent to the domain and approaches 0 over time without further email communication. You can also set the trust to a fixed value. See [Level of Trust](#).
7. Click **Close dialog**.

Recommended partner settings for the URL Safeguard

We recommend the following partner settings for the URL Safeguard:

Trusted emails| Retain original URLs

Untrusted emails| Rewrite URLs

Track URL access|

For **maximum security** we recommend the following settings:

Trusted emails| Rewrite URLs and block access, Additionally rewrite URLs in text attachments, Additionally rewrite host names

Untrusted emails| Rewrite URLs and block access, Additionally rewrite URLs in text attachments, Additionally rewrite host names

| Adding user entries to partner domains

1. Go to **Identities > Partners > Partners** and click **Add**.
2. Double-click the domain to which you want to add a user entry.
3. Switch to the **User entries** tab and click **Add**.
4. Enter the email address for the new user.
5. Select the settings for content filters for inbound and outbound emails.

6. Select the settings for the URL Safeguard.



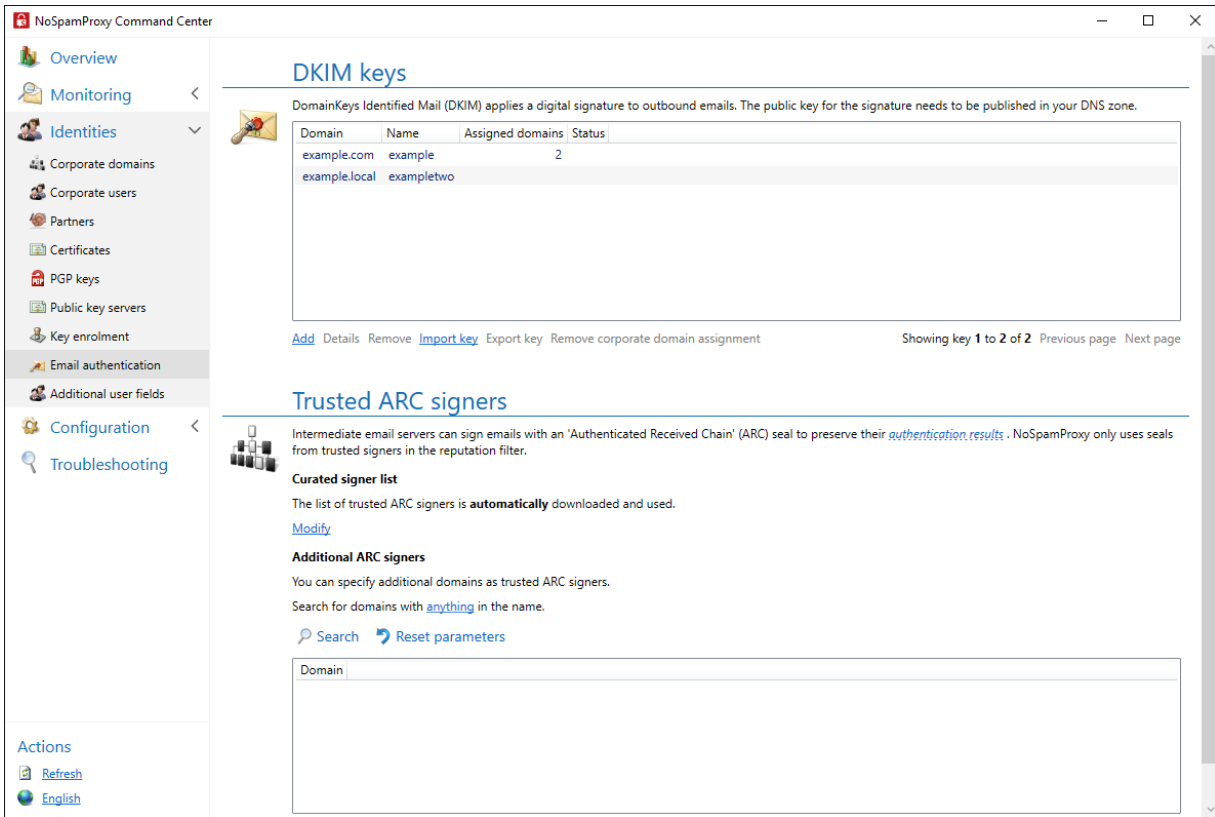
Details on the configuration options can be found under [URL Safeguard](#).

7. Click **Finish**.



NOTE: A user entry is associated with an email address and overrides the settings on the domain when communicating with that email address.

Email authentication



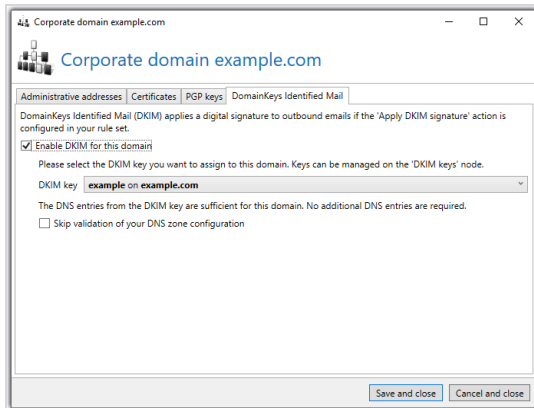
DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) secures outgoing emails with an electronic signature. By evaluating this signature, the recipient can see whether the email was sent from the correct domain (ensuring authenticity) and whether it was modified during transport (ensuring integrity).

Activating DKIM

You can create the keys required for this process under **DKIM keys**. The secret private part of the asymmetrical key is stored securely in the NoSpamProxy settings and is therefore only known to you.

1. Go to **Identities > Corporate users > Corporate users**.
2. Double-click the domain you want to edit.
3. Switch to the **DomainKeys Identified Mail** tab.
4. Activate **DKIM** for the domain.



5. Select one of the already created keys from the list of DKIM keys.



NOTE: If the domain of the DKIM key is identical to the domain you have now configured, the DNS entry you published when you created the key will suffice. If the domains are different, the configuration page will display another necessary DNS entry. If you need to publish more DNS entries, NoSpamProxy prepares the required entry so that you can copy it to the clipboard to publish it to the DNS. The DKIM configuration for this domain must then be terminated. When all necessary DNS entries have been published and are known on the Internet, please start the selection of the DKIM key again.



WARNING:

When publishing DNS records, it takes some time for all DNS servers on the Internet to receive these changes. Therefore, wait at least 24 hours after changing your DNS entries before checking and applying them. If you activate DKIM and your DNS configuration is incorrect, emails can no longer be delivered to recipients who evaluate DKIM signatures.

The DKIM signature requires the action **Apply DKIM signature**. This allows you to use DKIM for part of your emails and suppress DKIM for another part through differently configured rules.



NOTE: If an internal DNS server is configured for the Intranet Role that does not resolve to the Internet, the DKIM entries must also be created on this DNS server.

DKIM keys

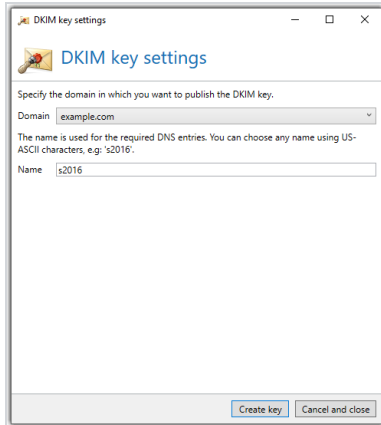
DomainKeys Identified Mail (DKIM) secures outgoing emails with an electronic signature. By evaluating this signature, the recipient can see whether the email was sent from the correct domain (ensuring authenticity) and whether it was modified during transport (ensuring integrity).

DKIM-signed emails can also be read by email recipients who cannot evaluate the DKIM signature. For these recipients, DKIM-signed emails look exactly the same as emails without a DKIM signature.

When you add a new DKIM key, the required asymmetric key pair is generated by NoSpamProxy for you. The secret private part of the asymmetrical key is stored securely in the NoSpamProxy settings and is therefore only known to you.

Adding DKIM keys

1. Go to **Identities > Email authentication > DKIM keys**.
2. Click **Add**.



DKIM key settings

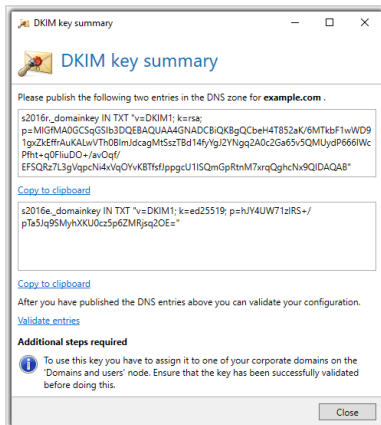
Specify the domain in which you want to publish the DKIM key.

Domain

The name is used for the required DNS entries. You can choose any name using US-ASCII characters, e.g. 's2016'.

Name

3. Specify the domain where you want to publish the DKIM key.
4. Specify a selector.
5. Click **Next**.
6. Publish the two entries shown to the DNS zone of the respective domain.



DKIM key summary

Please publish the following two entries in the DNS zone for **example.com**.

```
s2016r._domainkey IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCgsqSlb3DQEBAQUAA4GNADCBiQKgQCbeH4T852aK/6MTkbF1wWD9
1gxZKEHrAuKALwVTh0BlmJdcagM5SzT8d14fyIglZlYNgq2A0c2Ga65v5QMUYdP666IWc
PfhH-gOfIuDO-/avOqf/
EFSQRz7L3gVqpcN4xVqOYvKBTfslppgcU1ISQmGpRtnM7xrgQghNv9QIDAQAB"
```

[Copy to clipboard](#)


```
s2016e._domainkey IN TXT "v=DKIM1; k=ed25519; p=hjY4UW71zIRS-/
pTz51q95MyhXKU0cz5p6ZMRjsq2OE="
```

[Copy to clipboard](#)

After you have published the DNS entries above you can validate your configuration.

[Validate entries](#)

Additional steps required

 To use this key you have to assign it to one of your corporate domains on the 'Domains and users' node. Ensure that the key has been successfully validated before doing this.

7. Click **Finish**.



NOTE: To use the DKIM key, you must activate it under Corporate domains. Before doing so, make sure that the verification of the key is successful.



TIP: Alternatively, you can create your own RSA key with OpenSSL, for example, and import it using the corresponding button.

Enabling DKIM for corporate domains

You will need to activate the DKIM keys you create for your corporate domains. See Email authentication.

Importing DKIM keys

1. Go to **Identities > DKIM keys > DKIM keys**.
2. Click **Import key**.
3. Select the key on your hard disk and click **Open**.
4. On the following page, select the corporate domain where you want to publish the key.
5. Assign a name for the selector and click **Next**.
6. Follow the instructions on the next page.
7. Click **Finish**.

Exporting DKIM keys



TIP: We recommend that you export the DKIM key so that you can recover it in case of data loss. You can do this using the **Export key** button. The key is stored in PKCS#8 format.

How to use DKIM version 13 or higher

Starting with version 13, NoSpamProxy generates two DKIM keys, one in RSA format and one EdDSA format (Edwards-Curve Digital Signature Algorithm). The RFC for this can be found at <https://tools.ietf.org/html/rfc8463>.

DKIM-Schlüssel

DKIM-Schlüssel

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

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

[In die Zwischenablage kopieren](#)

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

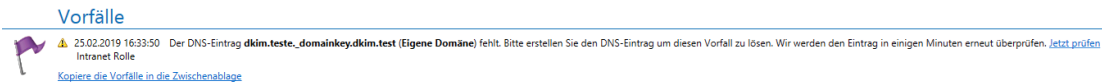
[Eintrag validieren](#)

Schließen

In the example the "key2018r" is in RSA format as before. The "key2018e" is new with version 13 and must be published in the DNS as well.

Upgrading to NoSpamProxy Version 13

After an upgrade to version 13 the EdDSA key is automatically generated in addition to the existing keys. The following incident is also displayed on the console home page "The DNS entry dkim.teste._domainkey.dkim.test (My Domain) is missing. Please create the DNS entry to solve this incident. We'll check the entry again in a few minutes."



Emails are considered valid as long as one of the applied DKIM keys has been successfully validated. It is unproblematic if the DKIM key is used in EdDSA format but has not yet been released. However, this should nevertheless be implemented promptly.

If an internal DNS server is configured for the Intranet Role that does not resolve to the Internet, the DKIM entries must also be created on this DNS server.

Creating a new key pair

Starting with version 13, greater encryption security (2048bit) is used for the RSA key, making the key larger than the 255 characters allowed in the DNS. To do this, the generated key must be correctly wrapped when it is included in the DNS. To do this, use the double quotation mark (") and wrap accordingly there, so that the first part contains less than 255 characters.

Generated key in NoSpamProxy (without wrap):

```
"v=DKIM1; k=rsa;  
  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
```

```
EAvzf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstllgGY
XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw
P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy
J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH6kQ+SEc
a0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6FpneHXCfAY6m
OI6vykmkVfb/MAR9CZFKrWY+17dPHDhKJDEwsQymCGUu
GwzLwIPcjLVbMSQGxrtWy8cJbeOa+iO2Gwp4yS2urmT
/k8aK4256GhSQbBH3HOCxRgNL3Yb4G1mo92QIDAQAB"
```

Key to be used in DNS (with wrap)

```
"v=DKIM1; k=rsa;
p=MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
EAvzf5N0hu8i4wM5quF3e5otVwN/IhKeoEEbkstllgGY
XSZQ+Tc7tJmkn/QyD8rvTWhAdmrLPfsDt2GwCkKBlupw
P7mtyQYR8bzw2fPCiUMW+Y7FyfRJSAFhRwykkrG1JbCy
J5Phn8qRYH4Rq1lo8BavEr7+/MeEf/CR1gdXH"
"6kQ+SEca0M/2OJjoHOLdmvsyb9qnBa5HB58DQr6Fpne
HXCfAY6mOI6vykmkVfb/MAR9CZFKrWY+17dPHDhKJDEw
sQymCGUuGwzLwIPcjLVbMSQGxrtWy8cJbeOa+iO2Gwp
4yS2urmT/k8aK4256GhSQbBH3HOCxRgNL3Yb4G1mo92Q
```


IDAQAB"

Backing up the DKIM keys

Before each update of the NoSpamProxy system to a new version, or during normal backups, the current DKIM key should be exported and backed up. The key can be exported under "Identities > DKIM Keys" and also imported again in case the system is restored.



NOTE: Some DKIM validation tools still produce an error with DKIM keys in the new EdDSA format because they expect only RSA formats. Recommended tools are e.g. MXToolBox <https://mxtoolbox.com/dkim.aspx>

See also

- [DKIM keys](#)

Configuration

This section provides access to settings for connecting to other roles, database settings and notification addresses.

Setting up email routing	92
Adding corporate email servers	92
Creating inbound connectors	97
Creating outbound send connectors	99
Creating receive connectors	105
Invalid requests for SMTP receive connectors	106
Queued delivery	108
Setting up header-based routing	110
Creating rules	111
General Information	111
Steps in creating rules	113
Related topics	118
NoSpamProxy components	121
Intranet Role	122
Gateway Role	123
Web Portal	132
Databases	141
How to change the WebPort for NoSpamProxy	159
Connected systems	162
DNS Servers	163
Archive connectors	164
De-Mail via Mentana-Claimsoft	167
CSA Certified IP List	168

User notifications	170
Inspection report	170
Email notifications	172
How to customise NoSpamProxy notifications	173
Procedure after updates	173
Using different designs for sender domains	180
Presettings	189
Branding	190
Word matching	191
Realtime block lists	193
Advanced settings	195
Sensitive data protection	196
Monitoring	197
Subject flags	200
Level of trust configuration	205
SMTP protocol settings	212
SSL/TLS configuration	218

Setting up email routing

The screenshot shows the NoSpamProxy Command Center interface. On the left is a navigation menu with options: Overview, Monitoring, Identities, Configuration (selected), Email routing (sub-selected), Rules, Content filter, URL Safeguard, NoSpamProxy components, Connected systems, User notifications, Presettings, Advanced settings, and Troubleshooting. Below the menu are 'Actions' with 'Refresh' and 'English' buttons.

The main content area is titled 'Corporate email servers' and contains a table with the following data:

Type	Details	Allowed domains	Comment
DNS name	localhost	Any	

Below the table are links: [Add](#) [Modify](#) [Remove](#) [Get Exchange configuration](#)

The next section is 'Inbound send connectors' with a table:

Type	Name	Assignment	Cost	DNS routing restrictions
SMTP	Default inbound connector	✓ INSTALLATION	100	From * to *

Links: [Add](#) [Modify](#) [Remove](#)

The next section is 'Outbound send connectors' with a table:

Type	Name	Assignment	Delivery method	Cost	DNS routing restrictions
SMTP	Default connector for outbound mails	✓ INSTALLATION	Direct delivery via DNS	100	From * to *

Links: [Add](#) [Modify](#) [Remove](#)

The final section is 'Receive connectors' with a table:

Type	Name	Assignment	Binding	Additional settings	Connection security
SMTP	SMTP on all addresses	✓ INSTALLATION	All : 25	Blocking is 30 minutes Tarptitting level is medium	⚠ Disabled

Links: [Add](#) [Modify](#) [Remove](#)

Adding corporate email servers

All email servers that are to use a corporate domain in the sender address of emails must be entered as corporate email servers in NoSpamProxy.

Add by IP address, subnet or DNS host name

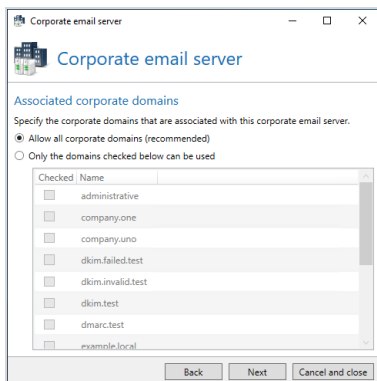
A server is here considered to be the company's e-mail server, provided that it

- sends from the specified IP address,
- sends from an address in the specified subnet or
- the DNS host name configured here points to the address of the server.



NOTE: A subnet is specified in the CIDR notation, e.g.
192.168.100/24

1. Go to **Configuration > Email routing > Corporate email servers**.
2. Click **Add**.
3. Select the **With an IP address, subnet or DNS host name** and click **Next**.
4. Enter the address of the server by specifying a fully qualified DNS host name, IP address, or subnet and click **Next**.
5. Determine which corporate domains are assigned to the server and click **Next**.

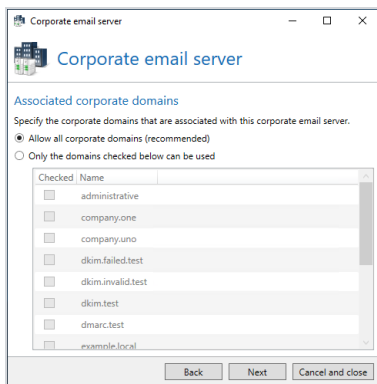


6. Enter a comment if required and click **Finish**.

Add as TLS-authenticated host

A server is considered a corporate email server if it performs TLS authentication with a client certificate during the connection. If a root or intermediate certificate is entered here, the server must log on with a certificate that contains the configured certificate in its certificate chain. If an end certificate is entered, the server must log on with this exact certificate.

1. Go to **Configuration > Email routing > Corporate email servers**.
2. Click **Add**.
3. Select **With a TLS client certificate** and click **Next**.
4. Click **Select Certificate** and highlight the certificate you want to use for authentication.
5. Click **Select and Close** and in the next dialog box click **Next**.
6. Determine which corporate domains are assigned to the server and click **Next**.



7. Enter a comment if required and click **Finish**.

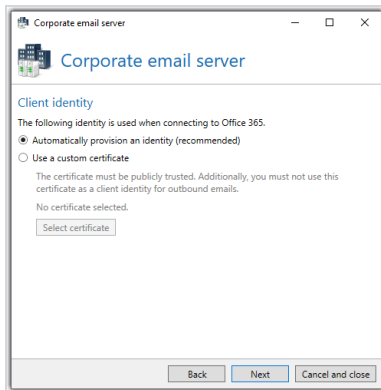
Add as Office 365 tenant

A server is considered a corporate email server here if it is an official Office 365 server.

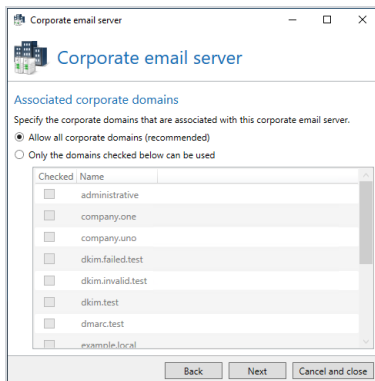


NOTE: If you configure Office 365 as the corporate email server, a send connector for Office 365 will be configured.

1. Go to **Configuration > Email routing > Corporate email servers**.
2. Click **Add**.
3. Select the **As Office 365 tenant** and click **Next**.
4. Enter your tenant name and click **Next**.
5. Configure the client identity used and click **Next**.



6. Determine which company domains are assigned to the server and click **Next**



7. Enter a comment if required and click **Finish**.

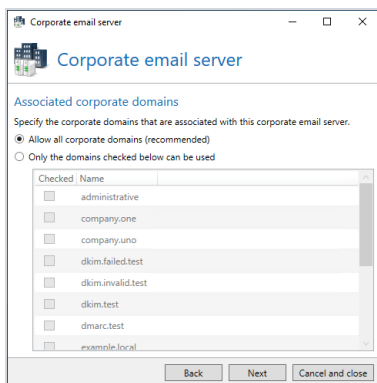


NOTE: By adding your Office 365 tenant, the required email routing is already created in NoSpamProxy Server. You now need to set up the message flow in Microsoft Exchange Online by running the provided PowerShell script or performing the setup manually. Highlight the entry for the Office 365 server and click **Show Exchange Configuration** to display the PowerShell script as well as further information.

Add via user name and password (SMTP AUTH)

A server is considered a corporate email server here if it uses a combination of user name and password for authentication.

1. Go to **Configuration > Email routing > Corporate email servers**.
2. Click **Add**.
3. Select **User name and password (SMTP AUTH)** and click **Next**.
4. Specify a user name, click **Copy to clipboard** and click **Next**.
5. Determine which corporate domains are assigned to the server and click **Next**.



6. (Optional) Enter a comment.
7. Click **Finish**.



NOTE:

- A TLS-secured connection is required to add servers with SMTP authentication.
- NoSpamProxy supports the **AUTH** and **LOGIN** authentication methods.

Add via a specific sender address

Any server that uses a 'MAIL FROM' address is considered a corporate email server.



WARNING: The 'MAIL FROM' address can be forged very easily. Only use this option if you have no other way to identify the server.

1. Go to **Configuration > Email routing > Corporate email servers**.
2. Click **Add**.
3. Select **With a specific sender address** and click **Next**.
4. Click **Add**.
5. Specify the address pattern you want to use for the sender address, click **Save and close** and click **Next**.
6. Enter a comment if required and click **Finish**.

Creating inbound connectors

Inbound emails are routed via inbound send connectors. If several connectors are suitable for routing an email, the most cost-effective one is selected.



NOTE: The option for direct delivery to the local email server is obsolete and is no longer available in NoSpamProxy since version 13. Delivery via queues is always applied.

1. Go to **Configuration > Email routing > Inbound send connectors**.
2. Click **Add**.
3. Follow the instructions in the dialog box.
Please refer to the notes under Mehrfach verwendete Einstellungen bei Konnektoren.
4. Click **Finish**.



Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

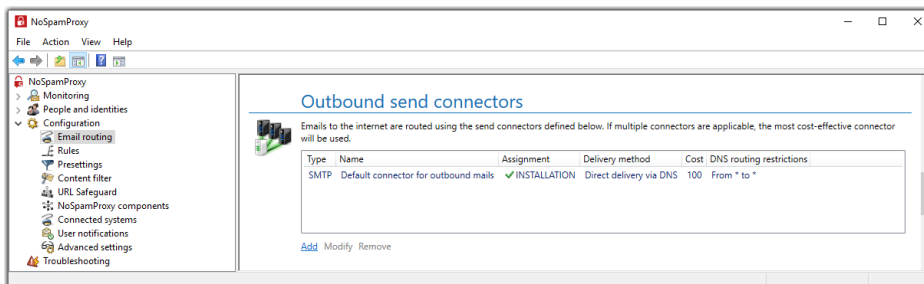
If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

Creating outbound send connectors

Outbound send connectors are used to send emails to external servers.





Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

Creating an SMTP send connector

1. Go to **Configuration > Email routing > Outbound send connectors**.
2. Click **Add**.
3. Select **SMTP** as type.

4. Follow the instructions in the dialog box.

Please refer to the notes under *Mehrfach verwendete Einstellungen bei Konnektoren*.

5. Click **Finish**.



Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

Creating an De-Mail via Mentana-Claimsoft GmbH send connector



NOTE: To connect to Mentana-Claimsoft De-Mail, you must set up a connection to Mentana-Claimsoft under Connected systems.

1. Go to **Configuration > Email routing > Outbound send connectors**.
2. Click **Add**.
3. Select **De-Mail via Mentana-Claimsoft GmbH** as type.

4. Follow the instructions in the dialog box.

Please refer to the notes under **Mehrfach verwendete Einstellungen bei Konnektoren**.

5. Click **Finish**.



Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

Creating a Deutschland-Online - Infrastructure (DOI) send connector

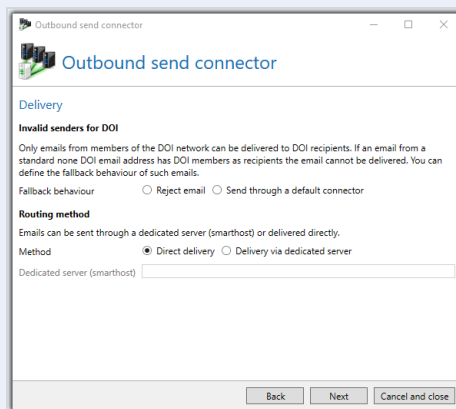
The Deutschland-Online - Infrastructure (DOI) project is used by local authorities, among others, for the secure transmission of messages.

1. Go to **Configuration > Email routing > Outbound send connectors**.
2. Click **Add**.

3. Select **Deutschland Online - Infrastruktur (DOI)** as type.
4. Follow the instructions in the dialog box.
Please refer to the notes under Mehrfach verwendete Einstellungen bei Konnektoren.
5. Enter the FTP or Web address from which you obtain the mailer table and click **Next**.
6. Configure the behaviour for invalid senders.



NOTE: Senders are always invalid if the sender domain is not part of the DOI network. These emails may not be delivered via the DOI network. You can choose whether these emails are returned to the sender or whether they are sent via a different connector with a higher Kosten level. You can also use this page to define how emails are delivered. On the one hand, the emails can be delivered directly, on the other hand, a smarthost can be used (which we recommend). Such a smarthost is provided by the DOI network.



7. Click **Finish**.



NOTE: When delivered via the DOI Network, the delivered email is described in message tracking as **not encrypted**. In this case, the email is encrypted via the DOI network and is thus delivered in a tap-proof manner. This protection is not listed under transport safety.



Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

Creating receive connectors

You can configure multiple receive connectors to receive email on different network cards, but also to implement different security requirements for email traffic. If you have a NoSpamProxy Encryption license, additional connectors for De-Mail and POP3 mailboxes are available.

Creating an SMTP receive connector

The SMTP receive connector defines on which IP address and which port emails are received by NoSpamProxy. It also determines how invalid requests from external email servers are handled and what connection security should be applied when transporting emails.

1. Go to **Configuration > Email routing > Receive connectors** and click **Add**.
2. Select **SMTP** as type.
3. Set the Gateway Roles of the receive connector, the IP address and the port of the connector. Please refer to the notes under Mehrfach verwendete Einstellungen bei Konnektoren.
4. For an address binding to a **specific address**, specify the IP address at which the connections are to be accepted.



NOTE: If you have selected multiple Gateway Roles, you cannot perform a binding to individual IP addresses. In this case select **All** or **Loopback**.

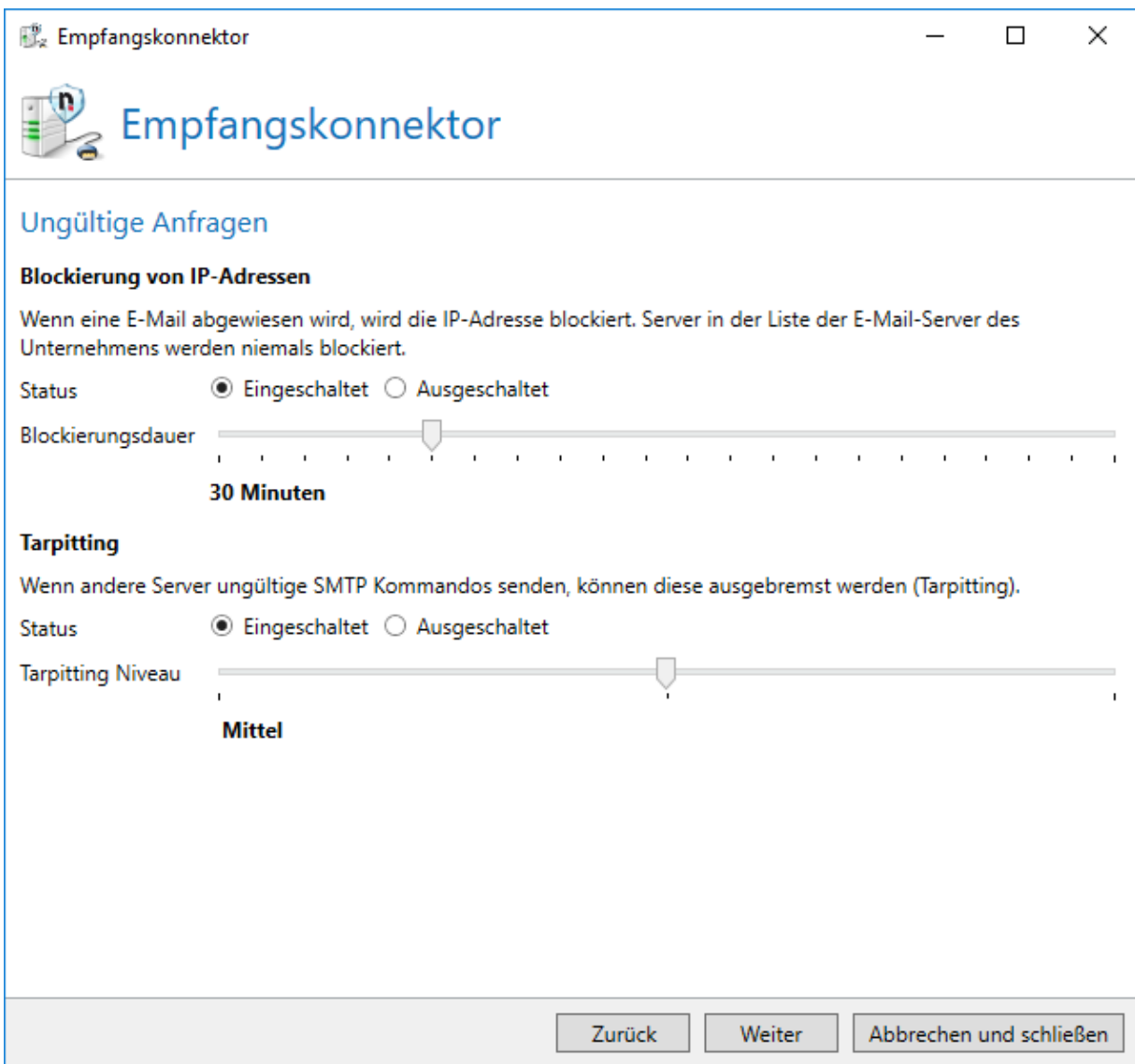
5. For **Port**, specify the port at which NoSpamProxy should receive emails and click **Next**.

6. Make the settings for invalid requests. Please refer to the notes under [Invalid requests for SMTP receive connectors](#).
7. Make the settings for connection security. Please refer to the notes under Mehrfach verwendete Einstellungen bei Konnektoren.
8. Click **Finish**.

I Invalid requests for SMTP receive connectors

Some participants on the Internet try to overload other email servers by sending invalid requests (so-called denial-of-service attacks) or exploit security holes to break into servers. In order to minimize these attacks, you can specifically slow down such requests, for example by using the so-called **tarpitting**.

Settings for invalid requests when configuring SMTP receive connectors



The screenshot shows a Windows-style window titled 'Empfangskonnektor'. The main content area is titled 'Ungültige Anfragen' (Invalid Requests). Under the sub-heading 'Blockierung von IP-Adressen' (IP Address Blocking), there is a descriptive text: 'Wenn eine E-Mail abgewiesen wird, wird die IP-Adresse blockiert. Server in der Liste der E-Mail-Server des Unternehmens werden niemals blockiert.' (When an email is rejected, the IP address is blocked. Servers in the list of company email servers will never be blocked.) Below this, the 'Status' is set to 'Eingeschaltet' (On) with a selected radio button. A slider for 'Blockierungsdauer' (Blocking duration) is positioned at the 30-minute mark, with the text '30 Minuten' displayed below it. The next section, 'Tarpitting', has a descriptive text: 'Wenn andere Server ungültige SMTP Kommandos senden, können diese ausgebremst werden (Tarpitting).' (When other servers send invalid SMTP commands, they can be slowed down (Tarpitting).) The 'Status' is also 'Eingeschaltet' (On). A slider for 'Tarpitting Niveau' (Tarpitting level) is positioned at the 'Mittel' (Medium) mark, with the text 'Mittel' displayed below it. At the bottom of the window, there are three buttons: 'Zurück' (Back), 'Weiter' (Next), and 'Abbrechen und schließen' (Cancel and close).

Blocking of IP addresses | The blocking serves to specifically slow down servers that have already been identified as spam senders. If a server sends an email to your NoSpamProxy and it is classified as spam, subsequent emails from the same sending server will be blocked for the specified time period.

A regular email sender will make a new attempt to deliver the email after this period.

A spammer is likely to abort delivery and focus on unprotected email recipients. Use the Blocking for suspicious IP addresses radio button to set or turn off the option to block suspicious IP addresses. With the slider for the Blocking period you can set the duration of the blocking from 5 minutes to one day (1440 minutes).

Tarpitting | Tarpitting is a method of slowing down email relays that do not follow the RFC for SMTP command sets and/or their correct order. As soon as an SMTP command is transmitted incorrectly or in the wrong place, NoSpamProxy waits five seconds with its response for each subsequent command. The transfer of the commands is thus artificially aggravated as if taking the route through a tar pit, hence the name tarpitting.

With the slider for the tarpitting level you can set by how many seconds NoSpamProxy Protection delays the response. If you set the slider to **Low**, the gateway will wait 2 seconds. **Medium** results in a 5 second delay and **High** results in a 10 second delay.

Queued delivery



NOTE: The option for direct delivery to the local email server is obsolete and is no longer available in NoSpamProxy since version 13. Delivery via queues is always applied.

NoSpamProxy first places the email in a queue after receipt and only then forwards the email to the configured smarthost(s). For the successful receipt of the email it is not relevant whether the next smarthost is available or not.



NOTE: If you select the queued delivery mode for the send connector, any existing configuration is replaced by the newly configured queued delivery mode. When you switch to queued delivery mode, the first SMTP connector is immediately configured.



NOTE: If you added to the local servers under [Adding corporate email servers](#), an Office 365 connector will be displayed here. This connector is responsible for delivering local emails to Office 365. Apart from being bound to certain gateway roles, you cannot modify or delete this connector.

Settings

General settings | Enter a name and select one or more Gateway Roles. Subsequently, determine the cost of the connector.

SMTP connections | You can configure multiple smarthosts under SMTP connections. An attempt will be made to deliver the email to one of the configured smarthosts in turn. The sequence is neither configurable nor can it be influenced by the user. As soon as a smarthost receives the email, the email has been successfully delivered.

Configuring the smarthost | The configuration of a smarthost for local delivery proceeds as described in the chapter Smarthost: Email Delivery via Dedicated Server. The send connector for local addresses uses a client identity for connection security.

DNS routing restrictions | You define the restrictions for the namespace managed by the connector under DNS routing restrictions. The configuration of the restrictions for local delivery is done as described under DNS-Routing-Einschränkungen durch Konnektor-Namensräume.

■ Setting up header-based routing

You can set up header-based routing in NoSpamProxy. With this, routing is not based on IP addresses or domains, but on entries in the header of emails.

To set up header based routing, please contact our [Support](#).

Creating rules

Each email must pass at least one of these rules. Rules are processed top-down until a match is found. A match is defined by the combination of source gateway, sender and receiver address. The first active rule is selected all subsequent ones are ignored. If no active match is found the email is rejected.

#	Enabled	Managed	Name	Sender scope	Recipient scope	IP filtering	Decision	Filters	Actions
..	✗		Outbound mails without signature and/or encryption	Corporate domain	External address	Disabled	Pass		
..	✓		All outbound mails	Corporate domain	Any address	Disabled	Check	Reject if SCL reaches 4	
..	✓		All other inbound mails	External address	Corporate domain	Disabled	Check	Reject if SCL reaches 4	

[Add](#) [Modify](#) [Remove](#) [Duplicate rule](#) [Reorder rules](#) [Generate default rules](#)

General Information

About rules

NoSpamProxy applies rules that you can configure individually when processing emails. These rules are modular in structure. You can create your own rules and modify existing rules by selecting the desired filters from the available filters for each individual rule. Within each rule you can weight and configure them as you wish using a multiplier.

You can also specify that rules apply only to certain IP addresses or recipients, for example, only to senders with a certain TLD (Top Level Domain) or to IP addresses from a certain subnet.



TIP: After reinstalling NoSpamProxy, a set of Related topics can be created after installing the licence. These enable the gateway to start functioning as quickly as possible with minimal administration effort. Nevertheless, you should check these rules and adapt them to your needs if necessary.

Rules and their order

If a rule is responsible for an email to be checked, it will be used. If more than one rule applies to an email, the rule that is highest in the list is applied.

Rules, filters and actions

- To process emails, NoSpamProxy applies rules that you can configure individually. For each email, the individual filters of the applicable rule are executed.
- Filters evaluate how strongly the email meets a certain filter criterion and award corresponding penalty and bonus points. The awarded points are weighted with the multiplier of the filters and then added to a total value. If this value exceeds the set Spam Confidence Level (SCL) of the rule, the email will be rejected. You can set the allowed SCL individually for each rule. See Filter konfigurieren and Filters in NoSpamProxy.
- Actions in NoSpamProxy are called up after the filters have determined whether the email is rejected or allowed to pass. Actions can, among other things, modify the emails, for example to add a footer or remove unwanted attachments. However, actions can also reject emails that would actually happen after they have been evaluated by the filters. This means that a virus scanner, for example, can still reject the email even though it has not been

detected as spam. Actions are therefore higher-level settings with which filters can be overridden if necessary. To find out which actions are available and how they work exactly, see [Actions available in NoSpamProxy](#).

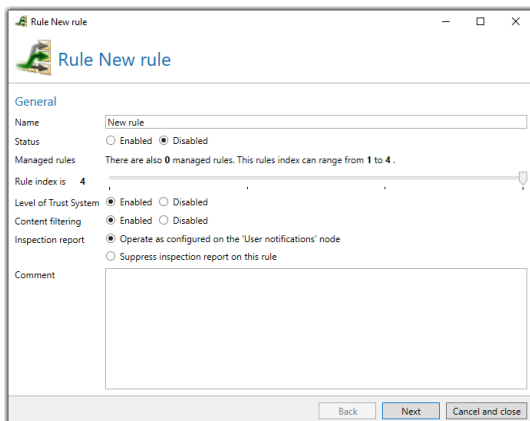
When are emails considered spam?

In the rules you configure various filters and actions. Filters evaluate emails and thereby influence the **Spam Confidence Level (SCL)** of the emails. The SCL determines whether emails are rejected if the inspection result exceeds a certain SCL.

Steps in creating rules

Step 1: Configuring general settings for rules

To create a new rule, go to **Configuration > Rules > Rules** and click **Add**. First, set the basic properties for the respective rule.



Name| Enter a unique name for the rule.

Status| Enable or disable the rule.

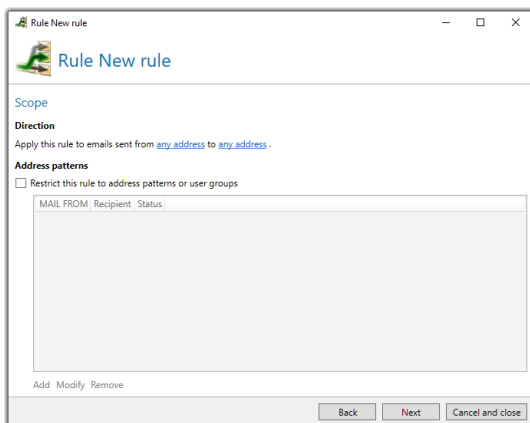
Rule index| Specify the position within the list of rules.

Level of Trust| Turn Level of Trust on or off. See [Level of Trust](#).

Content filtering| Enable or disable the content filter for this rule. See [Content filters](#).

Comment| Enter a comment if required.

Step 2: Configuring the scope of rules



Direction| Select for which sender and recipient the rule should apply.

Address pattern| Restrict the rule to certain address patterns or user groups.



NOTE: Use the MAIL-FROM domain or parts of it.



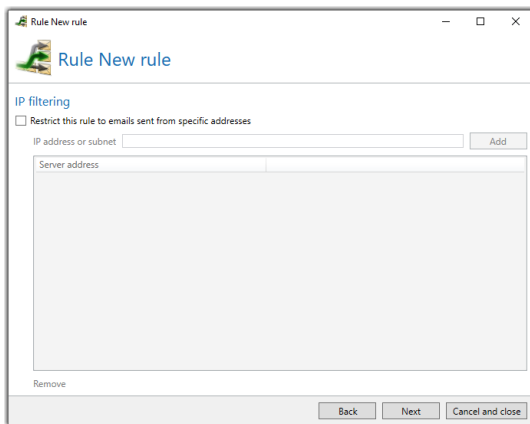
NOTE: The maximum number of configurable address patterns is 256.



NOTE: To get groups from a user directory, you must configure an automatic user import of LDAP or Active Directory users. Groups are available after the first synchronization has been performed. See [Automating the user import](#).

Step 3: Configuring IP filtering for rules

Here you can restrict the rule to certain submitting servers.



1. Tick the check box for **Restrict this rule to emails sent from specific addresses**.
2. Specify an IP address or subnet
3. Click **Add**.



NOTE: The maximum number of configurable address patterns is 256.

Next steps

If you are in the process of creating a new rule, select the filters now. See [Filter konfigurieren](#).

Step 5: Configuring actions

Here you select the actions that are triggered depending on the filter result.

Configuring the actions

1. Click **Add**.
2. Add the desired action to the rule by
 - double-clicking the respective action or
 - selecting them and clicking **Select and close**.



NOTE: Depending on the selected action you may have to further configure it. For details on the configuration options of each action, see the corresponding information. See [Actions available in NoSpamProxy](#).

3. Click **Next**.



NOTE: Some actions cannot be applied to the sender that is usually selected. In the Status column, the text **Only local (or external) senders are supported** is displayed. A rule containing invalid actions will not be saved.



NOTE: Adding an action to a rule based on the sender is only prevented if the rule would not have an effect when used in this direction. This restriction does not always represent the recommended use. This means that actions that are intended for a certain direction but also work in the opposite direction can be configured for both directions. In some cases, the recommended direction is part of the name of the action.

Step 6: Configuring rejection behavior

Here you configure how emails are treated that are rejected for reasons other than being suspected to be spam or malware.

The following basic options are available:

Reject and send a non-delivery report (NDR) for inbound emails. Discard and send NDR for outbound emails. | The receiving server refuses acceptance (SMTP message 5xx). As a result, the delivering server must generate a non-delivery report (NDR).

Discard and send NDR for outbound emails. | NoSpamProxy receives the email and sends a positive receipt to the sending server (SMTP message 200). The email is deleted immediately after acceptance; NoSpamProxy generates a non-delivery report and sends this to the delivering server.

Reject and send NDR for all emails. | NoSpamProxy rejects the email, generates a non-delivery report and sends it to the delivering server.

Reject all emails without sending NDR. | NoSpamProxy refuses to receive the email. The submitting server must generate a non-delivery report (NDR).

Changing the rule index

1. Open the rule.
2. Under **Rule index**, set the new position of the rule.
3. Click **Save and close**.

| Related topics

Default rules

Default rules make it possible to put NoSpamProxy into operation as quickly as possible and with minimal administrative effort. The configuration of the default rules is based on many years of operating numerous NoSpamProxy installations and represents a basic best-practice configuration.



NOTE: Nevertheless, you should check these rules and adapt them to your needs if necessary.

Creating default rules

You have two options for creating default rules:

- via the configuration wizard or
- under **Configuration > Rules > Rules**.

How NoSpamProxy Protection classifies emails as spam

In the rules you configure various filters and actions. Filters evaluate emails and thereby influence the **Spam Confidence Level (SCL)** of the emails. The SCL determines whether the email is rejected if the inspection result exceeds a certain SCL. See [Rules](#), [Filters in NoSpamProxy](#) and [Actions in NoSpamProxy](#).

- The higher the SCL, the higher the probability that the email is spam.
- The lower the SCL, the lower the probability that the email is spam.
- An SCL of 0 indicates that the email has been classified as neutral.
- The value range for the SCL extends from -10 and +10 points.

You can weight the filters differently within the rules using the multiplier. The weighting of the filter is calculated with the multiplier. This allows you to influence the influence of the individual filters within a rule. If this total weighting reaches the threshold value of the rule, the email is treated as spam and rejected.



TIP: The modular structure of the rules offers numerous possibilities for individual adaptation. In addition, the filter weighting with multipliers is crucial. For details on how the SCL is calculated, see [Spam Confidence Level \(SCL\)](#).

EXAMPLE:

You have created a rule with one active filter: the word filter. Also, Level of Trust is enabled for this rule. The word filter checks an email for unwanted expressions. Let us assume that an email contains a large number of unwanted expressions. The word filter will therefore sound the alarm on this email and deliver a high penalty value, for example 6. If the word filter were the only filter in this rule, the email would now have a total value of 6. For example, if you usually set the threshold value to 4, the email would now be blocked and rejected. The sender would receive a non-delivery report.

Keep in mind that Level of Trust is still activated in this rule. The email comes from a very reliable email partner with whom you have exchanged many emails. Level of Trust assigns -4 SCL points to this email.

The Level of Trust system always has a multiplier; this multiplier is composed of

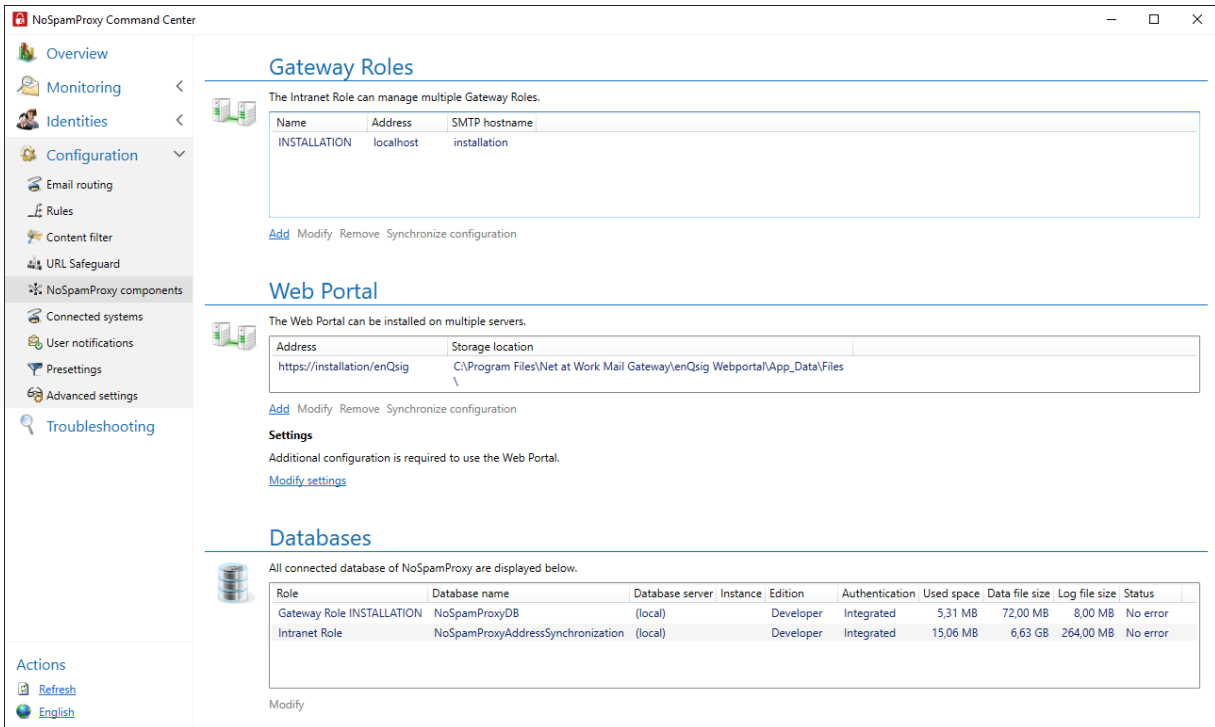
- the sum of the multipliers of all filters activated on the rule and
- the value 1, which is added to this sum.

This results in a factor of 2 in our example. The SCL value is therefore $6+2*-4$.

This results in an SCL of -2. The email would pass through NoSpamProxy Protection.

NoSpamProxy components

Here you configure the connections between the individual components of NoSpamProxy. Information on the selection of components can be found in the installation manual.



Configuration files for the roles

The configuration of NoSpamProxy is stored in an XML file on the server. This file can also be backed up using conventional backup software. However, NoSpamProxy writes this file back when the configuration is changed, so that a conflict can occur here during simultaneous backup.

NoSpamProxy creates the new file as a temporary file while writing the configuration, renames the original file, for example to *GatewayRole.config.backup*. Only then does NoSpamProxy rename the temporary file to *GatewayRole.config*.

With a normal, file-based backup, you have therefore always backed up either the most recent copy or the version of the configuration that was changed shortly before.



NOTE: We recommend that you save this file before making any changes to the configuration. This allows you to return to the previous state at any time.

Configuration files for the roles

Gateway Role | %ProgramData%\Net at Work Mail

Gateway\configuration\GatewayRole.config

Intranet Role | %ProgramData%\Net at Work Mail

Gateway\configuration\IntranetRole.config

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

I Intranet Role

The Intranet Role contains the entire configuration of NoSpamProxy and manages the cryptographic keys.

Setting up user notifications

To authorise other users to perform monitoring functions in NoSpamProxy, for example, you must assign these users corresponding roles.

1. Open the Windows computer management on the system on which the Intranet Role is installed.

2. Go to **Local Users and Groups > Groups**.

There you will find the following groups:

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

3. Assign the desired roles to the corresponding users.

4. Log out of Windows once and log in again with the corresponding user to use the added rights.

If the users are also to carry out updates at a later date, these users must be included in all groups and be authorised to manage the database of the respective role. See [How to set up database permissions](#).



NOTE: If NoSpamProxy has been installed on an Active Directory domain controller, there are no longer any local user groups. The groups can then be found there with the same names in the Active Directory.

| Gateway Role

The Gateway Role is the actual core of NoSpamProxy. It can either be installed on the same server as the Intranet Role or on a different server. Depending on your environment, this role can be installed either in a Demilitarized Zone (DMZ) or in the Intranet.

NoSpamProxy accepts the emails on port 25, checks them for spam and rejects them if necessary.



NOTE: To build a highly available system, several Gateway Roles can be installed on different servers. The current configuration is transferred from the Intranet Role to all connected Gateway Roles. See [Infrastruktur-Empfehlungen](#).

Adjusting the configuration

In some cases, the configuration of a Gateway Role may differ from that of the Intranet Role.

- Click **Synchronise configuration** to synchronize the configuration with the selected roles.



NOTE: Please note that the amount of data in the database of the Intranet Role will increase in the short term and can therefore lead to a full database. This is often the case when an SQL Express database is in use. The overfilling is normally reduced automatically.

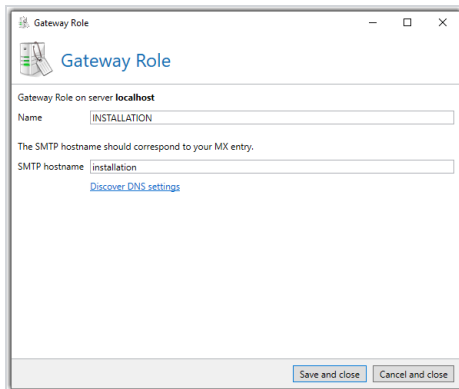
Server identity

When connecting to external servers, the client introduces itself to the received server with the HELO command or EHLO command followed by the server name.

EXAMPLE: EHLO mail.netatwork.com

Some servers check whether this name is resolvable by DNS. The resolvability of this name is specified in an RFC. If the name is not resolvable, some other email servers will consider this a spam feature. The FQDN, which can be resolved on the Internet, should be entered here. Usually the MX of the own email domain is entered here.

1. To change this setting, click **Modify** under **Server hostname**.



2. Specify a name under **SMTP Server Name**.



NOTE: You can also have the DNS name for your domain resolved automatically. The primary domain of your license is used for this purpose. Click **Find out** the DNS settings . A dialog will appear listing all available DNS identities for your domain in order of priority.

3. Click **Save and Close**.

Connecting to a Gateway Role



NOTE: If the Gateway Role is installed on a server outside your own domain, an integrated administrator account is required to establish the connection. This refers to the Windows account *Administrator*, not a self-created account with administrator rights.

1. Go to **Configuration > NoSpamProxy components > Gateway Roles** .
2. Click **Add**.
3. Specify your current installation configuration.
4. Perform one of the following two steps:
 - If both roles are on the same server
 - Click **Save and Close**.
 - If both roles are located on different servers
 1. Under
 1. Server **name and Port**, enter the name and port of the Gateway Role under which the Intranet Role can reach the Gateway Role.
 2. (Optional) If the NoSpamProxy Command Center and the Intranet Role require different connection information to connect to the Gateway Role, enable the appropriate radio button and specify the server name and port.
 3. Click **Save and close**.

Behaviour of connectors when adding Gateway Roles

Upon installation of the first Gateway Role, all inbound and outbound send connectors are automatically switched on.

If one or more additional Gateway Roles are added, the following (desired) behaviour occurs:

- Send connectors that were switched on on all existing roles are also switched on on the new roles.
- Send connectors that were switched off on one or more roles will not be switched on on the new roles.
- Receive connectors are not affected.

This behaviour prevents unwanted email traffic from being sent via a new Gateway Role whose configuration has not yet been completed.

How to query the Windows Performance Counter using PRTG

The following performance counters are available on the server with the NoSpamProxy Gateway Role and can be integrated into PRTG.

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

1. In PRTG select the device (Gateway Role Server).
2. Add a **PerfCounter Custom Sensor** using the right mouse button.

3. Restrict the search for the sensor to be created using **Custom Sensors/Performance Counters**.
4. The sensor name can be freely assigned
5. Under **List of Counters**, enter one of the above (copy and paste).



NOTE: The interval is inherited from the host by default, but it can also be defined (see below).

6. Click **Create**.

The screenshot displays a web-based configuration interface for creating a sensor. It is divided into two main sections: "Basic Sensor Settings" and "Performance Counter Settings".

Basic Sensor Settings:

- Sensor Name:** NoSpamProxy Queue momentan Aktiv
- Parent Tags:** new_nospamproxy, Windows, NSP, enqsig, SMTP, mail
- Tags:** performancecounter, performancecountercustom
- Priority:** ★★★★★
- Create:** A blue button with a plus icon is located on the right side of this section.

Performance Counter Settings:

- List of Counters:** %NoSpamProxy Queues(_total)\Currently active
- Mode:** Absolute (recommended), Difference

Scanning Interval: A section is visible at the bottom of the form, but its content is partially cut off.

Setting concurrent outbound connections

To change the number of outbound connections of the Gateway Role, proceed as follows:

1. Stop the Gateway Role for which you want to make the changes.
2. On the Gateway Role, go to **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

3. Open the file **Gateway Role.config**.
4. Add the following attributes below the tag

`<netatwork.nospamproxy.proxyconfiguration ... >`, in the tag `<queueConfiguration>`:

```
maxConcurrentConnections="NumberOfConnections"  
maxConcurrentConnectionsPerDomain="NumberOfConnections"<mtlingo  
type="
```

```
" prevChar="" nextChar="" />
```

5. Save the file.

This limits the number of concurrent connections to 100, whereby only a maximum of 10 simultaneous connections are permitted per domain.

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

Setting concurrent inbound connections

NoSpamProxy dynamically determines the number of parallel connections. The basis for this decision is the CPU and memory utilisation. To stop this behaviour, proceed as follows:

1. Stop the Gateway Role.
2. On the Gateway Role, go to **C:\ProgramData\Net at Work Mail Gateway\Configuration**.
3. Open the file **Gateway Role.config**.

4. Search for the line that begins with the following characters:

```
<netatwork.nospamproxy.proxyconfiguration...
```

5. Add the following value below this line:

```
<connectionLimits hardUpperConnectionLimit="NumberOfConnections"  
minimumNumberOfConcurrentSessions="NumberOfConnections" />
```

6. Save the configuration file.
7. Then start the Gateway Role.

If the values are not specified, as in this example, the dynamic limit applies (depending on the CPU load). Both values are integer values.

- With the value `hardUpperConnectionLimit` you set the maximum limit of connections.
- The value `minimumNumberOfConcurrentSessions` determines the minimum number of concurrent connections.

EXAMPLE:

```
<connectionLimits hardUpperConnectionLimit="100"  
minimumNumberOfConcurrentSessions="50" />
```

How to change the SMTP connection properties

1. Open the `Gateway Role.config` file in the directory "`C:\ProgramData\Net at Work Mail Gateway\Configuration\`.
2. Search for the following line:

```
<netatwork.nospamproxy.proxyconfiguration ... >
```

3. Add the following entry directly below this line:

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

4. Adjust the values to the desired value.



NOTE: Before you save the **Gateway Role.config** file, stop the **NoSpamProxy - Gateway Role** service. Only then can you save the configuration file properly.

Adjusting the delivery attempts and repeat intervals

The default settings are as follows:

- The first attempt is made after five minutes.
- The second attempt is made after ten minutes.
- The third attempt is made after 15 minutes.
- Each additional attempt is made every 30 minutes.
- The first delivery delay notification is generated after six hours.
- After one day, the delivery is stopped.

To make changes to the settings, proceed as follows:

1. Stop the Gateway Role.
2. Go to **C:\ProgramData\Net at Work Mail Gateway\Configuration** on all computers where Gateway Roles are installed.
3. Find the file **Gateway Role.config**.
4. Find the following line in the file:
`<netatwork.nospamproxy.proxyconfiguration ... >`
5. Add the following entry directly below this line if it does not already exist in a similar form:

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

6. Adjust the values as desired.
7. Save the file.
8. Restart the Gateway Role(s).

Web Portal

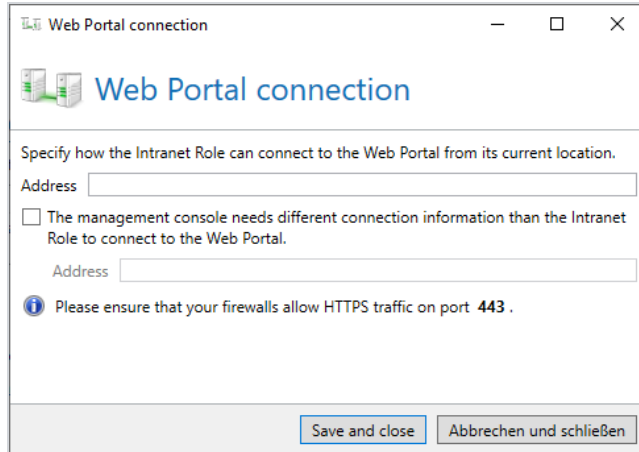


NOTE: To build a highly available system, the Web Portal can be installed on multiple servers.

Connecting Intranet Role and Web Portal

To use the Web Portal, you must first establish a connection between the Intranet Role and the Web Portal. You can then configure the individual features.

1. Go to **Configuration > NoSpamProxy Components > Web Portal**.
2. Click **Add**.



The screenshot shows a dialog box titled "Web Portal connection" with a standard Windows window control bar (minimize, maximize, close). Below the title bar is a header area with a server icon and the text "Web Portal connection". The main content area contains the instruction: "Specify how the Intranet Role can connect to the Web Portal from its current location." There are two "Address" input fields. The first is for the general connection. Below it is a checkbox labeled "The management console needs different connection information than the Intranet Role to connect to the Web Portal." If checked, a second "Address" field is used. An information icon (i) is followed by the text: "Please ensure that your firewalls allow HTTPS traffic on port 443." At the bottom right, there are two buttons: "Save and close" and "Abbrechen und schließen".

3. Enter the HTTPS address of the Web Portal under **Address**.
4. If the NoSpamProxy Command Center requires a different address for the connection to the Web Portal, tick the checkbox and enter this address.
5. Click **Save and close**.

Adjusting the configuration

In exceptional cases, the configuration of a Web Portal may differ from that of the Intranet Role.

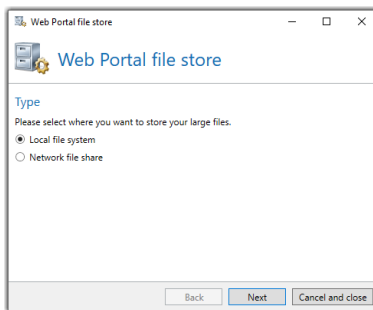
- In this case, click **Synchronize configuration** to synchronize the configuration with the selected Web Portals.



NOTE: Please note that the amount of data in the database of the Intranet Role will increase in the short term and can therefore lead to a full database. This is often the case when an SQL Express database is in use. The overfilling is normally reduced automatically.

Configuring the file storage location

You can adjust the file location for large files that you send via NoSpamProxy Large Files after you set up the connection.



The following locations are available:

Local file system| Specify a path on a local storage for which the accounts specified in the dialog have the appropriate rights.

Network file share| Specify the path to the network share. Select whether you access the share through the server's computer account or whether a specific user account is used for this.

Amazon S3| Amazon Simple Storage Service (Amazon S3) is a cloud-based object storage service.



NOTE: To be able to use Amazon S3 as a storage location, you must enable this option using the PowerShell cmdlet **Set-NspWebPortalSettings**.

Editing general settings

The current settings for the Web Portal are displayed under **Configuration > NoSpamProxy components > Web Portal > Settings**.

- Click **Edit settings** to make changes to the settings.

General tab

The screenshot shows a window titled "Web Portal settings" with three tabs: "General", "PDF Mail", and "Large Files". The "General" tab is active. Below the tabs, there is a text box for "External HTTPS address". Below that is a checkbox labeled "Use a different address for requests from within your organization". If checked, an "Internal HTTPS address" text box appears. At the bottom, there is a checkbox labeled "Enable secure web emails without an invitation link" with a note below it: "The address can be used by your partners." At the very bottom of the dialog are two buttons: "Save and close" and "Cancel and close".

Portal addresses | When using the Web Portal, a link to the Web Portal is inserted into emails if necessary. The link contains the address at which the Web Portal can be reached from the Internet.

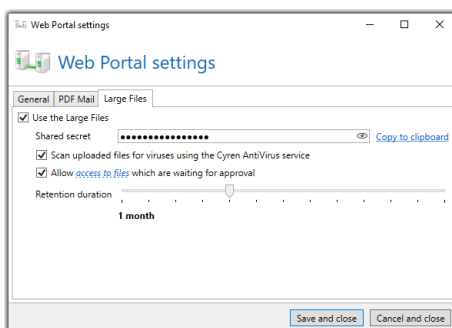
- Enter the address at which the Web Portal can be reached at **External HTTPS address**.
- To use a different address for access from the company network, enter it under **Internal HTTPS Address**.

Secure web emails| Under **Secure web emails** you can specify an address that allows the Web Portal to be used without an invitation link. If the Web Portal is used in this way, an external partner can send an email to recipients in your company via the Web Portal. To do this, he or she must enter a sender address and a valid recipient address of a corporate user stored in NoSpamProxy.



NOTE: If no company users are stored in NoSpamProxy, at least the domain is validated for the recipient address to see whether it is present in the list of corporate domains.

Large Files tab



Use Large Files| Activates the Large Files function.

Shared secret| A shared secret is required to secure communication between the Outlook Add-in and the Web Portal. Enter a password that is at least 12 characters long. The 'Large Files' files stored by the Web Portal are fully encrypted. The decryption key is only available to the recipient, so administrators of the server have no access to the files.

Allow access to files which are waiting for approval| If you want to check files waiting for approval before they are approved, you must explicitly allow this here.

Retention period After the file has been approved under **Large Files**, no further access by the 'Monitoring Administrators' group is possible.

Notes on the installation of the Web Portal

When integrating the Web Portal into the configuration, special settings must be observed in certain application scenarios:

The Web Portal is operated in parallel with the Gateway Role and/or Intranet Role

In this case, you must create the host names of the Local Security Authority that can be referenced in an NTLM authentication request. To do this, carry out the following steps for all nodes on the client computer:

1. Press **Windows + R** to open **Run**.
2. Enter **regedit** and then click **OK**.
3. Search for the following registry subkey and click on it: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**.
4. Right-click on **MSV1_0**, point to **New** and then click **Multi-String Value**.



NOTE: You can ignore the error message displayed.

5. Enter **BackConnectionHostNames** in the Name column and then press **Enter**.
6. Right-click on **BackConnectionHostNames** and then click **Modify**.
7. In the Value data box, enter the **CNAME** or the **DNS alias** that is used for the local shares on the computer.
8. Click **OK**.
9. Exit the registry editor and restart the computer.

**NOTE:**

- Enter each host name in a separate line.
- If the **BackConnectionHostNames** registry entry exists as a REG_DWORD type, you must delete the BackConnectionHostNames registry entry.
- Please also refer to [article KB926642 in the Microsoft documentation](#).

The Web Portal is operated on a system in the DMZ/computer(s) outside the domain

In this case, please refer to the corresponding [article KB926642 in the Microsoft documentation](#).

Changing the design of the NoSpamProxy Web Portal in version 10

This article describes how to change the colors and logo used on the Web Portal in NoSpamProxy 10.



NOTE: You need at least rudimentary HTML knowledge to be able to make the adjustments.

- The corresponding files are located in the directory **%Program Files%\Net at Work Mail Gateway\enQsig Webportal**.
- Make the changes in the files **..\Content\Site.css** (color adjustments) and the file **..\Views\Shared_Layout.cshtml** (logo and others).

Changing the colors

To edit the colors, edit the file `Site.css`. There are four relevant places for the color:

Upper area

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

- This position marks the colored bar in the upper area. Change the value `#C01B1B` to another value to change the color.
- To change the thickness of the bar, increase or decrease the value `10px`.

Progress bar

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

- This area determines the color of the progress bar when a file is transferred to the Web Portal. With `height` you change the thickness of the bar, with `background-color` you change the color.

Action buttons

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

- This area determines the appearance of the action buttons, such as the **Login** button. You can change the color with `background` or the size with `padding`.

Font colour of the listing of all files already uploaded

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

Changing the logo

To change the displayed logo, edit the file `_Layout.cshtml`. The following line is responsible for the display of the logo:

```

```

Name the position and name of the new file here and save the settings.

Databases

Under Databases, you make changes to the connection to the database of the corresponding role.



NOTE: The database is created during setup. You only need to make changes if you move the database to another SQL server.

Changing database connection settings

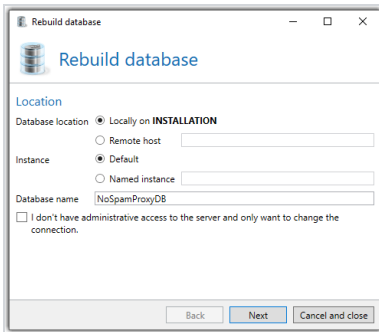


NOTE: Before you change the connection settings, back up the existing database and import this backup to the new database server.



NOTE: Each database of roles is independent and must not be shared between roles. This means that if you have two Gateway Roles, you also create two databases. These may share both a server and an instance, but are otherwise independent of each other. Independent databases increase the stability of NoSpamProxy and facilitate administrative tasks such as upgrades or database moves.

1. Go to **Configuration > NoSpamProxy components > Databases**.
2. Click **Modify**.



3. Under **Database location**, specify the server on which the database is located.



NOTE: If the database is on the same server as the Gateway Role, select **Local Server**. If the database is located on another server, first select the **Remote host** option and then enter either the IP address or the fully qualified domain name (FQDN) of the server where the database is located.

4. Under **Instance**, **specify** whether the default instance of the SQL server or a named instance is used for the database of the Gateway Role.



NOTE: If this is the default instance of the SQL server, select the option **Default**. Otherwise, click **Named Instance** and then enter the name of the corresponding instance.

5. Under **Database name**, **enter the** name of the corresponding database(s).
The following database names are used by default:

- Gateway Role
NoSpamProxyGatewayRole

- Intranet Role
NoSpamProxyIntranetRole



NOTE: If you only want to change the connection parameters, select the corresponding field in the lower part of the dialog.

6. Click **Next**.
7. On the Administrative Authentication page, specify which user account to use to make changes to the selected database, enter the appropriate credentials, and click **Next**.

Rebuild database

Rebuild database

Administrative authentication

Your current credentials can't be used to configure the database. Please provide administrative credentials.

Type Windows SQL Server

Username

Password

Back Next Cancel and close

8. Under **Service authentication**, specify how the Gateway Role should log on to the SQL Server.



NOTE: If SQL authentication is disabled on the SQL server, then the integrated authentication must be used. Otherwise you can choose between Integrated and SQL authentication.

9. Select the desired action on the next page. Depending on the available databases, different options are available here.

10. Click **Finish**.

Saving databases

The roles of NoSpamProxy use the following databases:

- **Gateway Role** NoSpamProxyGatewayRole
- **Intranet Role** NoSpamProxylntranetRole
- **Web Portal** NoSpamProxyWebPortal



NOTE: If NoSpamProxy uses your existing standard or Enterprise SQL Server, you can configure a periodic backup of all databases there using the Enterprise Manager. When using SQL Server Express Edition, you must manually back up the database with a script and restore it if necessary.

Backing up the databases via the command line

Enter the following lines in the command line:

For the Gateway Role database `osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE NoSpamProxyGatewayRole TO DISK = 'c:\NoSpamProxyGatewayRole.bak'"<mtlingo type="" prevChar="" nextChar=" " /> >`

For the Intranet Role database `osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE NoSpamProxylntranetRole TO DISK = 'c:\NoSpamProxylntranetRole.bak'"<mtlingo type="" prevChar="" nextChar=" " /> >`

For the Web Portal database `osql -S (local)\NameDerInstanz -E -Q "BACKUP DATABASE NoSpamProxyWebPortal TO DISK = 'c:\NoSpamProxyWebPortal.bak'">`

These rows save the corresponding databases in files without shutting down the database for this purpose. You should therefore check whether you schedule an appropriately customized call as a regular task with Windows Task Scheduling.

Creating a backup

Enter the following lines in the command line:

For the Gateway Role database `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyGatewayRole FROM DISK = 'c:\NoSpamProxyGatewayRole.bak' WITH FILE= 1, NOUNLOAD, REPLACE "<mtlingo type="" prevChar="" nextChar="" />`

For the Intranet Role database `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyIntranetRole FROM DISK = 'c:\NoSpamProxyIntranetRole.bak' WITH FILE= 1, NOUNLOAD, REPLACE "<mtlingo type="" prevChar="" nextChar="" />`

For the Web Portal database `osql -S (local)\NameDerInstanz -E -Q "RESTORE DATABASE NoSpamProxyWebPortal FROM DISK = 'c:\NoSpamProxyWebPortal.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

The databases must already exist in order for the recovery to work.



NOTE: Since the SQL server keeps the databases themselves permanently open, they cannot be captured via a normal backup of the files, such as via NTBACKUP.

How to set up database permissions

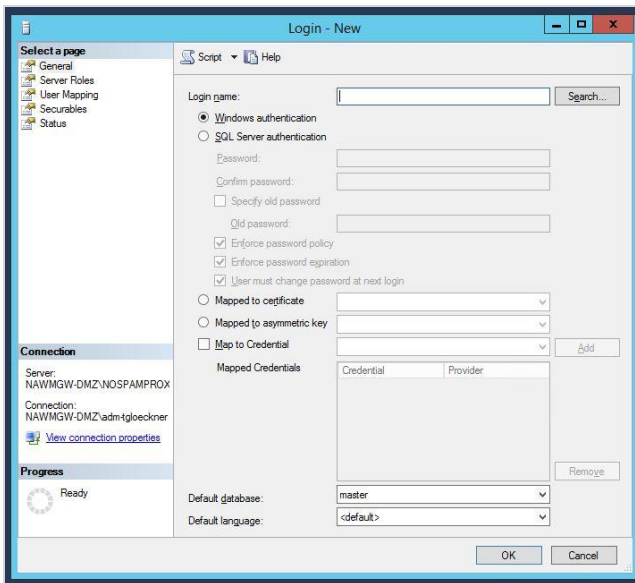
It is common that not only the user who originally performed the installation needs to perform updates, but also other administrator accounts. To do this, it is necessary to set up the appropriate permissions for these additional users. The corresponding steps are described below:

**NOTE:**

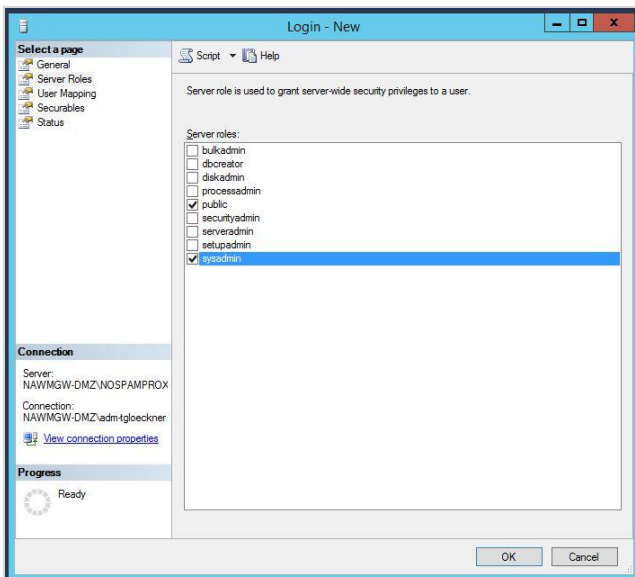
- All steps apply to all roles of NoSpamProxy; they only differ in the database names.
 - Database Intranet Role: NoSpamProxyIntranetRole
 - Database Gateway Role: NoSpamProxyGatewayRole
 - Database Web Portal: NoSpamProxyWebPortal
- Users and user groups (local or domain) can be registered

1. Log on to the system with the user who performed the installation.
2. Install the SQL Management Studio.
3. Open SQL Management Studio and log on to the local instance that contains the NoSpamProxy database(s), using Windows authentication.
4. Expand the **Security** and **Logins** folders.
5. Right-click the **Logins** folder.
6. Select **New Login** from the context menu.

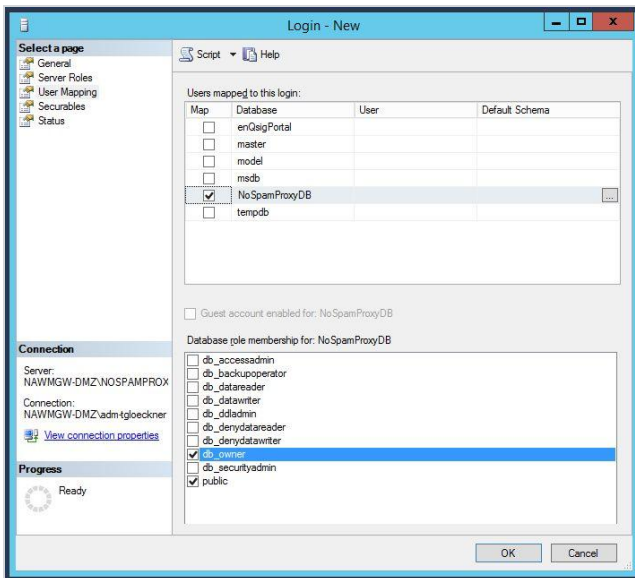
- Under **General**, select the user to be added.
Keep the item **Windows Authentication**.



- Under **Server Roles**, check **sysadmin**.



- Under **User Mapping**, check the box for the corresponding database. Additionally, activate the role **db_owner**.



- Make further optional settings if required.
- Save the new login and close SQL Management Studio.

To verify access, log on to the system with the added user, open SQL Management Studio and check if you can view the database tables. If this works, access is set up.

Checking the database integrity

This article describes how you can check the integrity of the database and repair it if errors occur.



NOTE: You need Microsoft SQL Server Management Studio for this action.

- Open the Microsoft SQL Server Management Studio.
- Expand the menu item **Databases**.

3. Click the **NoSpamProxyDB** database and then in the top left on **New query**. A white window appears on the right side.
4. To check a suspicious database for errors, use the following command in SQL Management Studio:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole')
```

5. The following command corrects any errors:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole', REPAIR_REBUILD)
```



NOTE: Before executing the command, you must change the access mode ("Restrict Access") from MULTI_USER to SINGLE_USER under Options in the database properties.

6. Check the success of the action with the following command:

```
DBCC CHECKDB ('NoSpamProxyGatewayRole')
```



NOTE: The output should now no longer contain any error messages. If the database could not be successfully repaired and error messages still appear, please execute the command **DBCC CHECKDB ('NoSpamProxyDB', REPAIR_ALLOW_DATA_LOSS)**. Afterwards you should check the success with the above mentioned command again. If the database cannot be repaired, you can also create a new database using the NoSpamProxy interface. Under certain circumstances there is a defect in the SQL Server.

Notes on database sizes



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).

Below are some instructions on how to react to a corresponding message in the NoSpamProxy Command Center:

Warning levels

NoSpamProxy warns you about a full database in two stages:

When the database is 70% full

- a message is added to the event log,
- a note is displayed on the start page of the NoSpamProxy Command

Center under "Issues" and

- a notification is sent to the set administrator email address.

When the database is 90% full

- a message is added to the event log,
- a note is displayed on the start page of the NoSpamProxy Command Center under "Issues" and
- a notification is sent to the set administrator email address.

What are possible reasons for a full database?

The reasons are listed below.

- The configured period of message tracking and its details (monitoring) is too long.
- There are problems with communication between two or more NoSpamProxy roles.
- Expired data has not been properly deleted from the database.

How to analyse the database

To find out why the database has reached the respective size, proceed as follows:

1. Install Microsoft SQL Management Studio on the system on which the affected database is installed. Microsoft SQL Management Studio is available free of charge from the Microsoft website.
2. Start the SQL Management Studio.

3. Log on to the SQL instance where the database is located. Usually these instances are called **(local)\SQLEXPRESS** or **(local)\NOSPAMPROXY**.
4. After successfully logging on, execute the following SQL queries (depending on the NoSpamProxy role involved); to do this, you only need to change the first row to the following databases:
 - Intranet Role: `USE [NoSpamProxyIntranetRole]`
 - Gateway Role: `USE [NoSpamProxyGatewayRole]`
 - Webportal: `USE [NoSpamProxyWebPortal]`

```
USE [NoSpamProxyIntranetRole] / USE
[NoSpamProxyIntranetRole] / USE [NoSpamProxyWebPortal]
GO SELECT isnull(t.NAME, 'Total') AS TableName, s.name as
SchemaName, p.rows AS RowCounts, CAST(ROUND(((SUM
(a.used_pages) * 8) / 1024.00), 2) AS NUMERIC(36, 2)) AS
SizeInMB FROM sys.tables t INNER JOIN sys.indexes i ON
t.OBJECT_ID = i.object_id INNER JOIN sys.partitions p ON
i.object_id = p.OBJECT_ID AND i.index_id = p.index_id INNER
JOIN sys.allocation_units a ON p.partition_id = a.container_id
LEFT OUTER JOIN sys.schemas s ON t.schema_id =
s.schema_id WHERE t.NAME NOT LIKE 'dt%' AND t.is_ms_
shipped = 0 AND i.OBJECT_ID > 255 GROUP BY ROLLUP
(t.Name, s.Name, p.Rows) HAVING p.rows is not null or (p.rows
is null and t.name is null) ORDER BY sum(a.used_pages) desc
GO
```


How can the results be interpreted and solved?

In the output of the SQL script you can find an overview of all existing tables of the database as well as information about their size.

	TableName	SchemaName	RowCounts	SizeInMB
1	Total	NULL	NULL	25789.40
2	UrlVisit	MessageTracking	104839460	15549.06
3	Operation	MessageTracking	4257612	6485.40
4	MessageTrackEntry	MessageTracking	1236374	935.69
5	MessageOperation	MessageTracking	4254899	581.94
6	Action	MessageTracking	5832197	538.54
7	MessageAddress	MessageTracking	2530697	473.00
8	DeliveryAttempt	MessageTracking	2272604	403.08
9	Filter	MessageTracking	3124350	389.36
10	Url	MessageTracking	866710	258.39
11	Attachment	MessageTracking	367485	58.34
12	LevelOfTrust	MessageTracking	751502	38.86
13	UserAndDomainStatistic	MessageTracking	155662	32.83
14	Certificate	CertificateStore	4759	16.75
15	Association	LargeFileTransfer	14095	7.59
16	Certificate	MessageTracking	8138	3.80

There are two specific tables that should be empty in normal operation or whose entries should change constantly each time they are called:

- DataReplication.artefact

PendingRequest	CertificateEnroll...	45	0.16
Artefact	DataReplication	0	0.16
Rule	Disclaimer	17	0.08

- MessageTracking.LegacyMessageTrackEntry

Mapping	AddressRewriting	54	0.08
LegacyMessage Track...	Message Tracking	0	0.05
Key	Dkim	2	0.03

If data accumulates in these tables but does not degrade, this indicates that problems exist. These must be clarified and solved by the NoSpamProxy support. In this case, please contact the partner responsible for you or - if you have purchased manufacturer support - the NoSpamProxy support directly.

All other scenarios indicate too large a memory space for message tracking, which you can edit and reduce in the NoSpamProxy Command Center under **Configuration > Advanced Settings > Monitoring**. The reduction usually takes up to 24 hours, so that a result is usually not visible until the next day.

Saving databases

The roles of NoSpamProxy use the following databases:

- **Gateway Role** NoSpamProxyGatewayRole
- **Intranet Role** NoSpamProxyIntranetRole
- **Web Portal** NoSpamProxyWebPortal



NOTE: If NoSpamProxy uses your existing standard or Enterprise SQL Server, you can configure a periodic backup of all databases there using the Enterprise Manager. When using SQL Server Express Edition, you must manually back up the database with a script and restore it if necessary.

Backing up the databases via the command line

Enter the following lines in the command line:

- For the Gateway Role database

```
osql -S (local)\NameOfTheInstance -E -Q "BACKUP DATABASE  
NoSpamProxyGatewayRole TO DISK =  
'c:\NoSpamProxyGatewayRole.bak'" >
```

- For the Intranet Role database

```
osql -S (local)\NameOfTheInstance -E -Q "BACKUP DATABASE  
NoSpamProxyIntranetRole TO DISK = 'c:\NoSpamProxyIntranetRole.bak'"  
>
```

- For the Web Portal database

```
osql -S (local)\NameOfTheInstance -E -Q "BACKUP DATABASE  
NoSpamProxyWebPortal TO DISK = 'c:\NoSpamProxyWebPortal.bak'" >
```

These rows save the corresponding databases in files without shutting down the database for this purpose. You should therefore check whether you schedule an appropriately customized call as a regular task with Windows Task Scheduling.

Creating a backup

Enter the following lines in the command line:

- For the Gateway Role database

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

- For the Intranet Role database

```
osql -S (local)\NameOfTheInstance -E -Q "RESTORE DATABASE  
NoSpamProxyIntranetRole FROM DISK =  
'c:\NoSpamProxyIntranetRole.bak' WITH FILE= 1, NOUNLOAD,  
REPLACE "
```

- For the Web Portal database

```
osql -S (local)\NameOfTheInstance -E -Q "RESTORE DATABASE  
NoSpamProxyWebPortal FROM DISK = 'c:\NoSpamProxyWebPortal.bak'  
WITH FILE= 1, NOUNLOAD, REPLACE "
```

The databases must already exist in order for the recovery to work.



NOTE: Since the SQL server keeps the databases themselves permanently open, they cannot be captured via a normal backup of the files, such as via NTBACKUP.

Creating an encryption dump

You can configure NoSpamProxy so that it saves decrypted data in a file before this data is processed further in an email. This can be very helpful in analysing formatting problems related to encryption and decryption.

To create the encryption dump, proceed as follows:

1. Go to **C:\ProgramData\Net at Work Mail Gateway\Configuration**.
2. Open the file **Gateway Role.config**.
3. Search for the following line:
`</configSections>`
4. Add the following lines below the line just mentioned:

```
<netatwork.nospamproxy.cryptography> <debugging  
dumpDecryptedContentToDisk="true"/>  
</netatwork.nospamproxy.cryptography>
```



NOTE: If the section `netatwork.nospamproxy.cryptography` already exists, just add the line `<debugging dumpDecryptedContentToDisk="true"/>`.



NOTE: Before you save the configuration file, you must stop the Gateway Role service. Only then can you save the configuration file properly.



NOTE: The decrypted contents are now stored in the local service temp folder. Usually this is the folder
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp
. If the files are not created there, please check the folder
C:\Windows\Temp.

Creating a memory dump

This article describes how to create a memory dump for NoSpamProxy support on a Windows 2008 Server R2 or later.

1. Open the Task Manager on the appropriate server.
2. Switch to the **Details** tab and sort the entries by name.
3. Right-click the appropriate process and choose **Create dump file**.

Send the memory dump to the NoSpamProxy Support at support@nospamproxy.de.

How to export static domain trust settings

To extract the static entries from the trust positions, proceed as follows:

1. Open SQL Management Studio (Express) to manage your NoSpamProxy database.

2. Connect to the database server on which the NoSpamProxyGatewayRole database is located.
3. Click **Neue Abfrage / New query** to create a new SQL query for the NoSpamProxyGatewayRole.
4. Add this query to the query editor:

```
USE NoSpamProxyGatewayRole; SELECT Domain, Gravity,
LevelOfTrust FROM DomainTrustEntry WHERE (Gravity = 0);
```

5. Perform the query by clicking on the red exclamation mark.

This query lists all static entries in the domain trust. If you need a application to import into version 7.6, or if you have problems executing these commands, please contact our support team. With this query you can bypass the use of our Mail Gateway API sample for reading the domain trusts.



NOTE: In a new installation, the static domain trust settings for known email providers are automatically entered during setup.

How to change the WebPort for NoSpamProxy

The Web Port is the port that the NoSpamProxy Command Center connects to when accessing the individual roles. Furthermore, the roles connect via the configured port and add 1. If the WebPort is configured to 6060, the services connect via 6061.



WARNING: Only change this port if absolutely necessary. In any case, read this article in its entirety.

To change the WebPort, proceed as follows:

1. Stop all NoSpamProxy services.
2. Go to **C:\ProgramData\Net at Work Mail Gateway\Configuration**.



NOTE: If you also use the Web Portal, go to **%Program Files%\Net at Work Mail Gateway\enQsig Webportal\App_Data**.

3. Locate the two configuration files **intranet role.config** and **gateway role.config**. In these files you make the appropriate settings.
4. Search for the line that begins with the following characters:
`<netatwork.nospamproxy.webservices`
5. Add the following attribute there:

```
port="NewPortValue"
```



NOTE: The `serverCertificateThumbprint` attribute is different on each NoSpamProxy server.

6. Change the URL reservation via netssh. Please use **HTTPSYSMANAGER** from <http://httpsysmanager.codeplex.com/>. Alternatively, enter the following command via the command line:

```
netsh http add urlacl url=http://+:8060/NoSpamProxy/ sddl=D:
(A;;GX;;;LS)(A;;GX;;;NS)
```

7. Now restart all services.
8. Right-click in the NoSpamProxy Command Center **NoSpamProxy** and then click **Change server**.
9. Adjust the port in this dialog.
10. Go to **Configuration > NoSpamProxy components** and recreate the role connections.

Connected systems

Here you manage connections to third-party products that interact with NoSpamProxy.

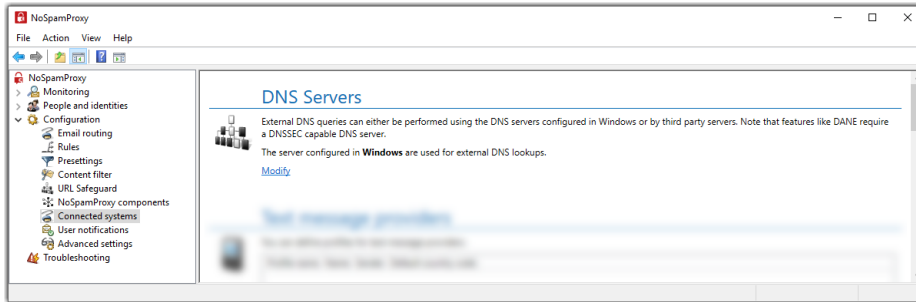
The screenshot displays the NoSpamProxy Command Center interface. On the left is a navigation sidebar with the following items: Overview, Monitoring, Identities, Configuration (expanded), Email routing, Rules, Content filter, URL Safeguard, NoSpamProxy components, Connected systems (highlighted), User notifications, Presettings, Advanced settings, and Troubleshooting. Below the sidebar are 'Actions' for Refresh and English.

The main content area is titled 'Connected systems' and contains several sections:

- DNS Servers**: Explains that external DNS queries can be performed using Windows-configured servers or third-party servers. A 'Modify' link is present.
- Text message providers**: Allows defining profiles for text message providers. A table with columns 'Profile name', 'Name', 'Sender', and 'Default country code' is shown. 'Add', 'Modify', and 'Remove' links are below.
- Archive connectors**: Explains that an archive connector provides a connection between a Gateway Role and an archive. A table with columns 'Connector name', 'Profiles', and 'Profile count' is shown. 'Add', 'Modify', and 'Remove' links are below.
- De-Mail providers**:
 - Telekom De-Mail connections**: Explains they are used to connect to Telekom De-Mail gateways. A table with columns 'Name', 'Certificate', 'Gateway Role', 'Target', and 'Domains' is shown. 'Add', 'Modify', and 'Remove' links are below.
 - Mentana-Claimssoft connection**: States 'No connection has been configured yet.' with an 'Add' link.
- digiSeal server connection**: States 'No connection has been configured yet.' with a 'Modify' link.
- CSA Whitelist**: States 'The CSA Whitelist is downloaded every 24 hours.' with 'Modify' and 'Download CSA Whitelist now' links.

■ DNS Servers

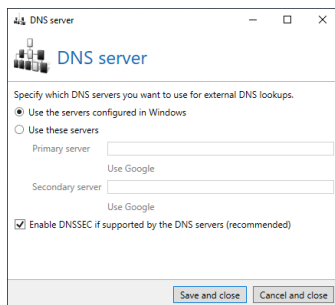
When using DANE you need a DNS server that supports DNSSEC. Since the DNS servers supplied with Windows server operating systems do not currently support this function, you can set up a connection to such a server here.



Configuring the DNS server

To enter the IP addresses of a primary and secondary server with DNSSEC support, proceed as follows:

1. Go to **Configuration > Connected systems > DNS Servers**.
2. Click **Modify**.



3. Perform one of the following two steps:
 - Select **Use the servers configured in Windows** if you want to use Windows' own servers.

- Select **Use these servers** if you want to use a third-party server. Then enter the corresponding addresses.



TIP: Click **Use Google** to enter the publicly accessible Google DNS server into the configuration.

4. Select whether you want to activate **DNSSEC** (recommended).



NOTE: DNSSEC secures the transmission of resource records through digital signatures. This ensures the authenticity of these resource records.

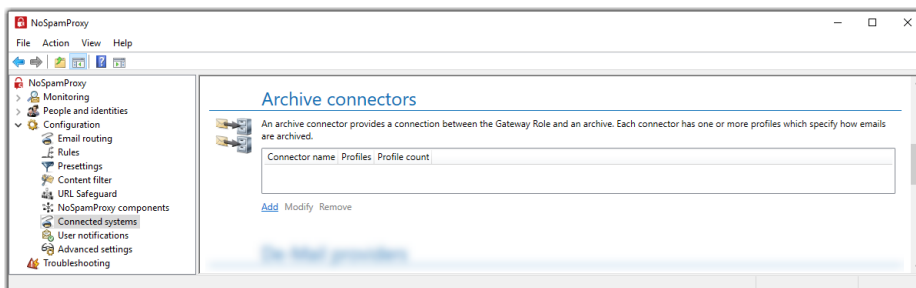
5. Click **Save and close**.



NOTE: DANE is used to check the transport encryption when delivering emails to your partners. See [Default partner settings](#).

Archive connectors

Via the archive interface, emails and qualified signed documents can be transferred to an external archive system. Currently supported are the file system, an archive mailbox and d.velop d.3. It is possible to use multiple archive systems in parallel.



The configuration of an archive connector comprises two areas:

Archive connectors| Connectors define the interface to an external archive system such as the file system.

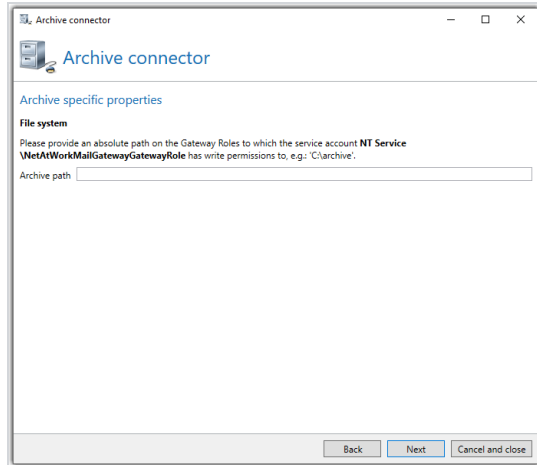
Profiles| One or more profiles are created within a connector. It can be used to set properties such as the exact storage location for emails and documents. In addition, the metadata of emails is mapped to metadata of the archive system, if necessary.



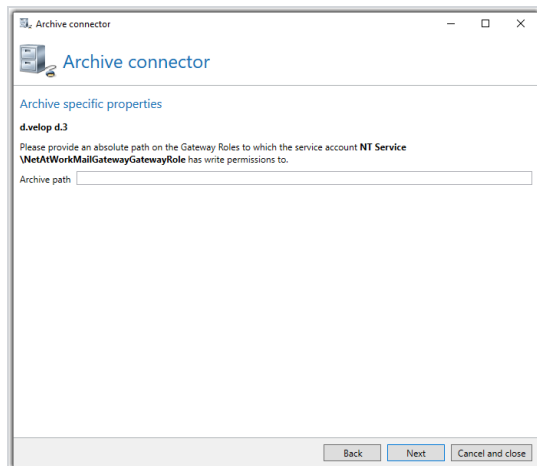
NOTE: Emails are archived as they are received by NoSpamProxy. NoSpamProxy does not perform encryption or decryption, nor does NoSpamProxy upload attachments to the Web Portal. Note that emails are only archived if NoSpamProxy does not reject the email. If, for example, the malware scanner responds or the email cannot be decrypted, the respective email is not archived.

Configuring archive connectors

1. Go to **Configuration > Connected systems > Archive connectors**.
2. Click **Add**.
3. Select the archive system and enter a name for the connector.
4. Make the appropriate configuration for the selected archive system and click **Next**.
 - When storing emails and documents in the file system, you only need to specify a path. Emails and documents are stored in folders below this path.



- The connector for the journaling mailbox has no other settings on the connector. The profiles are displayed directly.
- For a connector to a d.velop d.3 system you only have to specify a path. Emails and documents are written into this directory and are retrieved from this directory by the d.velop d.3 system.



5. (Optional) Create profiles for the connector.



NOTE: The content of the profile configuration page depends on the selected archive system.

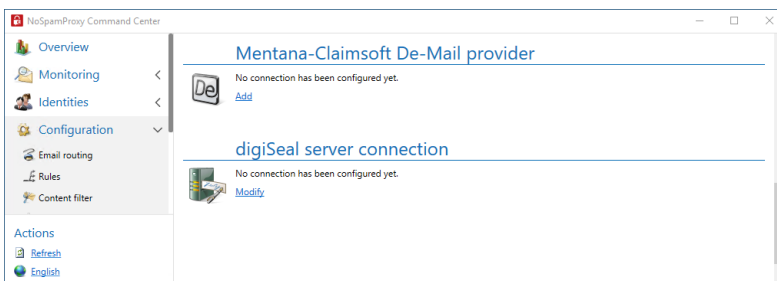


NOTE: Profiles allow you, for example, to distribute emails and documents to different folders within an archive system. Give the new profile a name and specify which emails are archived by this profile. Note that emails with a qualified signed attachment are always archived. You can optionally archive all other emails as well.

6. Click **Finish**.

De-Mail via Mentana-Claimsoft

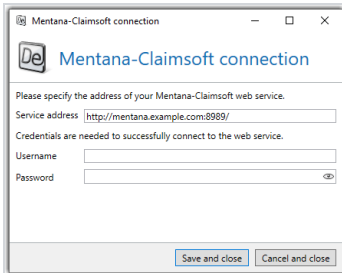
Here you can manage the connections to the De-Mail system.



Mentana-Claimsoft's De-Mail connectors require you to set up a connection to that provider's web service.

Proceed as follows:

1. Go to **Configuration > Connected systems > Mentana-Claimsoft De-Mail provider**.
2. Click **Add**.



3. Enter the service address at which the web service can be reached.
4. Enter the credentials to access the service.
5. Click **Save and close**.



NOTE: The information entered in this dialog is immediately available for both the De-Mail send connector and the receive connector. This means that you only have to configure the connection once and it is immediately available in all connectors.

CSA Certified IP List

To use the CSA Certified IP List filter, you must configure the download of the list.

Configuring CSA Certified IP List

1. Go to **Configuration > Connected Systems > CSA Certified IP List**.
2. Click **Modify**.

3. Select **Enable daily download of the CSA Certified IP List** if you want to use this filter CSA Certified IP List.



NOTE: If you do not want to use the above filter, select **Disable download**.

4. Click **Save and close**.



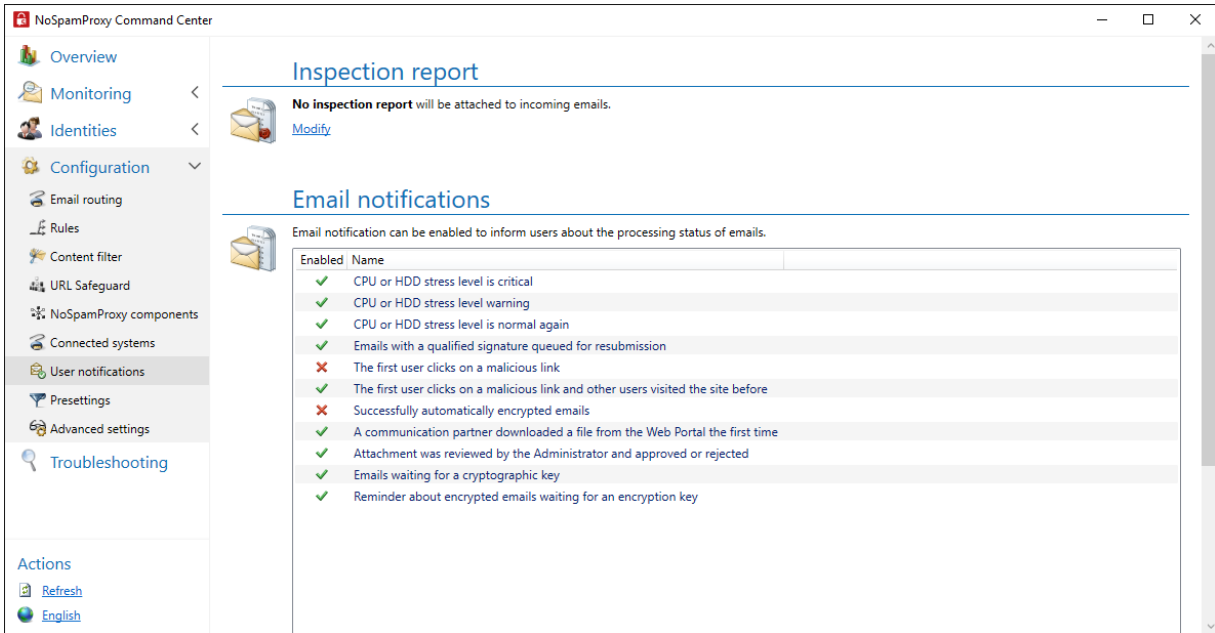
NOTE: To manually download the CSA Certified IP List, click **Download CSA Certified IP List now** under **Configuration > Connected Systems > CSA Certified IP List**.



NOTE: The CSA Certified IP List will be downloaded from `service.nospamproxy.de`. Access to this address is required for downloading the list. Make sure that your firewall settings allow this.

User notifications

Here you define which notifications NoSpamProxy sends to internal and external contacts and which sender addresses are used.



Inspection report



This feature is available if you have purchased a corresponding licence.

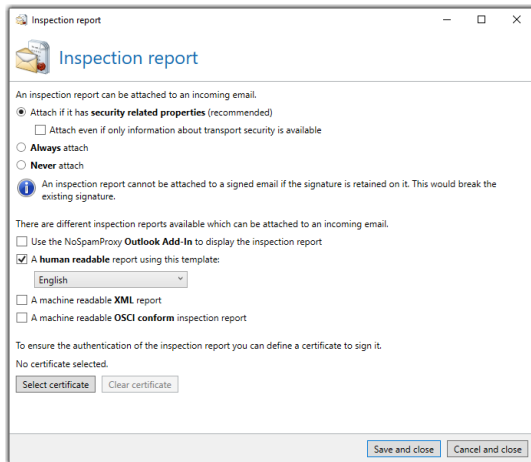
The inspection report contains information about security-relevant properties and procedures during email processing. It can be attached to emails to local addresses. The currently set values are displayed under **Inspection report**.



NOTE: No inspection report can be attached to signed emails if the signature remains on the email. This signature would otherwise break the existing signature. To configure the removal of signatures, see the information under [S/MIME- und PGP-Überprüfung sowie Entschlüsselung](#).

Configuring the inspection report

1. Go to Configuration > User notifications > Inspection report.
2. Click Modify.



3. Select to which emails the report should be attached.
4. Select the type of inspection report.
 - **Inspection report for the Outlook Add-In** This test report is embedded in the email as an X header. This embedded data can be displayed by the Outlook Add-In of NoSpam Proxy.



We recommend using this type of inspection report, as all other types create an attachment which will be attached to the respective email.

- **Human-readable report**| The textual inspection report presents the information in a human-readable form. Select a template for the report to be used for the presentation of the report. By default, there are two templates, German and English. The templates are located in the configuration directory of the Gateway Role and have the extension `HtmlProcessCardTemplate`. If you want to customize the templates, do not change the default templates as they will be overwritten when the software is updated. Instead, create a copy of an existing template and modify it.
 - **XML inspection report**| The XML test report is used for automatic processing of the inspection report data by another application.
5. (Optional) Select a private email certificate.
 6. Click **Save and close**.



NOTE: To suppress the creation of the test report rule-based, see the information under [Steps in creating rules](#).

■ Email notifications

Here you configure the notifications regarding the status of the email processing.

1. Go to **Configuration > User notifications > Email notifications**.
2. Select one or more notifications.

3. Click **Enable selected / Disable selected** to enable or disable the respective notifications.

I How to customise NoSpamProxy notifications

To customise the user notifications, you must adapt the corresponding default templates and save them in a special folder for customised templates.

Pay particular attention to the following points:

- The standard templates are available as CSHTML files (with the exception of two HtmlProcessCardTemplate files) and are located in the **%Program Files%\Net at Work Mail Gateway\Intranet Role\Templates** directory, or in the **%Program Files%\NoSpamProxy\Intranet Role\Templates** directory for new installations.
- Make sure that you save the customised template files under **C:\ProgramData\Net at Work Mail Gateway\Templates Customizations** to make them update-proof. The original files must remain in the default folder.
- You only need to make these changes on the Intranet Role. The contents are automatically replicated to all connected Gateway Roles.

I Procedure after updates

After updating NoSpamProxy, it is possible that changes have been made to one or more default templates. You can recognise this by a different version number, among other things. The version number of a template file can be found at the very beginning of the corresponding file, for example `@* Version: 1 *@` or `<?xml`

`version="1.0" encoding="utf-8" ?>`. In these cases, you must manually update the template files you have customised, otherwise the default template will be used again.

Proceed as follows to update the customised template files:

1. Copy the corresponding default templates into the folder for customised files (see above).
2. Match their version numbers with the version numbers of the default templates.
3. Make the desired changes to the files (again).

Overview of available template files

ApplySymmetricEncryptionPasswordNotice.cshtml

When a user sends an email as a PDF mail, he receives a notification about the password used, or an information that the recipient has been sent the password via SMS or that the creation of the PDF Mail failed. The text of the notification is in this file. The appearance is defined via the CommonMail template.

AttachmentManager.cshtml

When NoSpamProxy removes a file attachment from an email, a replacement file is attached to the email to notify the user that the original file has been removed. The corresponding message text can be edited in the Attachment Manager.cshtml file.

AttachmentQuarantine.cshtml

When NoSpamProxy removes an attachment from an email and quarantines it, a replacement file is attached to the email to notify the user that the original file has been removed. The user has the possibility to download the remote file directly from the quarantine via a download link. The corresponding message text can be edited in the attachment Quarantine.cshtml file.

AttachmentQuarantineApproval.cshtml

When NoSpamProxy removes an attachment from an email and quarantines it, a replacement file is attached to the email to notify the user that the original file has been removed. The user has the option to download the remote file from the quarantine via a download link after approval by the administrator. The corresponding message text can be edited in the attachment QuarantineApproval.cshtml file.

CommonMailTemplate.cshtml

This file defines the general appearance of notifications. Here, for example, the colors and the logos to be used are stored as HTML tags. All other files except the "ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml" contain only the text modules.

ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml

The appearance of the PDF file is defined in this file. Colors and logos must be defined here again.

ConvertMailContentToPdfAttachmentActionTeaser.cshtml

This file contains the text for the carrier email of the PDF file. The recipient of a PDF Mail is informed that the actual content of the e-mail is in the attached PDF document. The appearance is defined via the CommonMail template.

DeliveryNotificationReport.cshtml

This is the content of the transmission report if a user has requested it in Outlook. The appearance is defined via the CommonMail template.

DeMailConnectorIssueEscalationMail.cshtml

If NoSpamProxy cannot download de-mails from the DMDA for a period of time, a notification is sent to the administrative email address. The content of this notification can be edited here.

English.HtmlProcessCardTemplate

The content of the German test report can be edited in this file. Audit reports are generated at the request of the administrator if an e-mail was signed and/or encrypted, for example.

EmailHintsHTML.cshtml

The texts for the HTML versions of the email hints can be edited in this file.

EmailPlainText.cshtml

The texts for the plain text versions of the email hints can be edited in this file.

EncryptedMailNotificationTemplate.cshtml

If a user marks an email as "Encrypt automatically" and enQsig does not have a cryptographic key, the recipient will be informed. This email will tell you what options he or she has. The content of this email is recorded in this template. The appearance is defined via the CommonMail template.

EncryptionDelayedNotificationForSender.cshtml

If a user marks an email as "Encrypt automatically" and enQsig does not have a cryptographic key, the recipient will be informed. The content of the delay message is defined here. The appearance is defined via the CommonMail template.

EncryptionFailureNotificationForSender.cshtml

If a user marks an email as "Encrypt automatically" and an error occurs during encryption, the sender will be informed. The content of this message is here. The appearance is defined via the CommonMail template.

EncryptionSucceededNotificationForSender.cshtml

If a user marks an email as "Automatically encrypt", he will receive a notification as soon as the email has been encrypted. The appearance is defined via the CommonMail template.

English.HtmlProcessCardTemplate

The content of the English test report can be edited in this file. Audit reports are generated at the request of the administrator if an e-mail was signed and/or encrypted, for example.

LargeFileApprovalRequest.cshtml

In this file, you can customise the sharing request for files.

LargeFileDownloadNotification.cshtml

If a user sends a file via Large Files, he will receive a notification when the recipient has downloaded the file. The content of the notification can be edited here.

MailOnHoldExpired.cshtml

If a user marks an email as "Encrypt automatically" and enQsig has no cryptographic key and the recipient of the email does not deposit a cryptographic key within 5 days, the email will be discarded and the sender will be informed. The content of this message is here. The appearance is defined via the CommonMail template.

MailValidationError.cshtml

If a De-Mail cannot be sent via the De-Mail connector, the sender will be notified. The content of this message is here. The appearance is defined via the CommonMail template.

PolicyFailureNonDeliveryMessage.cshtml

If an email violates any of the guidelines in the rulebook, the sender is notified. The content of this message is here. The appearance is defined via the CommonMail template.

QualifiedSignatureIssueEscalationMail.cshtml

If the verification or creation of a qualified signature fails, a notification is sent to a specified address. The content of this message is here. The appearance is defined via the CommonMail template.

SampleAutoReply.cshtml

Since NoSpamProxy 10 it has been possible to have an automatic reply generated if, for example, a particular email address is contacted. The content of this automatic reply can be adjusted here.

You can copy this file and save it under a different name. You then specify the template file for the respective purpose in the NoSpamProxy rule set.

SymmetricPasswordUpdateNotification.cshtml

If an external recipient has stored a password for the PDF email on the Web Portal, he or she will be notified of the change. The content of this message is here. The appearance is defined via the CommonMail template.

WordFilterMatchNotification.cshtml

Since NoSpamProxy 10, it has been possible to send a notification to a specific email address as soon as certain words appear in an email. In this file you define the content of the notification.

Adaptation of the template files

Start with the file "CommonMailTemplate". Here you determine the appearance of all emails. Customise the StyleSheets in the respective files according to your needs. The integration of the corresponding logo is also done in this file. In later

operation, the logo files with the correct name must also be available in the Templates folder.

All other files contain only the text modules.

After restarting the Intranet Role, the new designs are used and replicated to the Gateway Role(s).



NOTE: Note that the files may be overwritten during patching/upgrading. After a patch/upgrade, check if your customised files are still present.

Using different designs for sender domains

This article describes how to adapt the templates for the design of the system emails of NoSpamProxy (including PDF mails) from NoSpamProxy 11.x onwards so that different designs are used based on the sender domain. NoSpamProxy uses the template engine for .NET "Razor" as the basis for the dynamic change.

The CSHTML files to be edited are located in the %Program Files%\Net at Work Mail Gateway\Intranet Role\Templates directory. After the change, the files are automatically replicated to all connected Gateway Roles.



NOTE: You need at least rudimentary HTML knowledge to be able to make the adjustments.

Adaptation of the template files



NOTE: You can request ready-made sample files with different designs from NoSpamProxy Support. This file can only be used from NoSpamProxy 11.0 onwards. In this example two different designs are used for the sender domains `netatwork.de` and `nospamproxy.de`. You can expand or reduce the number of domains at any time.

1. After downloading, first unpack the ZIP file into a temporary folder. It contains the following files:
 - `CommonMailTemplate.cshtml`
 - `CommonMailTemplateNaw.cshtml`
 - `CommonMailTemplateNsp.cshtml`
 - `ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml`
 - `ConvertMailContentToPdfAttachmentActionTeaser.cshtml`
 - `EncryptedMailNotificationTemplate.cshtml`
2. Start with the files that begin with "CommonMailTemplate". Here you determine the appearance of all emails that are required for PDF Mail.



NOTE: Make sure that you store the default design in the **CommonMailTemplate.cshtml**. Customize the stylesheets in the respective files according to your needs. The integration of the corresponding logos is also done in these files. In later operation, the logo files with the correct name must also be available in the Templates folder.

3. Customize the **ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml** file. This file determines the layout of the PDF file. Unlike the CommonMail template files, you only need one file to define the exceptions. The adjustments are made in the upper part. An example of three different designs is included.



NOTE: You define the design for the different domains. If NoSpamProxy does not find the corresponding send domain in active operation, the default design is used, which you can define with the template editor in the Admin GUI.

4. Copy all CSHTML files into the Templates folder of your program version.



NOTE: Back up all files contained in the file.



NOTE: Note that the files will be overwritten during patching/upgrading. After a version upgrade, do not copy the older, customized files over the newer ones, but adjust them again. Otherwise, there is a risk that new, necessary information will be missing from the template files.

Overview of available template files

The following list provides an overview of the function of the individual files:

ApplySymmetricEncryptionPasswordNotice.cshtml

When a user sends an email as a PDF Mail, he receives a notification about the password used, or an information that the recipient has been sent the password via SMS or that the creation of the PDF Mail failed. The text of the respective notification is in this file. The appearance regarding colours and logo is determined by the CommonMail template.

AttachmentManager.cshtml

If a file is removed from an email using the content filter rules, the recipient receives an information about it. The attachment can either be removed and deleted, it can be uploaded to the Web Portal and it can be uploaded to the Web Portal and assigned an admin share. A separate text is available for each of the three planned actions, which can be edited in this file. The appearance regarding colours and logo is determined by the CommonMail template.

AttachmentManagerNotificationForBlockedAttachmentsModel.cshtml

If emails with certain file attachments are rejected via the content filter rules, the sender receives an information about the rejection. The content of this message can be defined in this file. The appearance regarding colours and logo is determined by the CommonMail template.

AttachmentQuarantine.cshtml

If a file is moved to the Web Portal using the content filter rules and assigned an admin share, the administrator receives an information mail about it. The content of this email is defined in this file. The appearance regarding colours and logo is determined by the CommonMail template.

AttachmentQuarantineApproval.cshtml

If a file is moved to the Web Portal using the content filter rules, assigned an admin share, and then released by the administrator, the actual recipient of the file receives information about the release. The content of this email is defined in this file. The appearance regarding colours and logo is determined by the CommonMail template.

CommonMailTemplate.cshtml

This file defines the general appearance of notifications. Here, for example, the colors and the logos to be used are stored as HTML tags. All other files except the **ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml** contain only the text modules.

ConvertMailContentToPdfAttachmentActionPdfHeader.cshtml

The appearance of the PDF file is defined in this file. Colors and logos must be defined here again.

ConvertMailContentToPdfAttachmentActionTeaser.cshtml

This file contains the text for the carrier email of the PDF file. The recipient of a PDF Mail is informed that the actual content of the e-mail is in the attached PDF document. The appearance is defined via the CommonMail template.

ConvertOfficeDocumentToPdfPreface.cshtml

With the "ConvertOfficeDocumentToPDF" action it is possible to convert Office documents into PDF to provide the recipient with a preview without active content. Information is placed in front of the created PDF document. The content of this message can be defined in this file.

DeliveryNotificationReport.cshtml

This is the content of the transmission report if a user has requested it in Outlook. The appearance is defined via the CommonMail template.

DeMailConnectorIssueEscalationMail.cshtml

If NoSpamProxy is repeatedly unable to retrieve or send De-Mail, an administrator is notified. The content of this message can be defined here.

EncryptedMailNotificationTemplate.cshtml

If a user marks an email as "Encrypt automatically" and enQsig does not have a cryptographic key, the recipient will be informed. This email will tell you what options he or she has. The content of this email is recorded in this template. The appearance is defined via the CommonMail template.

EncryptionDelayedNotificationForSender.cshtml

If a user marks an email as "Automatically encrypt" and enQsig does not have a cryptographic key, the sender will be informed of the delay. The content of the delay message is defined here. The appearance is defined via the CommonMail template.

EncryptionFailureNotificationForSender.cshtml

If a user marks an email as "Encrypt automatically" and an error occurs during encryption, the sender will be informed. The content of this message is here. The appearance is defined via the CommonMail template.

EncryptionSucceededNotificationForSender.cshtml

If a user marks an email as "Automatically encrypt", he will receive a notification as soon as the email has been encrypted. The appearance is defined via the CommonMail template.

LargeFileDownloadNotification.cshtml

If the recipient of a file that was previously moved to the Web Portal downloads it, the sender is notified. The content of this message can be defined in this file.

MailOnHoldExpired.cshtml

If a user marks an e-mail as "Automatically encrypt" and enQsig does not have a cryptographic key and the recipient of the email does not deposit a cryptographic key within 5 days, the email will be discarded and the sender will be informed. The content of this message is here. The appearance is defined via the CommonMail template.

MailValidationError.cshtml

If a De-Mail cannot be sent via the De-Mail connector, the sender will be notified. The content of this message is here. The appearance is defined via the CommonMail template.

PolicyFailureNonDeliveryMessage.cshtml

If an email violates any of the guidelines in the rulebook, the sender is notified. The content of this message is here. The appearance is defined via the CommonMail template.

QualifiedSignatureIssueEscalationMail.cshtml

If the verification or creation of a qualified signature fails, a notification is sent to a specified address. The content of this message is here. The appearance is defined via the CommonMail template.

SampleAutoReply.cshtml

With the action "AutoReply" it is possible to answer emails with an automatically generated email. The content of this message can be defined here.

SymmetricPasswordUpdateNotification.cshtml

If an external recipient has stored a password for the PDF email on the Web Portal, he or she will be notified of the change. The content of this message is [here](#). The appearance is defined via the CommonMail template.

WordFilterMatchNotification.cshtml

The word filter offers the possibility of a notification to any email address if certain words are found in emails. The content of this notification can be defined [here](#).

Presettings

Presettings This section contains global settings that can be used in other areas of the configuration. See [.RulesPartnersCorporate users](#)

Branding

The settings below are used on the NoSpamProxy Web Portal and for notification emails.

The font is **Calibri,Verdana,Arial** with a size of **16px**.

The colours are **#000000** for the text colour, **#C01B1B** for the accent colour, **#d2d6d9** for borders and **#F8F8F8** for content background.

The logo below is aligned **left** and has a logo background colour of **#ffffff**.

[Modify](#)

Word matching

Global word groups

Name	Scope	Find mode	Match format	Points per match
Common notation for medical products	Subject and body	Obfuscated words	Wildcards	2
Common notation of commercial words	Subject and body	Obfuscated words	Wildcards	2
Common notation of porn words	Subject and body	Obfuscated words	Wildcards	2
Common spam words (german)	Subject and body	Obfuscated words	Wildcards	2

[Add](#) [Modify](#) [Remove](#)

Realtime block lists

Global block lists

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

[Add](#) [Modify](#) [Remove](#)

Actions

[Refresh](#)

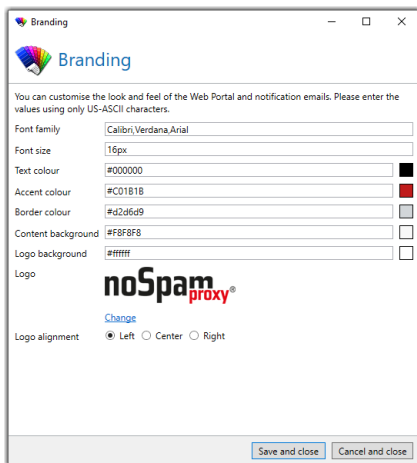
[English](#)

NOTE: The changes made here also affect existing rules, partners or corporate users. The settings always apply to all configurations in which they are referenced.

Word matching

Branding

The branding determines the appearance of the emails generated by NoSpamProxy as well as that of the Web Portal.



In most cases you will only need to adjust the accent color and logo to reflect your corporate identity.

The branding is applied to the following elements:

- Web Portal
- All email notifications generated by NoSpamProxy
- The replacement attachment for files sent via Large Files

I Word matching

In this area, you have the option of maintaining lists of expressions for which you want to assign positive or negative SCL points using the **Word matching** filter. The expressions are grouped into individual word groups, which you can use later in the individual rules. For each group of words, you determine whether the corresponding SCL points are to be awarded for the terms. This way you have the possibility to create groups with wanted and unwanted expressions.

Adding a new word group

1. Go to **Configuration > Presettings > Word matching**.
2. Click **Add**.
3. On the **General** tab, determine
 - the name of the word group,
 - whether points are awarded for matches or for non-matches,
 - the area to which the phrase is applied and

- the SCL points awarded.

Inhalt der Wortgruppe

Allgemein Wörter

Name

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

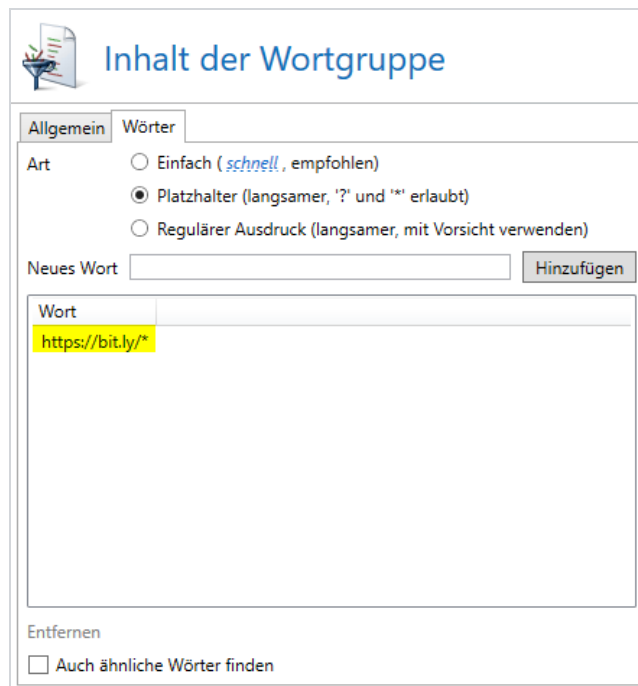
Bereich Betreffzeile
 E-Mail-Inhalt

Punkte
10 SCL-Punkte

4. On the **General** tab, determine

- whether you want to search for exact matches (simple) or use wildcards or regular expressions,
- the words contained in the word list and

- whether you also want to search for similar words.



Inhalt der Wortgruppe

Allgemein Wörter

Art

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

Neues Wort

Wort

- https://bit.ly/*

Entfernen

Auch ähnliche Wörter finden

5. Klicken Sie auf **Finish**.

Realtime block lists

Realtime blocklists (RBL) manage lists of suspicious spam IP addresses. RBLs can be selected individually in the rules.

Adding a new block list

1. Go to **Configuration > Preferences > Realtime block lists**.
2. Click **Add**.
3. Under **Common Settings**, enter a name and description.

4. Under **Blocklist target**, specify

- whether it is an RBL list that is addressed via DNS or HTTP and
- in the Address field either the IP address or the server name of the server to be queried.

5. Under **Responses**, define

- the possible answers of the requested server and their meaning,
- how many SCL points result from it and
- a descriptive error text.



NOTE: A negative value corresponds to bonus points, a positive value corresponds to penalty points. The text of the response may appear in the non-delivery report if the originating server supports this. Thus, the sender of the rejected email knows which blacklist he is on and for what reason. The answer can also be deactivated.

6. Click **Finish**.

Advanced settings

The screenshot displays the 'Advanced settings' section of the NoSpamProxy Command Center. The left sidebar shows a navigation menu with categories: Overview, Monitoring, Identities, Configuration (expanded), and Troubleshooting. Under Configuration, options include Email routing, Rules, Content filter, URL Safeguard, NoSpamProxy components, Connected systems, User notifications, Presettings, and Advanced settings (selected). At the bottom of the sidebar are 'Actions' with 'Refresh' and 'English' options.

The main content area is titled 'Advanced settings' and contains four sections:

- Sensitive data protection:** Sensitive data is **protected**. [Modify](#)
- Monitoring:** Message tracks are stored for **1 month** and their details are stored for **10 days**. Subjects are **recorded**. **Clickable** URL Safeguard visits are stored for **10 days**. Message statistics are stored for **1 year**. Emails are kept on hold for **3 days** when waiting for an encryption key from a partner. [Modify](#)
- Subject flags:** Insert subject flags into the subject line to control the processing of outbound emails.

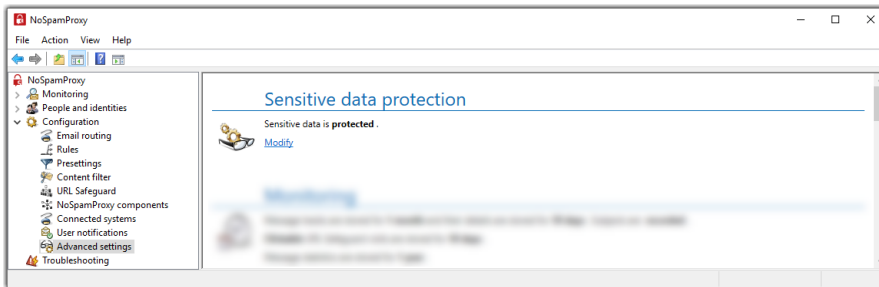
Name	Subject flag	Header	Additional h
De-Mail: Request confirmation of dispatch	Versandbestätigung	X-de-mail-confirmation-of-dispatch	
De-Mail: Request confirmation of receipt	Eingangsbestätigung	X-de-mail-confirmation-of-receipt	
De-Mail: Request confirmation of retrieval	Abholbestätigung	X-de-mail-confirmation-of-retrieve	
De-Mail: Mark email as sender-authenticated	Absenderbestätigt	X-de-mail-authoritative	
De-Mail: Mark email as private	Persönlich	X-de-mail-private	
Attachment password	AP	X-NoSpamProxy-RequireAttachmentPassword	
PDF encryption password	PW	X-enQsig-SymmetricEncryptionPassword	
Number for text message notification	SMS	X-enQsig-SymmetricEncryptionNotificationAddress	

[Modify](#)

Square brackets are used to mark subject flags. Example: [PW:123]
[Modify](#)
- Level of Trust configuration:** 'MAIL FROM' and 'Header-From' sender addresses are evaluated. The address pairing bonus is set to **200** trust points and the domain trust bonus is set to **25** trust points. Domain bonus is **not** granted for emails sent from free email service providers. Email Authentication is required for **all bonuses**. Smart DSN handling is set to **automatic**. Invalid DSNs get **50** detention points. Valid DSNs get **50** bonus points. [Modify](#)

Here you will find configuration options that you usually do not need to adjust.

Sensitive data protection



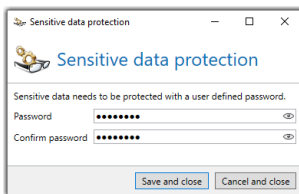
To protect sensitive data such as cryptographic keys or authentication information from being accessed by third parties, you must encrypt them.



NOTE: Once activated, the protection cannot be reversed.

Enabling protection of sensitive data

1. Go to **Configuration > Advanced settings > Sensitive data protection**.
2. Click **Modify**.



3. Enter a password for the protection of sensitive data.
4. Click **Save and close**.

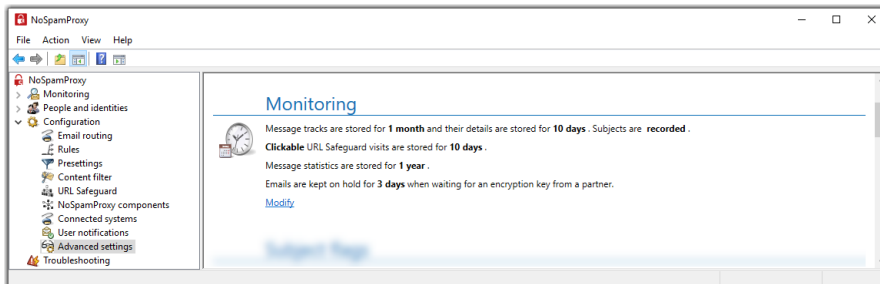


NOTE: You can change the password at a later time.



WARNING: If you forget the password and the configuration with the encrypted password is deleted, there is no way to access the protected data. Always keep a copy of the password in a safe place.

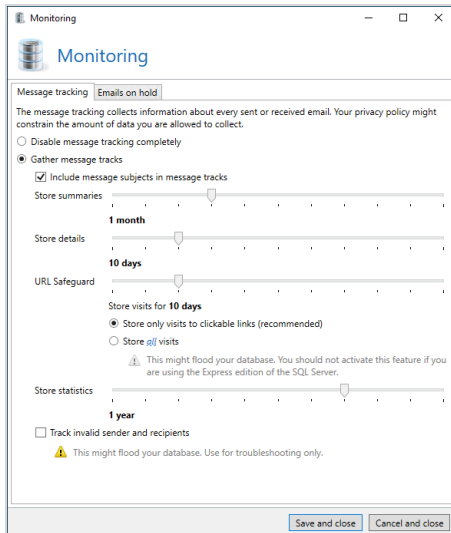
Monitoring



NoSpamProxy can log all connections in the message tracking. This allows you to see how the individual emails were processed.

Activating message tracking

1. Go to **Configuration > Advanced settings > Monitoring**.
2. Click **Modify**.



3. On the **Message tracking tab**, select the **Gather message tracks** option.
4. Configure the following options:

Save the summaries | The time period for which you can track emails. The message summary information only allows you to see in the message tracking overview whether and when the email you are looking for has arrived and whether it has been accepted or rejected.

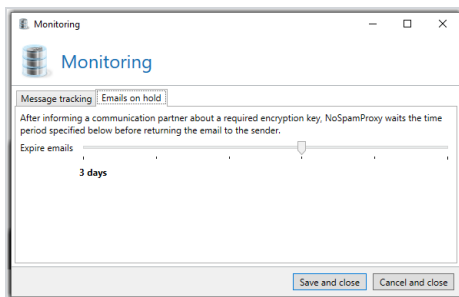
Save the details | The storage duration for the associated message details. In the details you will find the assessment of each filter, information about the origin of the email and the duration of the inspection, as well as other useful information. Since this information makes up the majority of message tracking, it is possible to keep it for a shorter period of time than the summary information.

URL Safeguard | The storage time for visits from clickable links or other URLs such as non-embedded images. If you select the option **Store all visits**, a large

amount of data is generated. You should not activate this option if you are using the Express Edition of Microsoft SQL Server.

Store statistics The period for which you can create reports. To be able to create a meaningful report, we recommend a minimum retention period of 12 months.

5. On the **Emails on hold** tab, configure the retention period for emails that are waiting for an encryption key.



6. Click **Save and close**.

Notes



NOTE: Please consider the data protection regulations existing in your company when configuring this section.



NOTE: In order not to let the database size of the message tracking and reports grow uncontrolled, the Intranet Role cleans up the database on a regular basis. All elements that have exceeded a specified age are deleted from the database.



NOTE: If you want to discard all message tracking records and statistical data, please select the option **Disable message tracking completely** under the **Advanced Settings** of the Gateway Role. In this case no data will be collected. For example, if you only want to record statistical data, select the option Message tracking records are deleted immediately to delete all message tracking records at 2 a.m.



NOTE: If you receive several tens of thousands of emails or spam emails per day, the database size limit may be exceeded with an Express Edition SQL Server. With so many emails, shorter retention periods of message tracking records should be chosen or a SQL Server database should be installed without this limitation.

Subject flags



Depending on the functions you have licensed, different subject flags may be available.

Subject flags are keywords that enable you to control the processing of individual emails. Inserting a keyword into the subject of an email triggers certain actions. These keywords are removed from the subject line before NoSpamProxy sends the message.

Inserting subject flags

- Add the desired keywords in brackets to the subject line at the beginning or end.



NOTE: Spaces and differences between upper and lower case in keywords are ignored.



NOTE: Subject flags must be placed at the beginning or end of the subject line to be processed properly.

Examples of use

EXAMPLE:

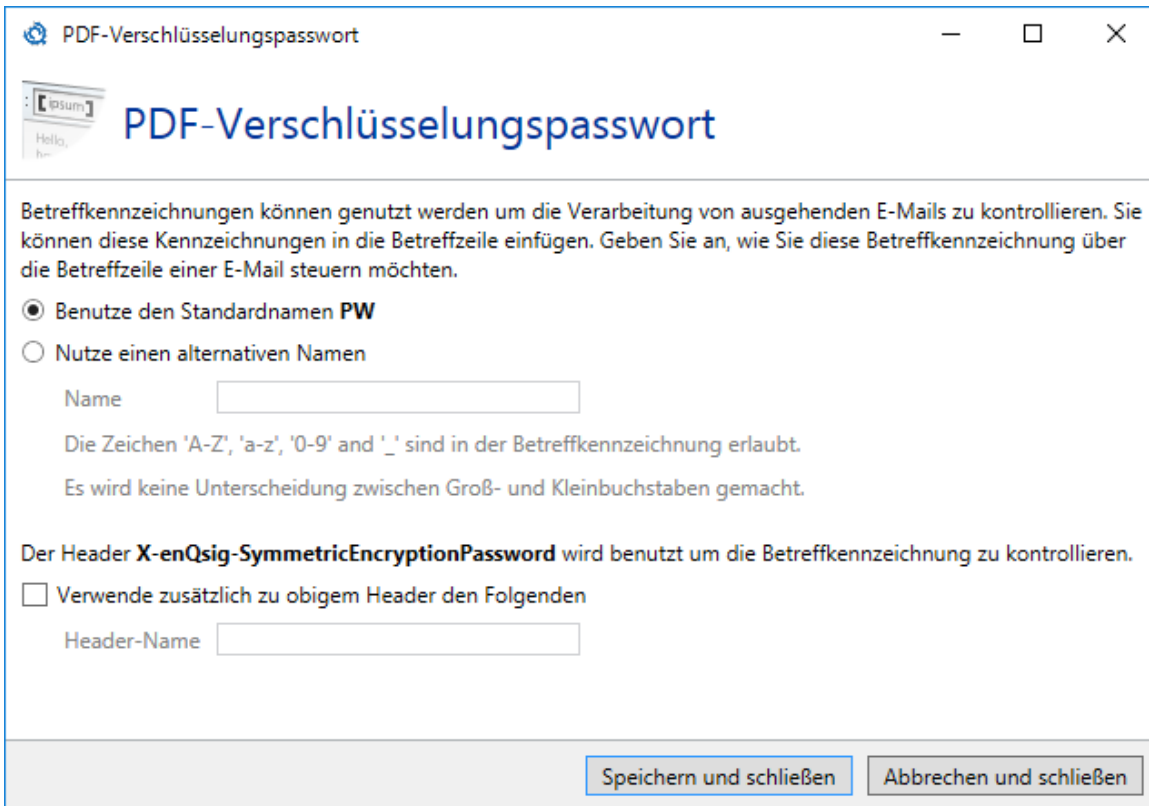
- The following two examples give the same result:
[pw:geheim4312] I hereby send you the encrypted document
[PW : secret4312] I hereby send you the encrypted document
- Several markings in one bracket at the same time:
Several flags in one bracket:[Unencryl am sending you the encrypted document
- Several markings simultaneously in different brackets:
Several flags in one bracket:[Unencryl am sending you the encrypted document

Available subject flags

[Delivery confirmation]	De-Mail: Requests a dispatch confirmation from De-Mail. Corresponds to a registered letter.
[Receipt confirmation]	De-Mail: Requests a receipt confirmation from De-Mail. Corresponds to a registered letter.
[Collection confirmation]	De-Mail: Requests a collection confirmation from De-Mail.
[Confirmed by sender]	De-Mail: Adds the status Authenticated by sender to De-Mails.
[Personal]	De-Mail: Adds the status Private to De-Mails. Corresponds to a Registered letter to addressee only for letters.
[SMS:No]	Text message notification: The phone number is used in the Protect attachments with a password action to send a PDF password entered by one of the configured text message providers directly to the recipient's mobile phone via text message. If no password has been assigned, this number is ignored.
[PWreport]	Enforce password notification: The set or generated password of the Protect Attachments with a password action is always sent to the sender of the email when using this subject flag.
[AP]	Attachment Password: Protects all attachments with a password that must be entered by the recipient before downloading the attachments. This feature is available in NoSpamProxy Large Files.

Customising subject flags

You can customize subject flags to your needs and reset them to their default values at any time.



The screenshot shows a Windows-style dialog box titled "PDF-Verschlüsselungspasswort". The title bar includes a minimize button, a maximize button, and a close button. The main content area has a header with a small icon and the text "PDF-Verschlüsselungspasswort". Below the header, there is a paragraph of German text explaining that subject flags can be used to control outgoing email processing. Two radio buttons are present: "Benutze den Standardnamen PW" (selected) and "Nutze einen alternativen Namen". The second option has a text input field for "Name" and two lines of explanatory text. Below this, another paragraph states that the header "X-enQsig-SymmetricEncryptionPassword" is used for control. A checkbox "Verwende zusätzlich zu obigem Header den Folgenden" is unchecked, with a corresponding text input field for "Header-Name". At the bottom right, there are two buttons: "Speichern und schließen" and "Abbrechen und schließen".



WARNING: In the NoSpamProxy Outlook Add-in you can configure the subject flags to be used instead of the X headers. In this case, do not make any changes in this area. Otherwise, the add-in will no longer work.

Particularities when automatically sending emails

When sending emails automatically, you can also use email headers instead of subject flags.

Proceed as follows:

1. Go to **Configuration > Advanced settings > Subject flags**.
2. Open the desired subject flag.
3. Check the box **In addition to the header above, also use this header**.
4. Enter the desired header into the input field.
5. Click **Save and close**.

The specified header is now used in addition to the regular header.

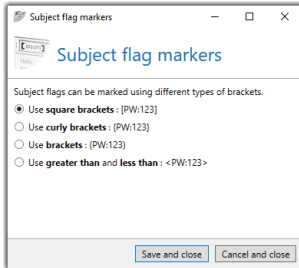
NoSpamProxy Outlook Add-in

You can also install the Outlook Add-In for NoSpamProxy instead of the subject flags. The Outlook Add-in is used with Microsoft Outlook instead of the subject flags.

Customising markers for subject flags

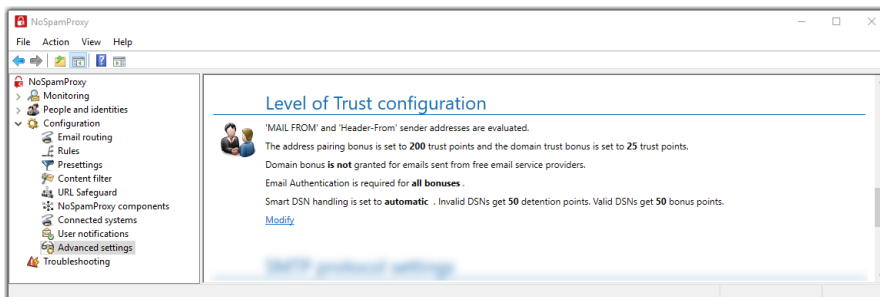
By default, square brackets are used to indicate the subject flags. To change this, proceed as follows:

1. Go to **Configuration > Advanced settings > Subject flags**.
2. Click **Modify**.



3. Select the desired marker type.
4. Click **Save and close**.

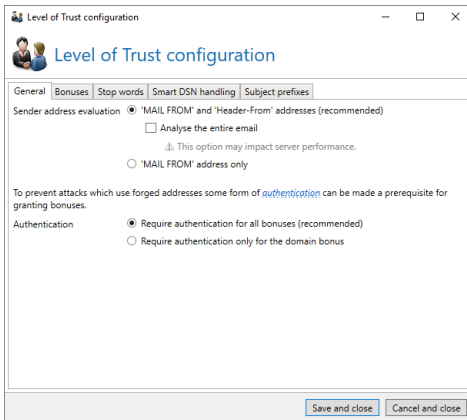
Level of trust configuration



To configure Level of Trust, proceed as follows:

1. Go to **Configuration > Advanced settings > Level of Trust configuration**.
2. Click **Modify**.
3. Make the settings on the individual tabs (see below).
4. Click **Save and close**.

General tab



- **Sender address evaluation** | Determines which addresses are used for the analysis if the **MAIL FROM address** and the **header FROM address** are different. If both addresses are verified, the email will be rejected if either address is not trustworthy.

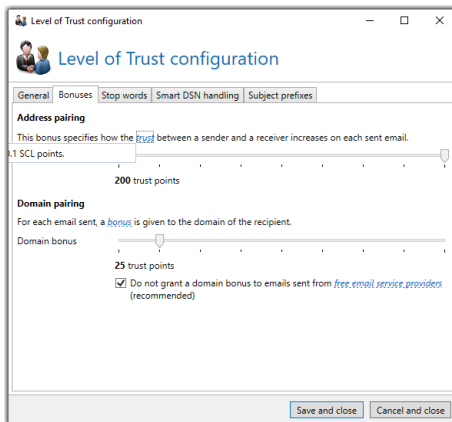
- 'MAIL FROM' and 'Header From' addresses (recommended)
 - (Optional) The entire email (may affect server performance)



NOTE: If the entire email is analysed, it is evaluated using all the filters configured in the respective rule. The result of this evaluation is correspondingly more accurate than the sole evaluation of 'MAIL FROM' and 'Header-From' and can overrule the latter evaluation. As all emails are received in full, this option can have a negative impact on server performance.

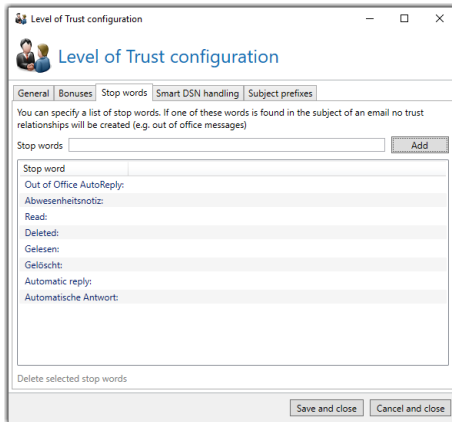
- 'MAIL FROM' addresses only
- **Authentication** | Determines whether successful authentication through DKIM, S/MIME and SPF checks is a prerequisite for all bonuses or only for the domain bonus (see **Bonuses** tab).

Bonuses tab



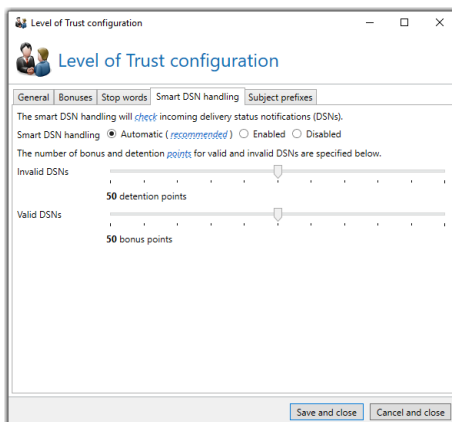
- **Address pairing**| Determines by how many points the trust between a sender and a recipient is increased per email. With the slider you can set a value between 0 and 200. One point corresponds to (-0.1) points for the **Spam Confidence Level (SCL)**. For each email to external addresses, not only the so-called address relationship bonus is increased, but also a bonus for the respective recipient domain.
- **Domain pairing**| Determines how many points the domain bonus is increased by. This value should be smaller than the bonus for address relationships. You can set a value between 0 and 200 with the slider. One point corresponds to (-0.1) points for the **Spam Confidence Level (SCL)**.

Stop words tab



Once the Gateway Role finds any of the words defined here in the subject of an email to external addresses, both the address relationship bonus and the domain bonus remain unchanged and are not increased. This is a useful setting for automatically generated emails such as out-of-office notes.

Smart DSN handling tab



Smart DSN handling checks Delivery Status Notifications (DSNs) to local addresses. Since NoSpamProxy knows which emails have been sent from the company, it can also determine whether a corresponding email has left the company for the DSN that is currently available.

- **Smart DSN handling|** Determines if and how intelligent DSN filtering applied.
- **Automatic|** NoSpamProxy first checks whether there are any elements in the Level of Trust database that are older than seven days. Only then does NoSpamProxy evaluate inbound DSNs.
- **Enabled|** NoSpamProxy evaluates the DSN in every case; even if no data records exist in the Level of Trust database.
- **Disabled|** The intelligent DSN filtering is disabled.

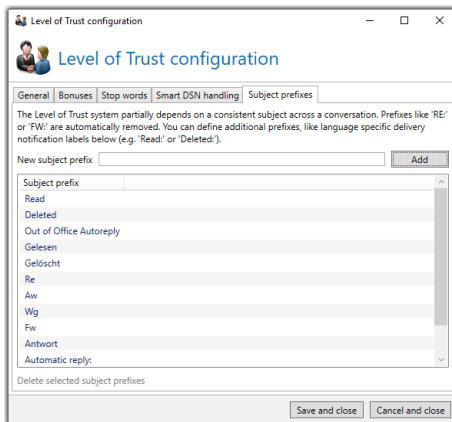
EXAMPLE:

A DSN arrives and NoSpamProxy determines that the original message for that DSN was sent from **schmidt@example.com** to **schulze@netatwork.de**. NoSpamProxy now checks whether there is an address pair **schmidt@example.com/schulze@netatwork.de** in the Level of Trust database.

If this is not the case, the DSN in question may not be valid and receives penalty points. If a suitable address pair is found, the DSN receives bonus points. For this analysis to take place, two conditions must be met:

- There must be an RFC-compliant DSN. This means that the original message is attached to the DSN so that NoSpamProxy can determine the original address pair.
- It must be ensured that the mail gateway knows all emails to external addresses. In networks with distributed Internet connections, this can be a problem under certain circumstances.

Subject flags tab



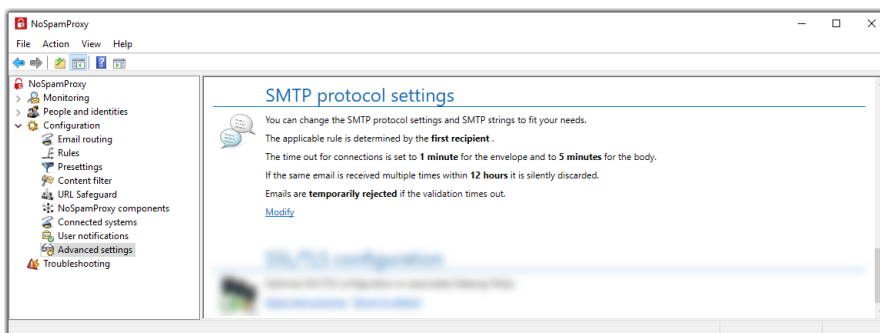
Level of Trust partially requires consistent subject lines over a conversation. Subject prefixes such as **RE:** or **FW:** must be removed for this purpose. Here you configure all prefixes used by your email system.

See

Level of Trust

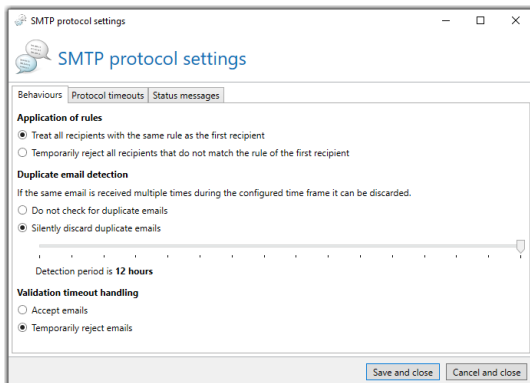
Points allocation for domains for Level of Trust

SMTP protocol settings



The protocol settings control the behaviour when receiving emails, the SMTP timeouts and the SMTP status messages.

Behaviour tab



Application of rules

If an email is sent to multiple recipients, different rules may apply to the email. NoSpamProxy can force the sending system to send a separate email for each individual recipient. This setting prevents conflicts caused by emails sent to multiple recipients, e.g. if an email is sent to two recipients via one connection and two different rules would apply.



NOTE: By using SMTP, it is not possible to provide independent feedback for individual recipients. Only the entire connection can be terminated.

Treat all recipients with the same rule as the first recipient| The rule that applies to the first recipient is applied to all recipients of this email.

Temporarily reject all recipients that do not match the rule of the first recipient| All recipients that do not match the rule of the first recipient are temporarily rejected. NoSpamProxy sends the error message **Too many recipients** to the inbound system. A new delivery attempt will be made for the rejected emails. This allows NoSpamProxy to apply the appropriate rule for each recipient. However, the emails are delivered multiple times by the sender.



NOTE: This function allows you to control the email assessment. Disadvantages are multiple transmissions and not fully RFC-compliant behavior.

Duplicate email detection

NoSpamProxy recognises if the same email is received multiple times. Sending the same email repeatedly usually occurs due to incorrect configuration such as email loops. You can set whether these emails should be discarded or not, as well as the time frame for the detection.

Do not check for duplicate emails| There is no check for duplicate emails.

Silently discard duplicate emails| Duplicate emails received within the configured time period are silently discarded.

Validation timeout handling

You can determine how emails whose validation time exceeds the maximum values configured under Protocol timeouts are handled.

Accept emails | E-mails whose validation time exceeds the maximum values are accepted.

Temporarily reject emails | Emails whose validation time exceeds the maximum values are temporarily rejected.

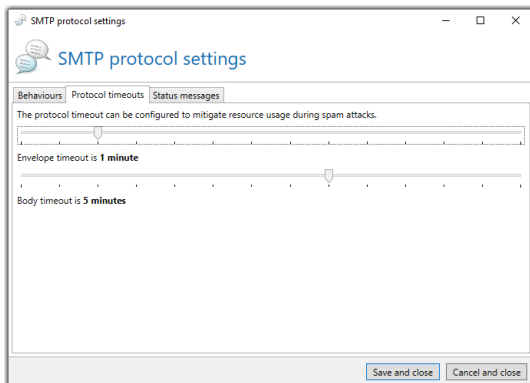


NOTE: If the malware scan is not completed when a validation timeout occurs, the respective email will always be temporarily rejected.



NOTE: Emails are rejected in any case if they were previously rejected temporarily or permanently by an action.

Protocol timeouts tab



NOTE: Adjusting the timeouts has a major impact on the resource requirements of your server during heavy email traffic.

In the SMTP protocol timeout settings section you can specify when NoSpamProxy disconnects in case of no activity. This is configured for two sections within the SMTP protocol.

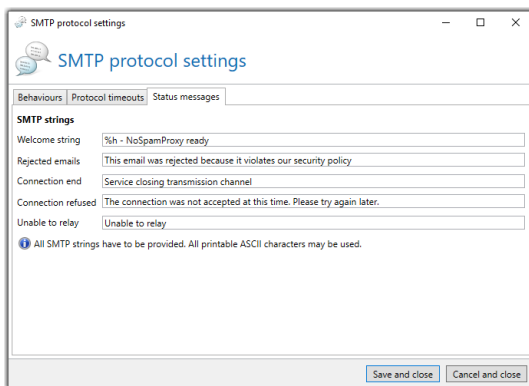
Envelope timeout| Defines the timeout for the commands within the so-called envelope. This affects all commands up to the DATA command (HELO/EHLO, MAIL FROM, RCPT TO).

Body timeout| As soon as the DATA command has been sent, the setting under **Body timeout** applies.



NOTE: It makes sense to separate the timeouts, since timeouts can occur more frequently than with the envelope when the body part is transferred by means of filters and actions connected in between. This is transmitted very promptly and smoothly during a normal transmission. A longer waiting time in this part of the email transfer rather indicates a DoS attack or similar. Therefore you have the possibility to reduce the timeout of the envelope part in case of emergency.

Status messages tab



The status messages determine which texts (SMTP strings) NoSpamProxy sends to other servers. The SMTP replies are standard specifications in the SMTP handshake, which are usually not visible to the normal user. Nevertheless, it may be useful to change the information as required. This can assist administrators with troubleshooting and analysis.

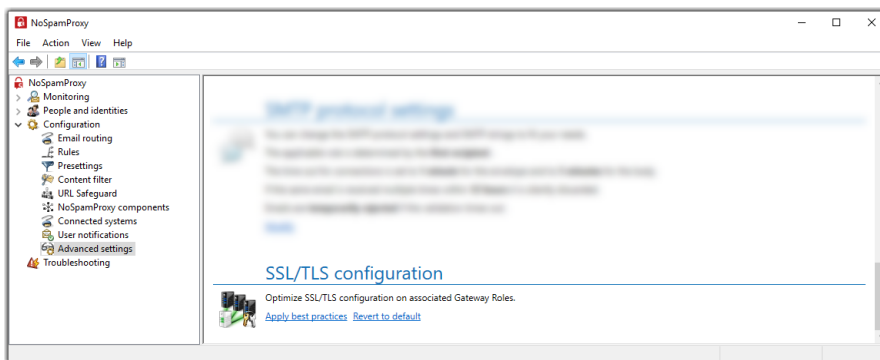
The messages Rejected emails and Blacklisted address are for example important information for the sender of a blocked email.

- To change a message, click in the corresponding input field and change the text.



NOTE: You must not use umlauts for SMTP messages. Umlauts are not supported by the SMTP protocol used.

SSL/TLS configuration



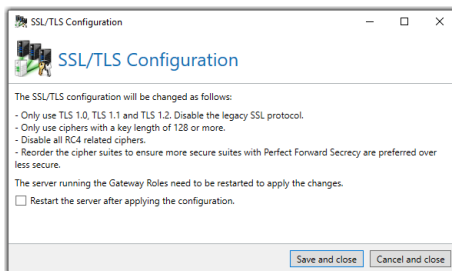
With transport encryption, the connection is secured via SSL or TLS. The Gateway Role accesses the operating system. Its settings are used for connections.



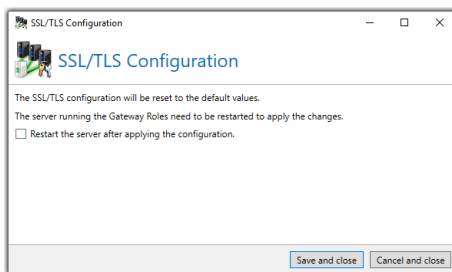
NOTE: Recently, some encryption methods (e.g. DES or RC4) have proven to be unsafe. It is therefore advisable to deactivate them. Some cipher suites support a procedure called Perfect Forward Secrecy. In short, this prevents the contents of connections from possibly being decrypted by unauthorized third parties, even if the private key of the server certificate is known. By default, Windows does not use these methods preferentially.

Adjusting SSL/TLS configuration

You can apply the recommended settings here in the interface. For the changes to take effect, the server must be restarted:



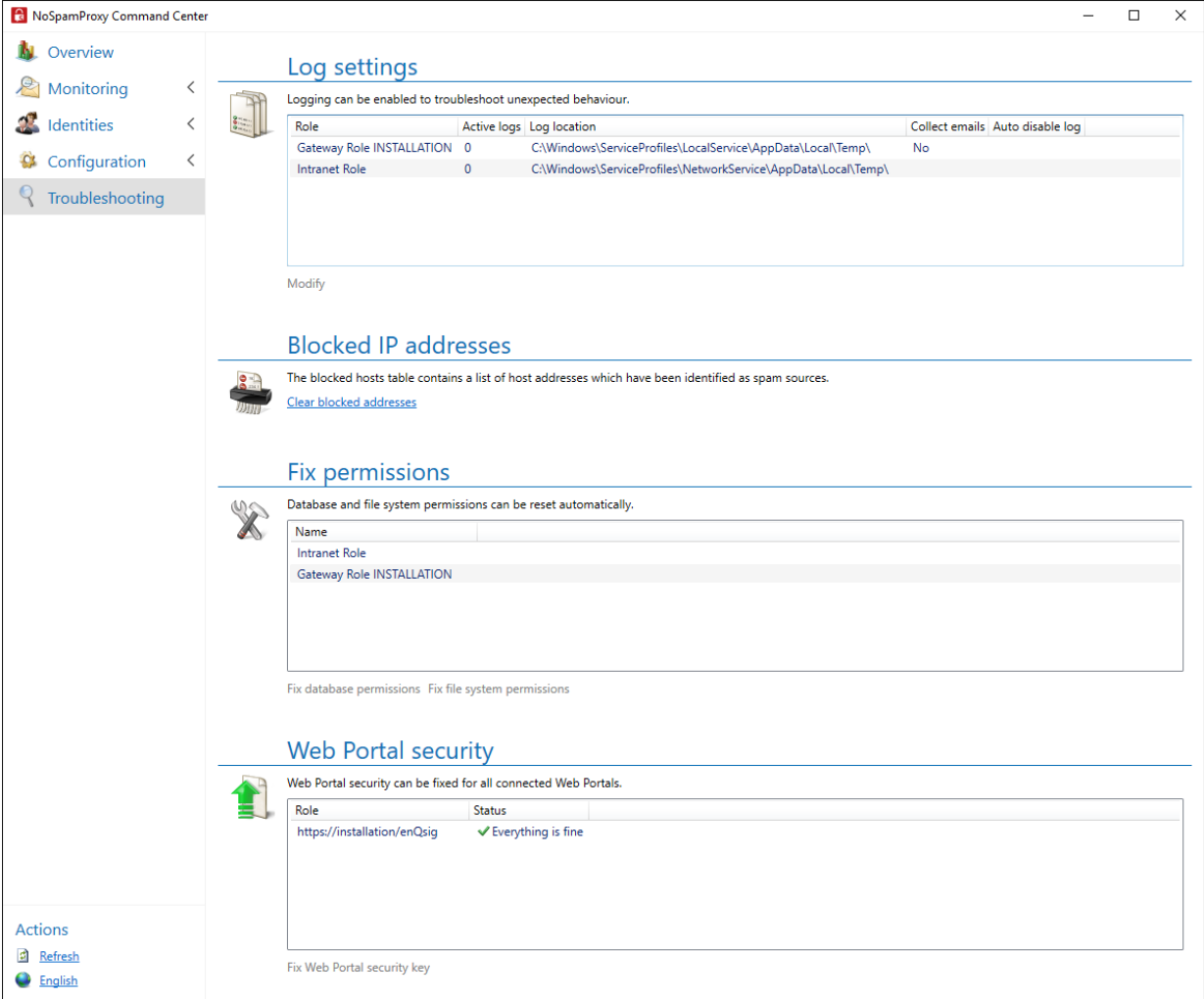
You can also use this section to restore the default values of Windows:





NOTE: This is a system-wide change which may also affect other applications.

Troubleshooting



This area provides access to tools to create activity logs or even a new database for the individual roles of NoSpamProxy. It may be necessary to create a new database if the old database has been damaged.

Log settings 224

Blocked IP addresses	226
Fixing permissions	227
Market communication with AS4	228
Step 1: Activating the AS4 module	229
Step 3: Creating the required Windows group	231
Step 4: Configuring the key management service	232
Configuring the service address	232
(Optional) Adding an HSM	233
(Optional) Configuring a token	234
Frequently asked questions	235
Step 5: Configuring your market partner account	237
Adding your market partner account	237
Creating a certificate request for AS4 communication	239
Importing certificates	240
Changing settings	241
Step 6: Activating market partner communication	242
Requesting outbound AS4	242
Confirm inbound AS4	243
Testing AS4 connectivity	244
AS4 Message tracking	246
Adding market partners manually	251
Editing the key storage	253
Configuring the storage location for EDIFACT documents	254

Log settings

To change the log settings for the respective Gateway or Intranet Role, proceed as follows:

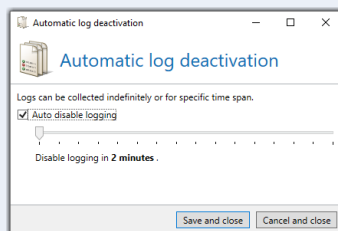
1. Go to **Troubleshooting > Log settings**.
2. Select the desired role.
3. Click **Modify**.
4. Make the desired settings (see below).
5. Click **Save and close**.

Log settings tab

- **Log path**| The location for the log files.
- **Log categories**| The categories for which you want to enable logging.



NOTE: Depending on the categories you select here, the log files can very quickly grow to several hundred megabytes in size. Select a drive for the files that has enough available disk space. We recommend that you create the log only for a fixed period of time. To do this, click **Change** and make the desired setting.



I Debug settings tab

You can save all emails to disk before and after processing by NoSpamProxy.

- **Storage location**| The storage location for emails as an absolute path on the Gateway Role.



NOTE: Storing all emails on the hard disk takes up a lot of space and can cause severe performance degradation of the server. Therefore, use this function only for error diagnosis and switch it off again afterwards.

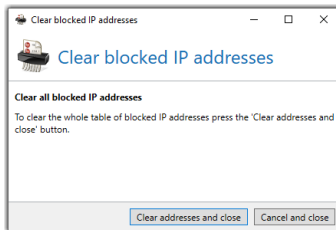


NOTE: This tab is only available for Gateway Roles.

Blocked IP addresses

NoSpamProxy blocks the sending gateway for 30 minutes by default after receiving a spam emails. If by mistake a trustworthy IP address is added to this blacklist, you can delete the list of blocked servers here.

1. Go to **Troubleshooting > Blocked IP Addresses**.
2. Click **Clear blocked addresses**.
3. Click **Clear addresses and close**.

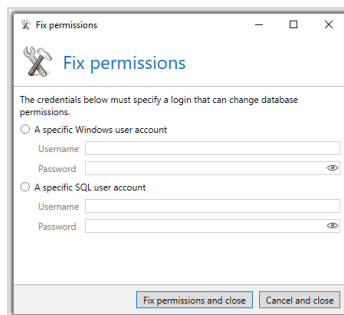


Fixing permissions

If the file system permissions for NoSpamProxy have been changed by third-party programs, for example, so that the function is restricted, you can correct this here.

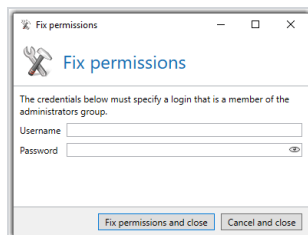
1. Go to **Troubleshooting > Fix permissions**.
2. Select the desired role.
3. Click either **Fix database permission** or **Fix file system permission** .

■ Fixing the database



The screenshot shows a dialog box titled "Fix permissions" with a wrench and screwdriver icon. The main heading is "Fix permissions". Below this, a message states: "The credentials below must specify a login that can change database permissions." There are two radio button options: "A specific Windows user account" and "A specific SQL user account". Each option has a "Username" and "Password" input field. The "Password" fields have an eye icon to toggle visibility. At the bottom, there are two buttons: "Fix permissions and close" and "Cancel and close".

■ Fixing file system



The screenshot shows a dialog box titled "Fix permissions" with a wrench and screwdriver icon. The main heading is "Fix permissions". Below this, a message states: "The credentials below must specify a login that is a member of the administrators group." There are two input fields: "Username" and "Password". The "Password" field has an eye icon to toggle visibility. At the bottom, there are two buttons: "Fix permissions and close" and "Cancel and close".

4. Make the desired changes.
5. Click **Fix permissions and close**.

Market communication with AS4

Market communication (MaKo) stands for the exchange of data between market participants in the German energy market. NoSpamProxy supports automated EDIFACT market communication for the energy industry according to the specifications of the cross-association expert group EDI@Energy.

I How to set up AS4 market communication in NoSpamProxy

Three steps are necessary to set up the sending and receiving of AS4 messages in NoSpamProxy:

Step 1: Activating the AS4 module

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

Step 3: Creating the required Windows group

Step 4: Configuring the key management service

Step 5: Configuring your market partner account

Step 6: Activating market partner communication

Step 1: Activating the AS4 module

To set up AS4 market communication, you must activate the relevant components **before installing** NoSpamProxy. Otherwise they will not be displayed during installation.

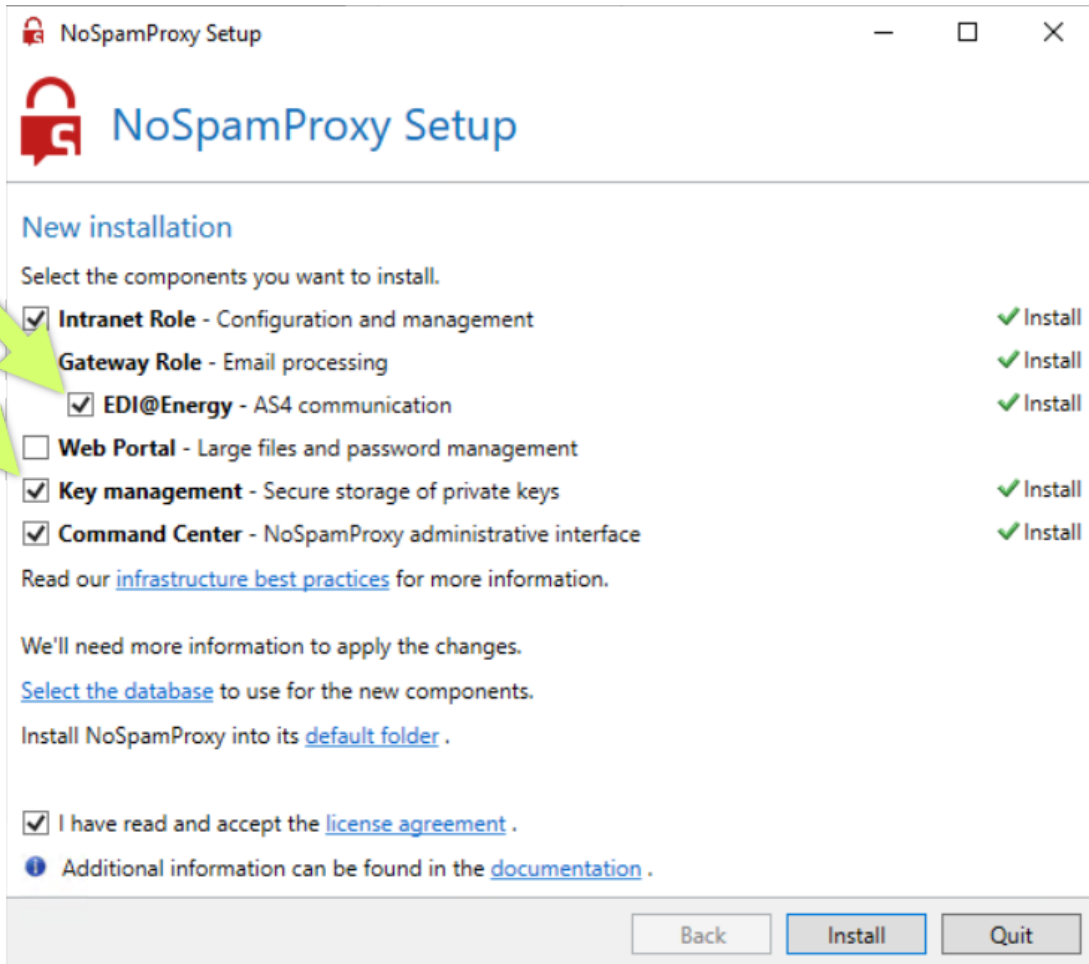
- Execute the following command line parameter in the directory in which the NoSpamProxy installation file is located:

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

The NoSpamProxy installation will now start. During installation, make sure that select the components

- **EDI@Energy** and
- **Key management**

during setup.



Step 3: Creating the required Windows group

After installing NoSpamProxy Server, you must create the required Windows group **NoSpamProxy EDI at Energy Administrators** via PowerShell.

1. Switch to the system on which the Intranet Role is installed.
2. Execute the cmdlet `New-NspEdiAtEnergyAdministratorsGroup` in PowerShell.

This cmdlet does the following two things:

- It creates the Windows group **NoSpamProxy EDI at Energy Administrators**.
- It assigns the created group to the **EdiAtEnergyAdministrator** role.

You can add users to the new Windows group using the MMC **Local Users and Groups**. If the assignment of the group to the role fails, you must assign the group to the role manually. To do this, enter the following command in PowerShell:

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



NOTE:

- The environment must be a NoSpamProxy Server installation.
- EDI@Energy must be licensed.
- If a Windows group with the same name already exists, the cmdlet will fail.

Step 4: Configuring the key management service

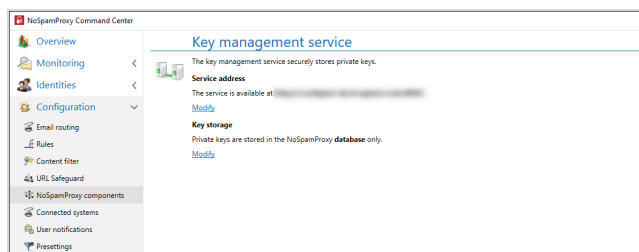
To set up the sending and receiving of AS4 messages in NoSpamProxy, you must first enter the service address of the key management service and optionally add a hardware security module (HSM) in NoSpamProxy.



NOTE: The key management service is used for the secure storage of private keys. For maximum security, we still recommend the use of an HSM. See below, [Who needs to use an HSM?](#)

Configuring the service address

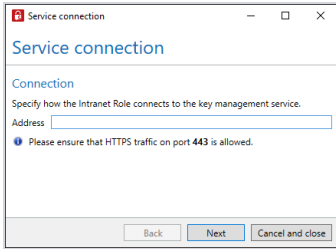
1. The service address is the address at which the Intranet Role connects to the key management service.
2. In the NoSpamProxy Command Centre, go to **NoSpamProxy components > Key management service** and click **Modify**.



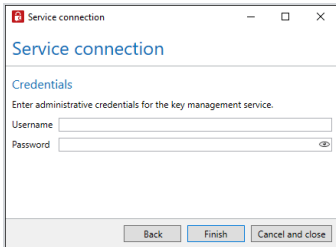
3. Enter the service address under **Connection**.



NOTE: The default address is `https://localhost:6064`. In any case, make sure that HTTPS traffic is permitted on port 6064.



4. Under **Credentials**, enter the administrative user information for the service.

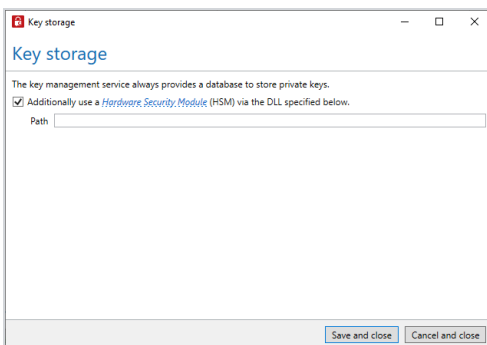


5. Click **Finish**.

! (Optional) Adding an HSM

If you also want to use an HSM to store your private keys, add it here.

1. In the NoSpamProxy Command Centre, go to **Configuration > NoSpamProxy components > Key management service**.
2. Under **Key storage**, click **Modify**.
3. Tick the **Additionally use a Hardware Security Module (HSM) [...]** box.



4. Enter the path to the HSM DLL file.
5. Click **Save and close**.

The **Configured tokens** area now appears under **Key management service**.



NOTE:

The following requirements must be met before you can use an HSM to store your private keys:

- The HSM must support the **PKCS #11 standard**.
- The HSM must use the **Elliptic Curve Brainpool P256r1 standard** for key generation (CKM_EC_KEY_PAIR_GEN).
- The HSM must use the key derivation function **SP-800 (CKD_SHA256_KDF_SP800)** for key derivation (CKM_ECDH1_DERIVE).

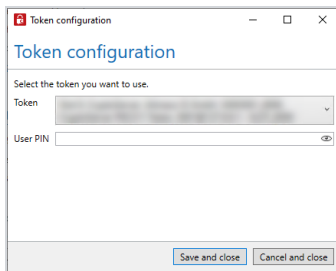
I (Optional) Configuring a token

If you are using an HSM and have added it, you can access the tokens of the HSM and configure the desired token.

1. Under **Configured tokens**, click **Modify**.



2. Under **Token**, select the desired token from the drop-down menu.



3. Enter the corresponding PIN under **User PIN**.
4. Click **Save and close**.

The HSM is now connected.

I Frequently asked questions

Who needs to use an HSM?

With regard to the use of an HSM, the version of the [Smart Metering PKI certificate policy](#) dated 25 January 2023 (version 1.1.2) states that "[...] passive EMT cryptographic modules [must] be used that are at least compliant with the [Key Lifecycle Security Requirements - Security Level 1](#). [...] Each market participant must derive the specific requirements for the cryptographic modules for itself in accordance with the security concept to be drawn up by it."

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

What are passive EMTs?

Passive external market participants (EMT) are defined in the Smart Metering PKI certificate policy 1.3.3.4 as market participants that receive or exchange data from the smart metering gateways (SMGWs) but do not control these devices.

What are active EMTs?

An EMT that uses an SMGW to address downstream devices (Controllable Local Systems, CLS) is referred to as an active EMT.

What are Security Level 1 cryptographic modules?

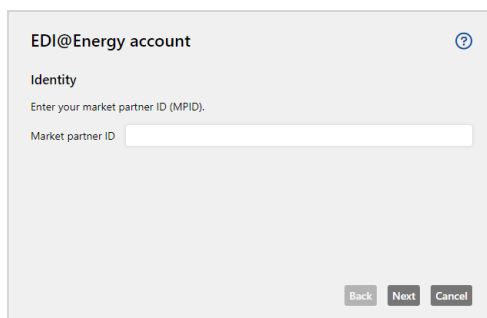
Cryptographic modules of security level 1 can be operated as software or servers with two-factor authentication and physically restricted access. A random number generator of classes NTG.1, DRG.4 or PTG.3 in accordance with AIS 20/31 must be used to generate random numbers for key generation as well as for signature and encryption.

Step 5: Configuring your market partner account

In this step, you store the account associated with your market partner ID (MPID) in NoSpamProxy, create the certificate requests and import the required certificates.

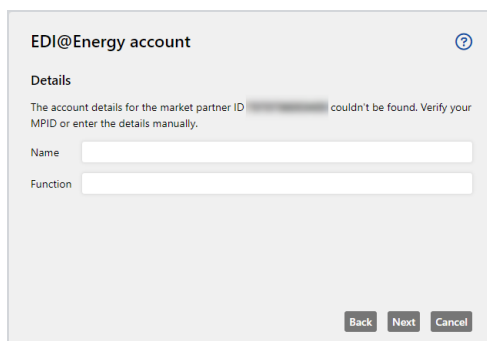
Adding your market partner account

1. Open the NoSpamProxy Web App.
2. Go to **EDI@Energy > Settings > Corporate EDI@Energy accounts**.
3. Click **Add**, enter your MPID under **Identity** and click **Next**.



The screenshot shows a web form titled "EDI@Energy account" with a help icon. Under the "Identity" section, there is a prompt "Enter your market partner ID (MPID)." and a text input field labeled "Market partner ID". At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

4. Under **Details**, enter the name associated with your account and your function and click **Next**.



The screenshot shows the "EDI@Energy account" form with the "Details" section active. A message states: "The account details for the market partner ID [redacted] couldn't be found. Verify your MPID or enter the details manually." Below this message are two text input fields labeled "Name" and "Function". At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

- Under **Routing**, enter the external **end point** for AS4 communication and the mailbox used for the process type **Marktprozesse**. Also enter (if used)
 - the email address of the internal mailbox for '**Redispatch 2.0**' messages,
 - the email address of the internal mailbox for '**Fahrplan**' messages and
 - the **Energy Identification Code (EIC)**.

The screenshot shows the 'EDI@Energy account' configuration page, specifically the 'Routing' section. The page title is 'EDI@Energy account' with a help icon. The 'Routing' section explains that the external endpoint is used for AS/4 messages. It includes a text input for 'External endpoint'. Below this, a note states 'A dedicated mailbox is used for each process type.' There are three main sections for process types: 'Marktprozesse' with a 'Select domain' dropdown; 'Process 'Redispatch 2.0' messages' with an 'Internal mailbox' dropdown; and 'Process 'Fahrplan' messages' with an 'Internal mailbox' dropdown. An 'EIC' text input is also present. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

- Under **Certificate details**, enter the name, the extension (optional), the country code and the email address used in the certificate.

The screenshot shows the 'EDI@Energy account' configuration page, specifically the 'Certificate details' section. The page title is 'EDI@Energy account' with a help icon. The 'Certificate details' section explains that the common name (CN) is derived from the information below. It includes a 'Name' text input with 'NewAccount', an 'Extension (optional)' text input with 'MAK', and a note that the common name will be 'NewAccount.EMT.MAK'. There is a 'Country' section with a 'Country code' text input with 'DE'. A 'Contact information' section explains that the certificate contains an email address, with an 'Email address' text input. At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons.

- Click **Finish**.

Your account is now stored in NoSpamProxy.

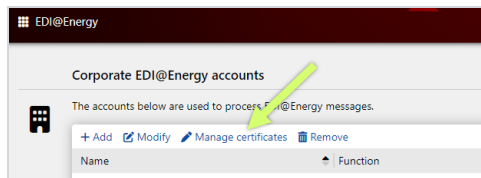


NOTE:

- The path of the AS4 endpoint must end with **/as4**.
- The port of the AS4 endpoint is 6063. If a reverse proxy or a network rule is present, you must change the port to 443.
- The port must be accessible from outside without the firewall intervening.
- The AS4 service should be located within the DMZ, i.e. it should be able to send to any address and any port.

Creating a certificate request for AS4 communication

1. Go to **EDI@Energy > Settings > Corporate EDI@Energy accounts**.
2. Select the relevant account, click **Manage certificates** and then **Create request**.



3. Check that the information displayed is correct and click **Create**.

Create certificate requests ⓘ

The certificate signing requests (CSR) will be created using the data below.

Subject

Common name [redacted]

Organization **SM-PKI-DE**

Organisational unit [redacted]

Country [redacted]

Subject alternative name

URI [redacted]

DNS [redacted]

Email address [redacted]

Create **Cancel**

4. Download the CSR files required for the request.
5. Submit the CSR files to a Sub-CA subordinate to the Root-CA of the Smart Metering PKI.



A list of the sub-CAs registered with the Root CA of the Smart Metering PKI can be found on the page Current registrations with the SM-PKI Root CA of the BSI.

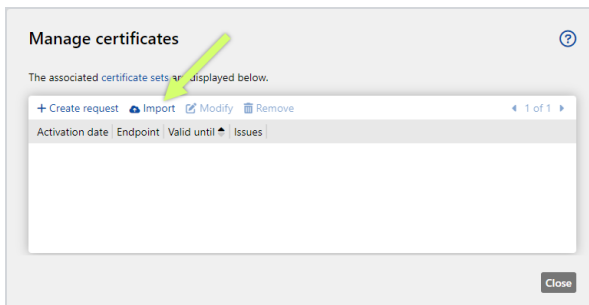
Importing certificates

As soon as the certificates have been issued and are available, you must import them.

1. Go to EDI@Energy > Settings > Corporate EDI@Energy accounts.
2. Select the relevant account and click **Manage certificates**.



3. Click **Import**.



4. Select the respective certificates and click **Import**.

Once the certificates have been successfully imported, the status **Ok** is displayed for the respective market partner.

| Changing settings

To change the settings later, select the relevant account and click

- **Modify** to adjust the external endpoint and the internal recipient or
- **Manage certificates** to import additional/other certificates.

Step 6: Activating market partner communication

In this step, you activate the outbound and inbound AS4 communication.

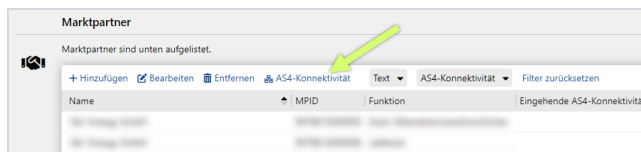


NoSpamProxy automatically downloads the current list of all market partners on a regular basis.

Requesting outbound AS4

To activate outbound AS4 communication with a market partner, you must make a corresponding request.

1. Go to **EDI@Energy > Market partners**.
2. Select the desired market partner and click **AS4 connectivity**.

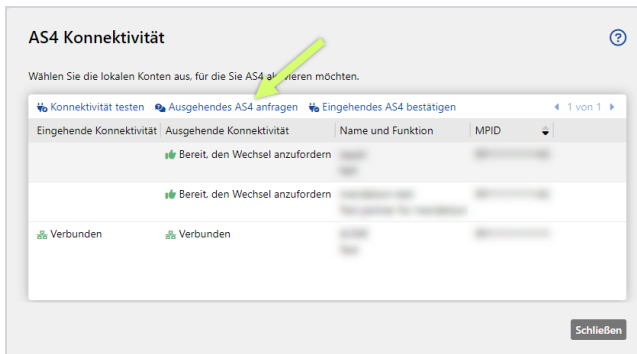


3. Select the corporate EDI@Energy account you have stored for which you want to activate AS4 communication with the market partner.



NOTE: Under **Outbound connectivity**, the message **Ready to request switch** must be displayed. Otherwise you cannot request the switch.

4. Click Request outbound AS4.

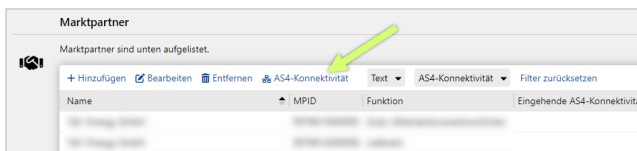


As soon as the market partner has confirmed the switch to AS4, the message **Connected** is displayed under **Outbound connectivity**. NoSpamProxy then only accepts outbound EDI messages via AS4. This process cannot be reversed.

Confirm inbound AS4

To activate inbound AS4 communication with a market partner, you must confirm the corresponding request from the market partner.

1. Go to **EDI@Energy > Market partners**.
2. Select the desired market partner and click **AS4 connectivity**.

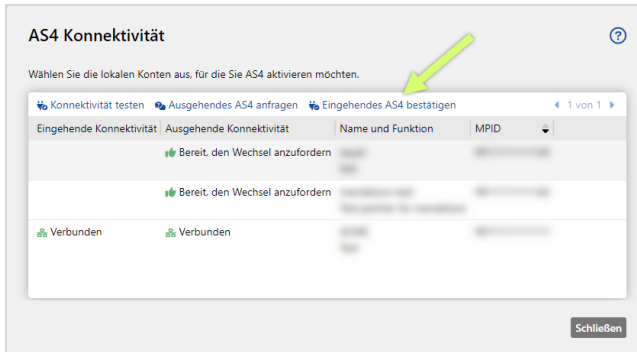


3. Select the corporate EDI@Energy account you have stored for which you want to activate AS4 communication with the market partner.



NOTE: The message **Request pending** must be displayed under **Inbound connectivity**.

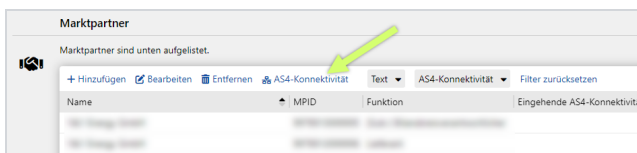
4. Click **Confirm inbound AS4**.



As soon as you have confirmed the switch to AS4, the message **Connected** is displayed under **Inbound connectivity**. NoSpamProxy then only accepts inbound EDI messages via AS4. This process cannot be reversed.

Testing AS4 connectivity

1. Go to **EDI@Energy > Market partners**.
2. Select the desired market partner and click **AS4 connectivity**.





Information on AS4 connectivity is displayed for the individual corporate EDI@Energy accounts you have stored.

3. If there are no certificate errors: Click **Test connectivity**.

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

AS4 Message tracking

AS4 messages are displayed in AS4-specific message tracking.

Under **EDI@Energy > Message tracking** you will find general information as well as information on AS4 conformity.

Icons used

- | Compliance: Complies with the specifications of the AS4 guidelines.
- | No compliance: Does not meet the specifications of the AS4 guidelines.
- 🌐| Received from the Internet
- 🏢| From a corporate email server



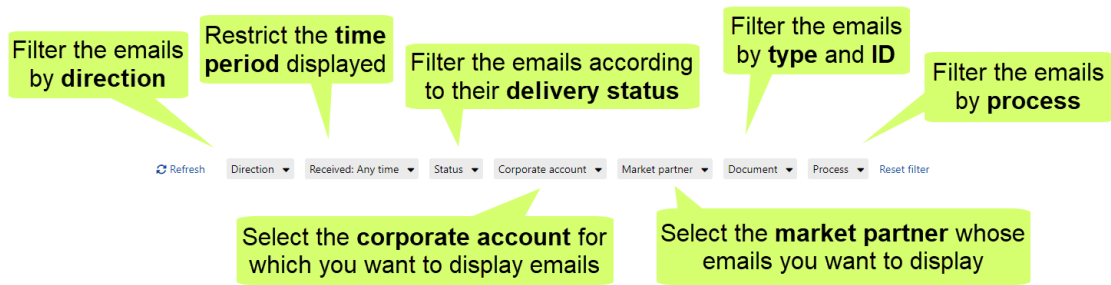
TIP: Details on the compliance of an email can be found on the **Compliance** tab in the detailed view of a message track.

Rearranging columns

To change the order of the displayed columns, drag the respective column and drop it in the desired place.

Filtering emails

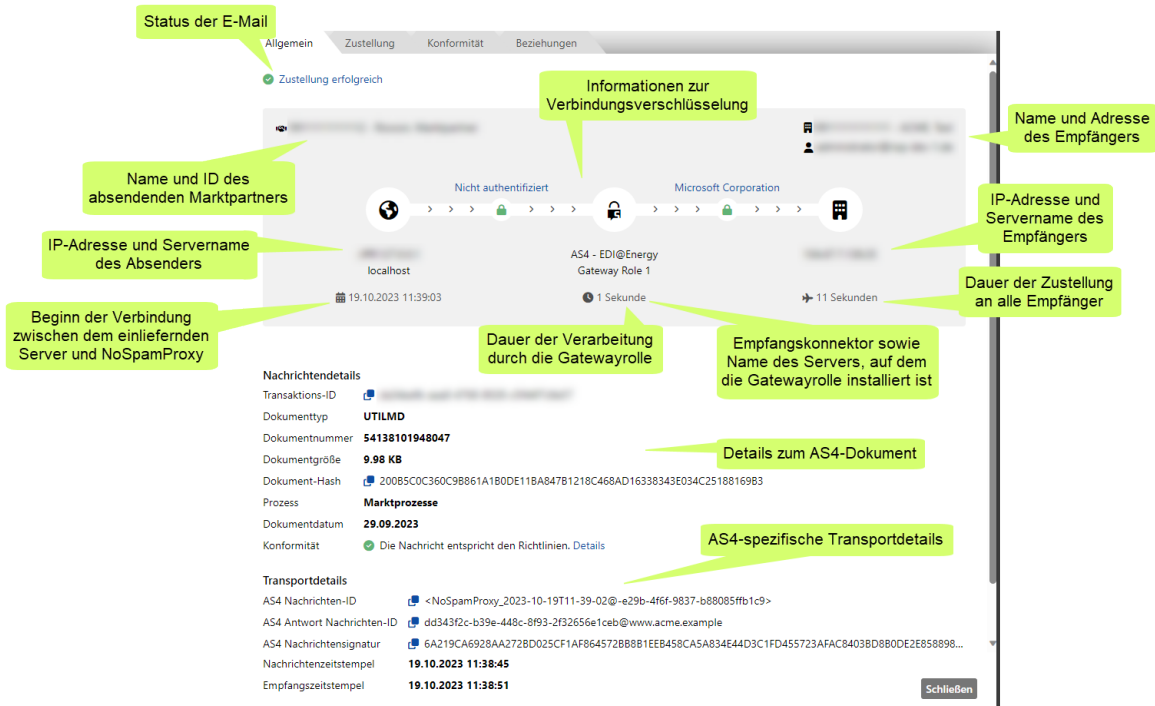
Use message tracking to find out how your AS4 messages were processed by NoSpamProxy. Various filters are available for a better overview:



Show details

General tab

Here you will find general information about the email and its attachments, the connection and transmission as well as AS4-specific details.



Delivery tab

Here you will find information about the individual delivery attempts.

The screenshot shows the 'Delivery' tab in a software interface. At the top, there are four tabs: 'Allgemein', 'Zustellung', 'Konformität', and 'Beziehungen'. The 'Zustellung' tab is selected. Below the tabs, there are sections for 'Empfänger' (Receiver) and 'Zustellversuche' (Delivery Attempts). The 'Empfänger' section shows 'Unternehmenskonto' and 'Interner Empfänger'. The 'Zustellversuche' section has a sub-header 'Der Status jedes einzelnen Zustellversuchs ist unten aufgeführt.' Below this is a table with columns 'Status', 'Datum', and 'Details'. The table contains two rows: 'Zustellung erfolgreich' (19.10.2023 11:39:14) and 'Ausstehend (Warteschlange)' (19.10.2023 11:39:03). A green callout box points to the 'Ausstehend' row with the text 'Der jüngste Zustellversuch erscheint oben in der Liste.' (The most recent delivery attempt appears at the top of the list.)

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

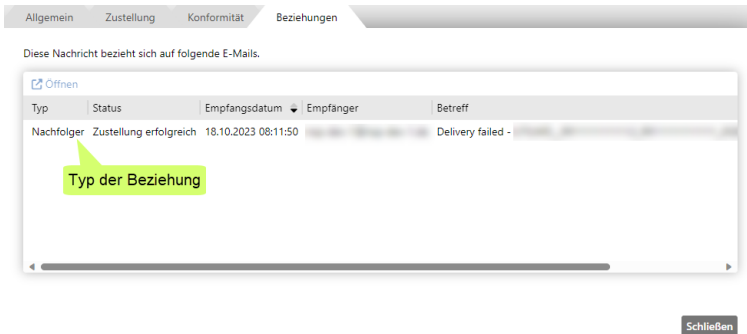
Compliance tab

Here you will find information on the certificates and algorithms used.

The screenshot shows the 'Compliance' tab in the same software interface. The 'Konformität' tab is selected. At the top, there are four tabs: 'Allgemein', 'Zustellung', 'Konformität', and 'Beziehungen'. Below the tabs, there is a green checkmark icon and the text 'Die Nachricht entspricht den Richtlinien.' (The message complies with the guidelines.) Below this is a section for 'Sicherheit' (Security) with the following details: 'Verschlüsselungs-Zertifikat' (redacted), 'Verschlüsselungs-Algorithmus' (AES-128 GCM mit ECDH), 'Signatur-Zertifikat' (redacted), and 'Signatur-Algorithmus' (SHA-256 mit ECDSA unter Verwendung der Kurve Brainpool P256R1). A 'Schließen' (Close) button is located at the bottom right.

Relations tab

Here you will find links to other message tracking records that are related to this record.



I Error when sending

If sending an outbound AS4 message fails, a new attempt is made, regardless of the EBMS errors received. If the answer is incorrect, the attempt is repeated. The repeat loop is cancelled after three minutes.

In the following cases, no new delivery attempt will be made after the first failure:

- DNS errors have occurred.
- The connection is denied. This usually means that the host is accessible but the service is not running.
- The recipient's TLS certificate is not trustworthy.

You can configure the EDI@Energy service so that it saves EDIFACT documents to your disc in case sending the corresponding message fails. See [Configuring the storage location for EDIFACT documents](#).

I When is an email considered an AS4 message?

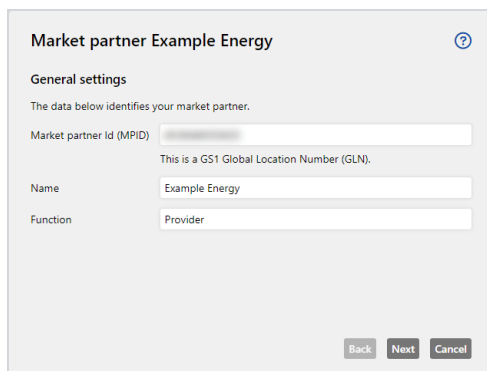
NoSpamProxy considers emails to be AS4 messages if all of the following conditions are met:

- The email has a recipient.
- The email has an EDIFACT attachment.
- The values for the subject and the name of the attachment are identical.
- The subject of the email is **BDEW-compliant**.
- The sender address corresponds to one of the configured EDI@Energy mailboxes.

Adding market partners manually

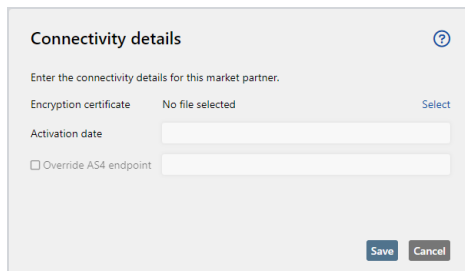
If a market partner is not included in the list under **Market partners**, you can add it manually.

1. Go to **EDI@Energy > Market partners**.
2. Click **Add**.
3. Under **General settings**, enter the MPID, the name and the function of the market partner and click **Next**.



The screenshot shows a form titled "Market partner Example Energy" with a help icon. Under the "General settings" section, there is a sub-header "The data below identifies your market partner." followed by three input fields: "Market partner Id (MPID)" with a note "This is a GS1 Global Location Number (GLN)", "Name" (Example Energy), and "Function" (Provider). At the bottom are "Back", "Next", and "Cancel" buttons.

4. Click on **Add** under **Encryption certificates**.
5. Add the relevant certificates and enter the respective activation date.



The screenshot shows a form titled "Connectivity details" with a help icon. Under the sub-header "Enter the connectivity details for this market partner.", there are three fields: "Encryption certificate" (No file selected, with a "Select" button), "Activation date", and a checkbox "Override AS4 endpoint" with an empty input field. At the bottom are "Save" and "Cancel" buttons.

6. Select whether you want to overwrite the AS4 endpoint.



NOTE: Activate this option if you **do not** want to use the address specified in the market partner's certificate.

7. Click **Finish**.

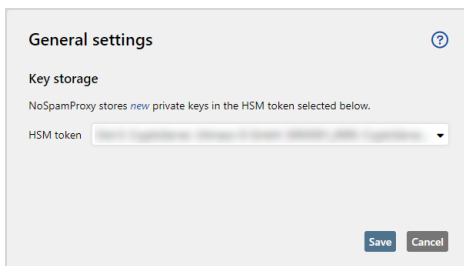
Editing the key storage



NOTE: This setting is only available if you are using an HSM. See [Step 4: Configuring the key management service](#).

To change the storage location of the EDI@Energy certificates you use, proceed as follows:

1. Go to **EDI@Energy > Settings > Certificate configuration**.
2. Click **Modify**.
3. Select the HSM slot that you want to use to save the certificates.



The screenshot shows a dialog box titled "General settings" with a help icon in the top right corner. Under the "Key storage" section, there is a note: "NoSpamProxy stores new private keys in the HSM token selected below." Below this note is a dropdown menu labeled "HSM token" with a downward arrow. At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

4. Click **Save**.

Configuring the storage location for EDIFACT documents

You can configure the EDI@Energy service so that it saves EDIFACT documents to your disc in case sending the corresponding message fails. See [Error when sending](#).

1. Switch to the computer on which the EDI@Energy service is running.
2. Open or create the file **ProgramData/Net at Work Mail Gateway/Edi@Energy/outbound-diagnostics-config.json**.
3. Set the following two properties within the file:
 - "SaveFailedDocuments": true
 - "FailedDocumentsPath": "C:/ProgramData/Net at Work Mail Gateway/Edi@Energy/attachments"



NOTE: You can also choose this path freely. However, make sure that the EDI@Energy service has write permission there.

4. Save the **outbound-diagnostics-config.json** file.

Annex

- Filters in NoSpamProxy 256
- Filters available in NoSpamProxy 259
- Actions in NoSpamProxy 282
- Actions available in NoSpamProxy 283
- Basic concepts 303

Filters in NoSpamProxy

Filters evaluate emails and thus influence the Spam Confidence Level (SCL) of the emails. The SCL determines whether emails are rejected if the inspection result exceeds a certain SCL.

I How do filters work?

The filters do the actual work when inspecting emails. They assess how well the email meets a certain filter criterion and award points for this. You can set up your own set of rules with completely different filter combinations and restrict the rules to certain senders and recipients. This allows you to react very individually and flexibly to spam attacks.

For example, if you use a word filter, the phrase *Viagra* is very likely to be on your block list. For a pharmaceutical company, however, this expression is only a spam criterion to a very limited extent. If an email otherwise appears legitimate or comes from a known email sender, the occurrence of the suspicious word may be acceptable under certain circumstances. For each email, the individual filters of the applicable rule are executed. The filters award penalty and bonus points for the email to be inspected. These points are weighted with the multiplier of the filters and then added to a total value. If this value exceeds the set Spam Confidence Level (SCL) of the rule, the email will be rejected. You can set the threshold value individually for each rule.

Example of a filter configuration

You set a word filter that blocks emails with Viagra ads. For a pharmaceutical company, however, this expression is only a spam criterion to a very limited extent. With NoSpamProxy Protection you can decide for yourself whether you want to include **Viagra** in the word filter or whether you want to use a word filter at all and if so, how strongly you weight it with the multiplier. If an email otherwise appears legitimate or comes from a known email sender, the occurrence of the suspicious word may be acceptable under certain circumstances. You can also specify that the rule with the word filter applies only to specific IP addresses or recipients; for example, only to senders with a specific TLD (Top Level Domain) or IP addresses from a specific subnet.

Position	Rule name	From	To	Action
1	General	*	john.doe@example.com	
2	Japan	*.jp	john.doe@example.com	

- Rule 1, which we call "General" here, is defined to all emails addressed to john.doe@example.com.
- Rule 2 with the name "Japan" on position 2 is also defined to recipient john.doe@example.com, but only considers senders from Japan.

Both rules apply to emails from Japan to "john.doe". However, only the "General" rule is used for evaluation because it is at the top of the list. Even if the Japan rule would actually be "more precise" - the order is the decisive criterion. To apply the "Japan" rule, the order of the rule must be changed as indicated below. This causes the more specific rule to be applied first.

Position	Rule name	From	To	Action
1	Japan	*.jp	john.doe@example.com	
2	General	*	john.doe@example.com	

Filters available in NoSpamProxy

- Core Antispam Engine Filter
- CSA Certified IP List
- Allowed Unicode language planes
- 32Guards
- Realtime block lists
- Reputation filter
- SpamAssassin connector
- Spam URI Realtime Blocklists
- Word matching

Core Antispam Engine Filter



NOTE: This filter is available if NoSpamProxy Protection is licensed.



This filter is valid for the following senders: External. The default SCL value for a single multiplier is 4.

This filter creates a fingerprint of the email to be checked based on defined criteria and compares it with the already known fingerprints. If the fingerprint is known, NoSpamProxy awards 4 SCL points. NoSpamProxy will thus already reject the

email with the default settings. The filter itself has no further setting options. The administrator can only exert further influence on the filter result by weighting with multipliers.

CSA Certified IP List

Many newsletters are desired, as their content is delivered with the consent of the recipient. Often the receipt of such newsletters cannot be guaranteed because no Level of Trust entry has been created. The manual entry of all trustworthy newsletter senders as trusted partners would require too much effort.

This gap is closed by the CSA Certified IP List. It represents a positive list, where a control committee monitors the legality of the newsletters sent. This means that newsletters from senders who are on the CSA Certified IP List can be delivered safely.

If the sender of a received email is on the CSA Certified IP List, the CSA Certified IP List filter marks the email as trusted and assigns negative SCL points. See [Spam Confidence Level \(SCL\)](#).

Enabling CSA Certified IP List

1. Open a rule for inbound emails.
2. Switch to the **Filters** tab.
3. Click **Add** and select **CSA Certified IP List**.
4. Click **Select and close**.



NOTE: You configure the filter under [Connected systems](#).

Allowed Unicode language planes

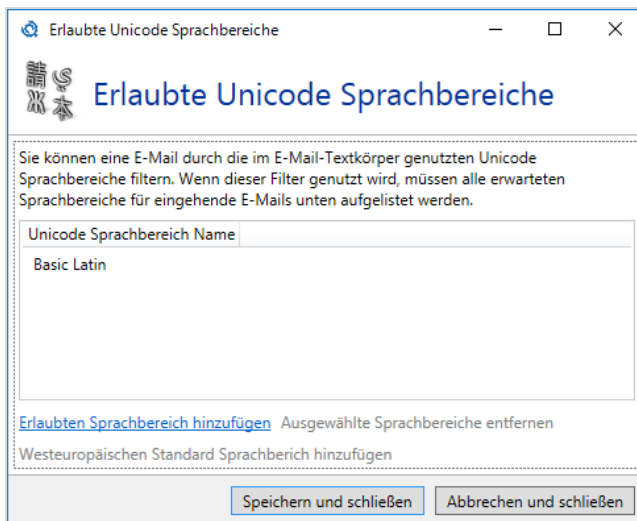


This filter is valid for the following senders: External and Local. The default SCL value for a single multiplier is 4.

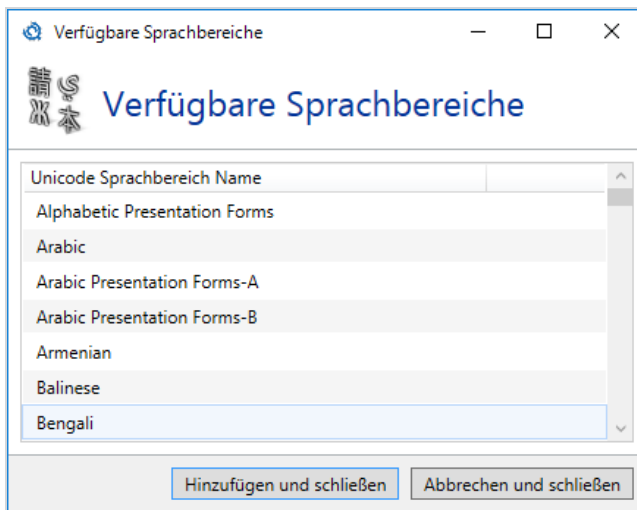
Spam emails sometimes come from language areas with which one does not usually communicate. For example, spam containing Chinese characters may arrive. This filter blocks emails by analysing all contained character sets and only let the email pass if all contained character sets are explicitly allowed by you.

Application

1. Add the Allowed Unicode language planes filter to your rule.



2. Now add all language planes that can be used in incoming emails to the allowed language planes.



TIP: If you only communicate with Western Europe or America, the language plane for Western European languages is usually sufficient. You can add it to the list by choosing **Add default western European language** plane if it is not already included in the list of allowed languages.

32Guards

32Guards is on the one hand a filter that influences the Spam Confidence Level rating, and on the other hand an action that can directly reject threats temporarily or permanently. See [32Guards](#).

Realtime block lists

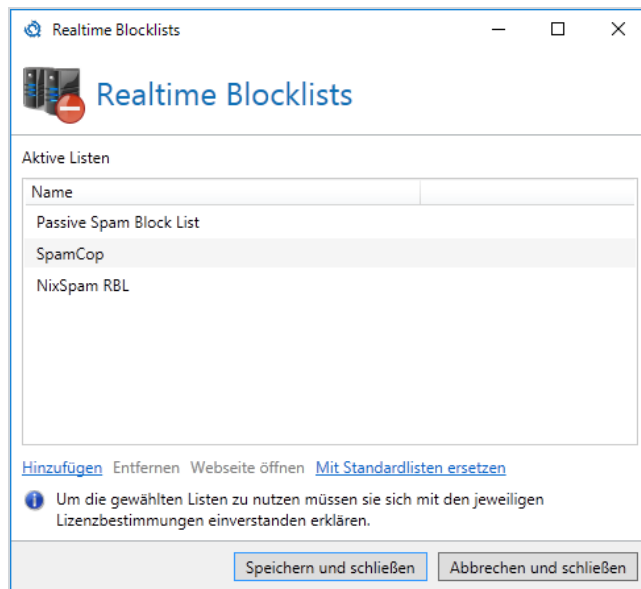


This filter is valid for the following senders: External. The default SCL value with single multiplier depends on the lists selected in the filter. The SCL points set in the list are assigned per hit.

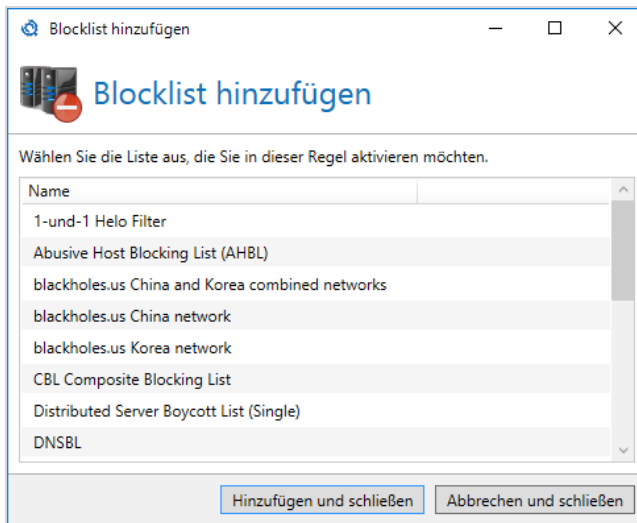
This filter checks whether an address entry exists in realtime block lists. You can select multiple block lists. Since even the best lists can contain false positives, you should always use several lists. Since every hit is counted as a penalty point, the risk of emails being blocked by a false positive based on a single blacklist is minimised.

Application

1. Add the filter to your rule
The configuration dialog opens.
2. Click **Add**.



3. Select one or more lists that you want to activate.



4. Click **Add and close**.
5. Click **Save and close**.



TIP: Click **Replace with default set** to replace the currently selected lists with the lists recommended by Net at Work.

Removing lists

- To remove one or more lists, select the entries to be deleted and click **Remove**.



NOTE: Removed lists are only removed from the rule currently edited. The lists still appear in the global rule settings.



NOTE: For the DNS queries to work correctly, you must configure the DNS settings of the operating system appropriately. The server must be able to resolve external domains. It can be useful to install your own DNS server as a forwarder.

Reputation filter

This filter performs various checks on the email envelope, the content of the email and the headers. Some of the checks also analyse DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework). Depending on the results of the individual tests, SCL points can be assigned, which can be configured individually. This allows you to adapt the assessments to the requirements of your company.

Title	Description
Unsecured connection	Checks if the inbound connection is secured by TLS. TLS encryption guarantees that both meta and content data are exchanged in encrypted form between the email client and the server or between different email servers. The General Data Protection Regulation (GDPR) prescribes the use of TLS encryption. Since spammers often do not comply with the GDPR, this test allows conclusions to be drawn about the legitimacy of the email.

Title	Description
Missing PTR record	Checks whether the IP address can be resolved back to a hostname. If this is not the case, the cause is a missing PTR entry. PTR (Pointer Resource Records) assign one or more hostnames to an IP address in the

Title	Description
	DNS. If this assignment is not possible, this indicates an attempt at misuse.
Suspected dynamic address	<p>Checks whether the hostname associated with the IP address includes the IP address in text form. NoSpamProxy checks whether the IP address originates from a dynamic IP address range.</p> <p>This often occurs with infected computers acting as spambots.</p>
Reverse lookup failed	Checks whether the hostname associated with the IP address of the email server can be resolved back to this IP address in a 'reverse lookup'. If this is not possible, this indicates spoofing, since it is highly likely that the actual identity of the host is to be concealed.
Missing IP address	Checks whether the 'MAIL FROM' domain can be resolved to an IP address. If this is not possible, this indicates an attempt at misuse, as the domain in question most probably does not exist.

Title	Description
SPF failed	<p>Checks whether a valid SPF record exists. Checks whether the IP address of the email server is stored in the DNS as an authorised MTA (Mail Transfer Agent), i.e. whether it is allowed to send emails for this domain. This test only awards points if no DMARC policy (see below) is active.</p>
DKIM failed	<p>Performs DKIM checks for the respective email. These checks consist of verification of the header signature and the hash calculated from the body of the email, which is also signed. The sender's public key is stored in the DNS.</p> <p>This test only awards points if no DMARC policy (see below) is active.</p>
DMARC result 'quarantine'	<p>The mode 'quarantine' is defined in the DMARC policy of the sender for the case of a failed check. The DMARC examination also includes the so-called 'alignment' between the domains examined by</p>


Title	Description
	<p>DKIM and SPF.</p> <p>The amount of points awarded depends on the DMARC result applied.</p>
DMARC result 'reject'	<p>In the DMARC policy of the sender, the mode 'reject' is defined for the case of a failed check. The DMARC examination also includes the so-called 'alignment' between the domains examined by DKIM and SPF.</p> <p>The amount of points awarded depends on the DMARC result applied.</p>
Address is not aligned	<p>Checks whether the 'MAIL FROM' domain and 'Header-From' domain are identical ('alignment'). This test only awards points if no DMARC policy is active.</p>



NOTE: If one or more DMARC-type checks, i.e. SPF, DKIM or DMARC fail, this result is overwritten by an intact ARC control chain. In such a case, no penalty points are awarded which would increase the **Spam Confidence Level (SCL)**. See **Vetruenswürdige ARC-Unterzeichner**.

Title	Description
Invalid angle brackets	Checks if the 'header-from' contains an angle bracket with an invalid email address, which is not RFC compliant. Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.
Missing sender	Checks if the 'MAIL FROM' is empty and the 'Header-From' contains a valid email address. If this is not the case, this indicates NDR backscatter. Mobile devices and email applications such as Outlook only show the display name, so abuse is not detected.
Corporate domain in email address	Checks whether the email address

Title	Description
	<p>specified in the header form contains a corporate domain. If this is the case, it indicates identity theft, since this test can only be used for inbound emails and therefore it must be an external email.</p> <p>Note that such a case can also occur if an external email system sends on behalf of the corporate domain but is not configured as <u>Adding corporate email servers</u>.</p> <p>EXAMPLE: <xyz@netatwork.de></p>

Title	Description
	 <p>NOTE: A valid DKIM signature for the 'Header-From' domain overrides this filter by default so that no penalty points are awarded. To prevent this behaviour, please refer to the information under <u>Aufheben der DKIM-Signatur im Reputationsfilter.</u></p>
Corporate domain in display name	<p>Checks if the display name contains an email address that includes a corporate domain. Email addresses that include corporate domain are used by spammers as part of display names, as this is the only name that initially appears in many mobile devices and email programs. The sender can thus pretend a false identity.</p>

Title	Description
	<p>EXAMPLE: "Uwe Ulbrich uwe.ulbrich@netatwork.de" <spam@spammer.de></p>
<p>Subdomain of a corporate domain in email address</p>	<p>Checks whether a subdomain of a corporate domain is in use. If this subdomain is legitimate, the filter 'Corporate domain in email address' is applied.</p> <p>EXAMPLE: <xyz@hr.netatwork.de></p>
<p>Subdomain of a corporate domain in display name</p>	<p>Checks if the display name contains a subdomain of a corporate domain. Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name. The sender can thus pretend a false identity.</p> <p>EXAMPLE: "hr.netatwork.de" <spam@spammer.de></p>

Title	Description
<p>Obfuscated corporate domain in email address</p>	<p>See filter 'Corporate domain in email address'. In addition, it is checked here whether ASCII characters were used in the domain that look similar to certain letters.</p> <p>EXAMPLE: <xyz@n3tatw0rk.de></p>
<p>Obfuscated corporate domain in display name.</p>	<p>See test 'Corporate domain in display name'. In addition, it is checked here whether ASCII characters were used in the domain that look similar to certain letters. Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name.</p> <p>EXAMPLE: "Uwe Ulbrich uwe.ulbrich@n3tatw0rk.de" <spam@spammer.de></p>
<p>Subdomain of an obfuscated corporate domain in email address</p>	<p>See test 'Subdomain of a corporate domain in email address'. In addition,</p>

Title	Description
	<p>it is checked here whether ASCII characters were used in the domain that look similar to certain letters.</p> <p>EXAMPLE: <xyz@hr.netatwork.de></p>
<p>Subdomain of an obfuscated corporate domain in display name</p>	<p>See test 'Subdomain of a corporate domain in display name'. In addition, it is checked here whether ASCII characters were used in the domain that look similar to certain letters. Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name.</p> <p>EXAMPLE: Uwe Ulbrich uwe.ulbrich@hr.n3tatw0rk.de" <spam@spammer.de></p>
<p>Multiple email addresses</p>	<p>Checks whether the 'Header-From' contains more than one email address, which is not RFC compliant.</p>

Title	Description
	Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.
Domain in display name different from email address	<p>Checks if a domain specified in the display name of the header-from is different from the domain that is part of the header-from email address. Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name.</p> <p>EXAMPLE:</p> <pre>"service@paypal.com" <spam@spammer.de></pre>

Title	Description
Invalid '@'	Checks if the 'Header-To' contains an '@' character that is not part of an email address, which is not compliant with

Title	Description
	<p>RFC 5322.</p> <p>Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.</p>
Invalid angle brackets	<p>Checks if the 'Header-To' contains angle brackets with an invalid email address, which is not compliant with RFC 5322.</p> <p>Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.</p>
Missing 'Header-To'	<p>Checks whether the 'Header-To' contains a specification or is present at all. If this is not the case, the recipient cannot be determined. In this case, information on the recipient can only be found in the 'Bcc' field.</p>
Missing corporate email address	<p>Checks whether the 'Header-To' or the 'CC' contains a corporate email address. In this case, information on the recipient can only be found in the 'Bcc' field.</p>

SpamAssassin connector



This filter is valid for the following senders: External and Local. The default SCL value at single multiplier depends on the return value of the SpamAssassin daemon.

SpamAssassin is a free spam filter that includes several predefined tests to classify messages. Many of these tests, such as RBL, NoSpamProxy Protection itself executes much earlier and more effectively. Nevertheless, it can be beneficial to integrate the other rules of this filter. SpamAssassin assesses a message and writes the result in the message header.

It consists of server (SpamD) and client (SpamC). The NoSpamProxy Protection filter acts as a SpamAssassin Client (SpamC) and only works in conjunction with a SpamAssassin Daemon (SpamD). You can install the SpamAssassin Daemon on a system of your choice. This can be a UNIX or Windows system. Operation directly on the same server as NoSpamProxy is also possible.



NOTE: Make sure that NoSpamProxy can also reach the requested system. Often port filters, IP routing and firewalls have to be configured.

Spam URI Realtime Blocklists



This filter is valid for the following senders: External and Local. The default SCL value with single multiplier depends on the lists selected in the filter. 2 SCL points are awarded per hit in a list.

Spam URI Realtime Blocklists manage lists of suspicious spam URLs. Via the Internet it is possible to check whether or not a URL exists in this list.

The Spam URI Realtime Blocklists Filter analyses links in emails and PDF documents and checks whether there is a corresponding entry in these lists. He also searches for addresses beginning with "www". and not appear as links in emails and PDF documents.



NOTE: As with the Realtime Blocklists filter, DNS queries must work correctly. The server must be able to resolve the specified service. It can be useful to install your own DNS server as a forwarder.

Malicious links are assigned to one of the following categories:

- Malware
- PhishingAndFraud
- Compromised
- CriminalActivity
- Botnets
- IllegalSoftware
- ChildAbuseImages
- SpamSites
- ParkedDomains

Word matching



This filter is valid for the following senders: External and Local. The default SCL value with a simple multiplier depends on the word groups selected in the filter. The SCL points set in the word group are awarded per hit.

This filter allows you to recognise previously defined words and phrases in both the subject line and the body of the email and rate them with penalty or bonus SCL points. Each appearance or, depending on the settings, absence of such an expression is awarded with the points set in the filter.

If one or more words from the configured word groups are found in the email, an optional email with a notification can be sent to a local email address. This email will contain the sender of the email, the recipient, subject, and the words found.

Application

1. Add the filter to your rule The configuration dialog opens.

Wortübereinstimmungen

Wortübereinstimmungen

Fügen Sie eine oder mehrere der bereits definierten Wortgruppen aus dem Bereich 'Wortübereinstimmungen' des Knoten 'Voreinstellungen' ein.

Aktive Wortgruppen

Wortgruppe
Common notation for medical products
Common notation of porn words

[Hinzufügen](#) [Entfernen](#)

Falls ein Übereinstimmung gefunden wird, kann eine E-Mail an eine lokale Adresse versandt werden.

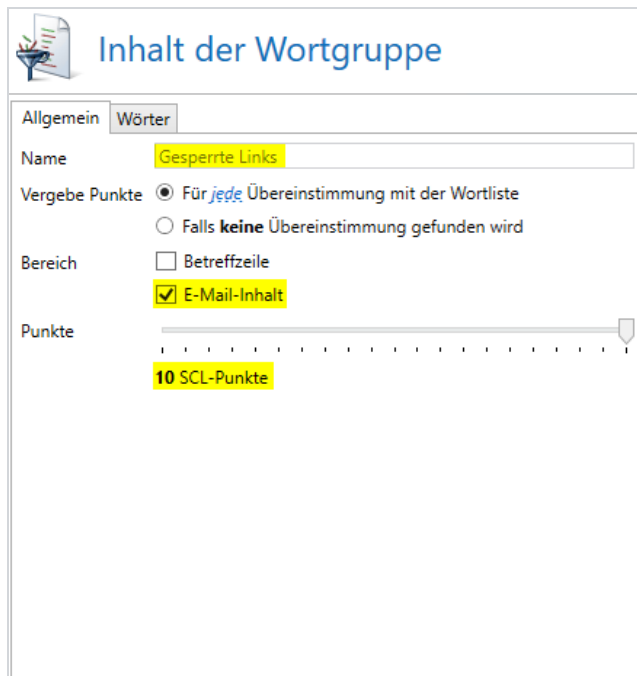
Sende eine Benachrichtigung

Adresse

2. Click **Add**.
3. Select the phrase you want to add and click **Add and close**.
4. **Optional** Specify an email address to which notifications are sent.
5. Click **Save and close**.

Adding a new word group

1. Go to **Configuration > Presettings > Word matching**.
2. Click **Add**.
3. On the **General** tab, determine
 - the name of the word group,
 - whether points are awarded for matches or for non-matches,
 - the area to which the phrase is applied and
 - the SCL points awarded.



The screenshot shows a configuration window titled "Inhalt der Wortgruppe". It has two tabs: "Allgemein" (selected) and "Wörter". The "Allgemein" tab contains the following fields and options:

- Name:** A text input field containing "Gesperrte Links".
- Vergebe Punkte:** Two radio button options. The first is selected and labeled "Für *jede* Übereinstimmung mit der Wortliste". The second is labeled "Falls **keine** Übereinstimmung gefunden wird".
- Bereich:** Two checkbox options. The first is "Betreffzeile" (unchecked). The second is "E-Mail-Inhalt" (checked).
- Punkte:** A horizontal slider bar with a value of "10 SCL-Punkte" displayed below it.

4. On the **General** tab, determine

- whether you want to search for exact matches (simple) or use wildcards or regular expressions,
- the words contained in the word list and
- whether you also want to search for similar words.

Inhalt der Wortgruppe

Allgemein Wörter

Art

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

Neues Wort

Wort
https://bit.ly/

Entfernen

Auch ähnliche Wörter finden

5. Klicken Sie auf **Finish**.

Actions in NoSpamProxy

Actions react to filter results and execute the configured tasks. In contrast to the filters, actions can change emails, e.g. by removing attachments. Actions can also override filter results. Examples are virus scanners and the [Greylisting](#) action.

Activating actions

1. Open the rule that should contain the action.
2. Switch to the **Actions** tab.
3. Click **Add**.
4. Select the action you want to add to the rule.
5. Click **Select and close**.

The action is added to the rule.



NOTE: If the rule needs to be configured, a configuration dialog opens first. After you have completed the configuration, the action will be added to your rule.

Available actions

For more information on available actions in NoSpamProxy, see [Actions available in NoSpamProxy](#).

Actions available in NoSpamProxy

The following actions are available in NoSpamProxy:

- [Receiver rewriter](#)
- [Automatic reply](#)
- [CxO Fraud Detection](#)
- [Applying disclaimers](#)
- [Apply DKIM signature](#)
- [Greylisting](#)
- [Redirect email](#)
- [Malware scanner](#)
- [32Guards](#)
- [URL Safeguard \(Action\)](#)
- [Hide corporate topology](#)

Receiver rewriter



This action is valid for the following senders: External and Local.

This action changes the destination address upon email receipt. For example, after a change of company name, you can have all emails addressed to the old address rewritten to the new address. A second use case is the definition of a so-called secret address. For example, you can specify that all emails containing the suffix `*secret*` in the address field are considered welcome and delivered without verification. A rule may look like this:

Position	From	To	Decision	Action
1	*@*	*secret@example.com	Pass	Receiver rewriter

The address manipulation removes the keyword and forwards this email to your correct email address. The keyword can of course be defined by you and changed again if necessary.

Using the Address Manipulation action

1. Activate the Address Manipulation action in a rule (see above).

The dialogue for the configuration opens.

Adressmanipulation

Diese Aktion sucht in jeder Empfängeradresse einer E-Mail nach dem angegebenen Text des Felds 'Suche' und ersetzt ihn durch den Text, der bei 'Ersetzen durch' angegeben ist (Platzhalter wie '?' und '*' sind verboten).

Beispiel: Ein Suchtext von 'geheim' und einem leeren Ersatztext wird aus einer E-Mail-Adresse wie 'max.mustergeheim@example.com' die Adresse 'max.muster@example.com' machen.

Suche (Pflichtfeld)

Ersetzen durch (optional)

Speichern und schließen Abbrechen und schließen

2. Under **Match**, enter the string to be replaced from the confidential address.
3. Under **Replace**, enter the text to replace the text from the **Match**.
4. Click **Save and close**.



TIP: For example, you may replace the string "confidential" in the confidential address "user1confidential@example.com" with an empty string for the correct address "user1@example.com".

Automatic reply



This action is valid for the following senders: External and Local.

This action sends an automatic reply to the sender of an email. The text of the email is created using a template from the Templates folder of the Intranet Role. A sample template (SampleAutoReply.cshtml) is copied by the setup into the folder. You can make copies of this template and adapt it to your needs. Changes to templates are replicated from the Intranet Role to all Gateway Roles within a few minutes. The roles do not need to be restarted for this.

Automatische Antwort

Automatische Antwort

Bitte wählen Sie die Vorlage aus, die für automatische Antworten verwendet werden soll.

Vorlage

Speichern und schließen Abbrechen und schließen



NOTE: The automatic responder responds to every email that is processed by the corresponding rule. Thus, it is possible for an email sender to receive multiple automatic replies. This behaviour differs from the out-of-office function in Microsoft Outlook/Exchange, which sends automatic replies only once per email sender.

Customising the response templates

1. Switch to the system on which the Intranet Role is installed.
2. Go to **C:\Program Files\NoSpamProxy\Intranet Role\Templates**.
3. Create a copy of the **SampleAutoReply.cshtml** file and save it under a different, unique name in the **%ProgramData%\Net at Work Mail Gateway\Intranet\Templates** folder.
4. Make the desired changes to the text part of the file.



NOTE: Make sure that you do not change the HTML structure. Otherwise the template will not be recognised.

5. Switch to the NoSpamProxy Command Center and restart the Intranet Role.



The templates are now read in again; email traffic is not affected.

Applying the action

1. Go to **Configuration > Rules**.
2. Open the rule to which the auto responder is to be applied.
3. Go to the tab **Actions** and add the action **Automatic reply**.
4. Select the desired template from the drop-down menu.
5. Save the rule.

| CxO Fraud Detection

CxO fraud detection is used to detect phishing attacks. It compares the sender name of incoming emails with the names of company users. Fake emails sent to you on behalf of superiors or employees are intercepted in this way.

During the analysis different variants of the sender name are included in the comparison:

- Jane Doe
- Doe Jane
- JaneDoe
- DoeJane

All corporate users that you want to use for CxO Fraud Detection must first be registered for the respective Corporate users.

I Getting to know CxO Fraud Detection

Getting to know CxO Fraud Detection

To familiarise yourself with how CxO Fraud Detection detection works, we recommend the following approach:

1. Add the email addresses of your IT staff to the appropriate AD group, not those of senior management. See [Automating the user import](#).
2. Create a separate, temporary rule that filters to the IT staff's **private** email addresses as **senders** and the **company email addresses** as **recipients** .
3. Now simulate attacks by sending emails from IT employees' private email addresses to their corporate email addresses.
4. Observe how the CxO Fraud Detection would behave if it were fully activated. The information on the **Activities** tab of an email in Message Tracking is helpful here. See [Viewing email details](#).

This allows your IT staff to understand how CxO Fraud Detection works.

**TIP:**

Before the actual activation of CxO Fraud Detection in NoSpamProxy, the IT department should inform senior management that they are now more carefully protected. It is often the case that higher management levels also communicate between private and business identities. If CxO Fraud Detection is activated, it is likely that this type of communication will be prevented by NoSpamProxy.

Senior management should therefore be informed about how Level of Trust can help to allow this communication to continue, for example by sending an email from internal to external and replying to this email.

Applying disclaimers



This action is valid for the following senders: Local.

This action adds a disclaimer to outbound emails. For this purpose, the disclaimer rules and templates are evaluated and attached to the appropriate places in the emails. See [NoSpamProxy Disclaimer](#).



NOTE: To use the Disclaimer function, it must be licensed.

Apply DKIM signature



This action is valid for the following senders: Local.

This action adds a DKIM signature (DomainKeys Identified Mail) to outbound emails. This allows the recipient to ensure that the email was actually sent by your company.

A DKIM key is required to create the signature. For information on how to create and publish DKIM keys, see **DomainKeys Identified Mail**.

| Greylisting



This action is valid for the following senders: External.

Greylisting is a precautionary measure against "suspicious" emails. If emails remain just below the spam threshold you defined, without greylisting these emails would be rated as sufficiently safe.

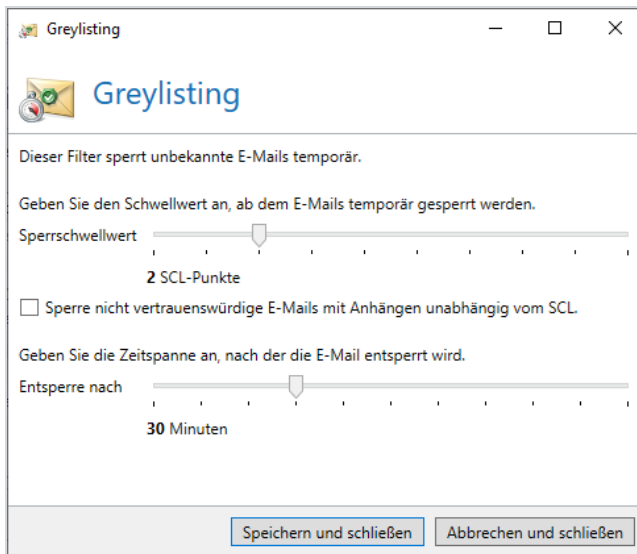
The greylisting action does not let this email pass immediately, but temporarily rejects it. The sending email server receives an error message instructing it to resend the email after a certain amount of time. The email will then be delivered again. You can set the time at which the submitting server may perform a second attempt.

Greylisting is based on the following principle: A spammer usually saves himself the effort of sending a second email. A regular sender, on the other hand, will try to have the email delivered again after some time. On the second attempt this connection is now considered to be of higher value, resulting in the email being allowed to pass. You can individually set the threshold for the number of penalty points that determines when emails that pass are still classified as suspicious.

Activating the Greylisting action

1. Open a rule for inbound emails.
2. Switch to the **Actions** tab.
3. Click **Add** and select the **Greylisting** action.
4. Click **Select and close**.

The configuration dialogue opens.



5. Specify,
 - the threshold value for activating greylisting and
 - the period of time after which emails are unblocked again.
6. **Optional** Check the box if you want to block untrusted emails with attachments regardless of the spam confidence level.



NOTE: The greylisting threshold must be lower than the spam threshold, otherwise greylisting will not work.

Redirect email



This action is valid for the following senders: External and Local.

The action offers the possibility to add or completely replace the email recipients. Depending on the settings, emails are either delivered additionally or solely to the recipients defined in the action.

Leite E-Mails um

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

Versende nur zu den **neuen** Empfängern

Versende **zusätzlich** zu den neuen Empfängern

Neue Empfänger

Adresse

Adresse

Entfernen

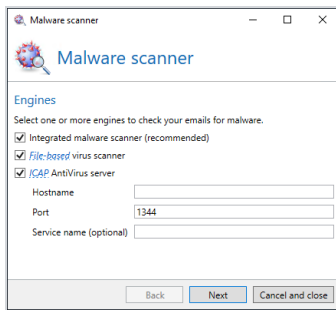


NOTE: One or more recipients must be entered into the list to be able to use the action.

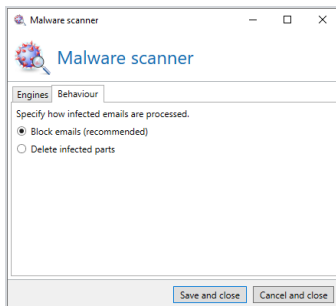
Malware scanner

This action comprises three different engines, each of which can be used individually or in combination with each other. Details on the individual engines can be found below.

- On the **Engines** tab, select the engine.



- On the **Behaviour** tab, determine how emails are processed if one or more engines detect an infection.



Integrated Malware Scanner

The Integrated Malware Scanner checks the attachments of incoming emails.



NOTE: To ensure parallel operation with other locally installed virus scanners on the gateway role, also observe the notes at [Installierte On-Access-Virens Scanner konfigurieren](#).

See

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

File-based virus scanner

This action is valid for the following senders: External and Local.

The file-based virus scanner stores attachments of incoming emails in a specific directory. If you have any on-access virus scanner installed, this scanner will deny read access to any infected attachments. NoSpamProxy Protection checks whether access is possible or not immediately after the attachments are placed in the directory. Attachments that can be accessed are considered free of viruses. NoSpamProxy Protection can work together with any virus scanner that monitors file accesses in real time. This scan method is already installed on many file servers, high-performing and reliable.

Attachments contained in emails in RTF format can also be processed by virus scanners. The attachments - which are named winmail.dat by default - are checked and blocked individually if necessary. Please note that this type of processing represents a change to the respective email.

The directory for the temporary storage of files in current installations is

C:\ProgramData\Net at Work Mail Gateway\Temporary
Files\Netatwork.NoSpamProxy.Addins.Core.Actions.MalwareScan.FilebasedMalwareScanner.

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



NOTE: If you have updated from version 13, the path is C:\Program Files\Net at Work Mail Gateway\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



NOTE: If you have updated from version 13, the path is C:\Program Files\Net at Work Mail Gateway\enQsig Webportal.

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.



NOTE: Make sure that your locally deployed virus scanner does not use behaviour-based analyses to draw conclusions from the fact that malware is actively stored by processes in the path **C:\ProgramData\Net at Work Mail Gateway\Temporary Files\Netatwork.NoSpamProxy.Addins.Core.Actions.MalwareScan.FilebasedMalwareScanner**. The files themselves should or must be checked, but the placement of malware in the folder in question must not lead to the classification of the corresponding process that performs 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.

You can determine whether contaminated attachments are deleted or whether the corresponding email is blocked automatically.



NOTE: In case emails are rejected, the sender is informed of this by the delivering server. Neither the sender nor the recipient is informed of a deleted attachment.



NOTE: As with all virus scanners, password-protected ZIP files are not checked and are passed on without further examination.

ICAP Antivirus Server

The Internet Content Adaptation Protocol (ICAP) is a protocol for forwarding content for HTTP-, HTTPS- and FTP-based services. An ICAP server receives data, which is then processed by a server-based virus scanner, for example.

If you select the ICAP Antivirus Server action, NoSpamProxy acts as an ICAP client. The data is then sent by NoSpamProxy to your ICAP server and scanned. When the scanning process is complete, the ICAP server sends the results to NoSpamProxy. Depending on this result, the configured action is executed.



NOTE: For the ICAP Antivirus Server action, you need access to an ICAP server.

32Guards

32Guards is on the one hand a filter that influences the Spam Confidence Level rating, and on the other hand an action that can directly reject threats temporarily or permanently. See [32Guards](#).

URL Safeguard (Action)

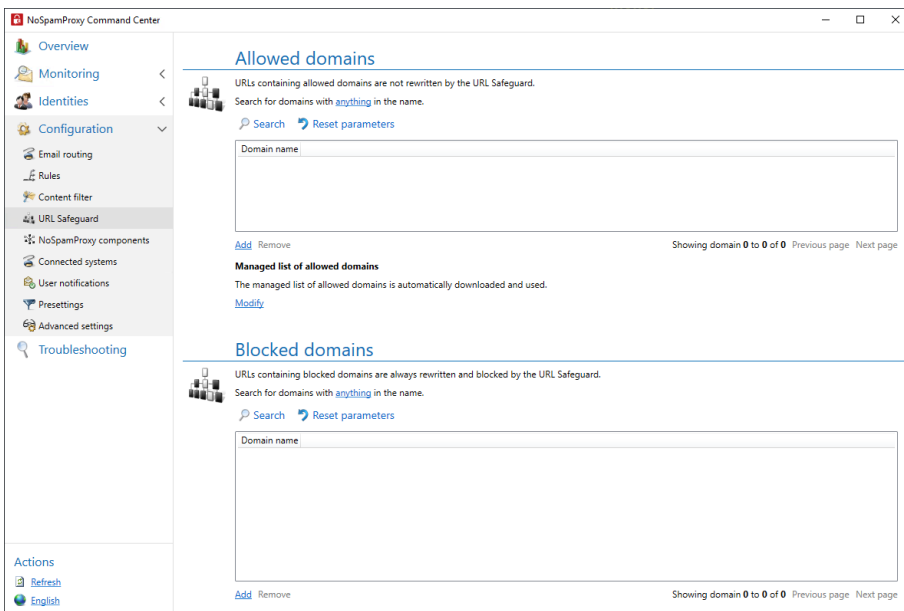
Activating the URL Safeguard

To use the URL Safeguard, you must add it as an action to a rule. See [Step 5: Configuring actions](#).

Configuring the URL Safeguard

Additional settings can be made in the default partner settings or for individual partner domains. See [Default partner settings](#) and [Editing partner domains](#).

Configuring allowed and blocked domains



Allowed domains

URLs that contain allowed domains are not rewritten by the URL Safeguard.

1. Go to **Configuration > URL Safeguard > Allowed domains**.
2. Click **Add**.
3. Do one of the following:
 - Enter the desired domain in the input field and click **Add**.
 - Click **Paste from clipboard** to add a list of domains from the clipboard.
4. Click **Save and close**.

Managed list of allowed domains.

NoSpamProxy provides a managed list of allowed domains of known websites.

1. Go to **Configuration > URL Safeguard > Managed list of allowed domains**.
2. Click **Modify**.
3. Tick or untick the box next to **Automatically download and use the managed list**.
4. Click **Save and close**.

Blocked domains

URLs that contain blocked domains are always rewritten and blocked by the URL Safeguard.

1. Go to **Configuration > URL Safeguard > Blocked domains**.
2. Click **Add**.
3. Do one of the following:
 - Enter the desired domain in the input field and click **Add**.
 - Click **Paste from clipboard** to add a list of domains from the clipboard.

4. Click **Save and close**.

Hide corporate topology



This action is valid for the following senders: Local.

The Hide corporate topology action removes the "received" email headers of emails from local senders. Otherwise, these Received entries can be used to draw conclusions about the local topology.

Basic concepts

I Sender reputation

NoSpamProxy uses a multi-level system for evaluating the sender reputation, which comprises a total of nine different checks. The most important ones include SPF, DKIM and DMARC checks, which can be used to identify beyond doubt whether an email originates from the specified sender.

- The Sender Policy Framework (SPF) prevents the forging of the sender address of e-mails.
- DomainKeys Identified Mail (DKIM) secures outgoing emails with an electronic signature. See [DKIM keys](#).
- With a DMARC entry, the sending domain can determine which quality criteria an email from it must meet. NoSpamProxy consistently evaluates this information. These methods are combined with the [Level of Trust](#).

You make the settings for evaluating the sender reputation in the [Reputation filter](#).

**TIP:**

See our series of articles on the NoSpamProxy blog for more information on sender reputation and email security:

[Sender reputation and email security - Part 1: Authenticated Received Chain \(ARC\)](#)

[Sender reputation and email security - Part 2: Sender Policy Framework \(SPF\)](#)

[Sender reputation and email security - Part 3: DomainKeys Identified Mail \(DKIM\)](#)

[Sender reputation and email security - Part 4: Domain-based Message Authentication, Reporting and Conformance \(DMARC\)](#)

[Sender reputation and email security - Part 5: DNS-based Authentication of Named Entities \(DANE\)](#)

32Guards

32Guards is on the one hand a filter that influences the calculation of the spam confidence level, and on the other hand an action that can directly reject threats temporarily or permanently.

The evaluation of emails by 32Guards is based on the evaluation of a number of indicators. This evaluation results in a final assessment of the email. Examples of such indicators are suspicious file names or the frequent occurrence of new or unknown URLs in a very short time.

This action/filter ensures that metadata on email attachments and URLs is collected and uploaded to the NoSpamProxy cloud. File contents are neither collected nor accessed. With 32Guards, attacks through spam and malware can be detected and

defended against faster and more reliably. Based on this metadata, 32Guards creates a threat assessment, which in turn is used as a basis for further actions in NoSpamProxy.

Only the following metadata is collected by NoSpamProxy:

Attachments

- File name
- File size
- Details of the first ten files within archives/to a maximum of 50 files in nested archives (sorted by file type): file name, hash value, size, number, size without compression
- SHA-256 hash value
- TLSH hash value
- MIME type (as detected by NoSpamProxy)
- Information about whether malware was found in the attachment

URLs

- The complete URL
- URL classification (spam, phishing, malware)

Emails

- Source IP of inbound emails
- Authenticated domain and source (DKIM/SPF/S/MIME)

- Salted hash of the local part of the header-from domain and MAIL FROM domain of inbound emails
- Salted hash of the local part of the Rcpt domain and To/CC header domain of outbound emails
- Message ID
- Whether it is an automatically generated email
- Status of the chain of custody within the framework of Authenticated Received Chain (ARC)
- Status with regard to the Certified IP List of the Certified Senders Alliance (CSA)
- TLS certificate including validity, trust status, thumbprint, domain name and issuer
- Transaction ID
- Information about whether the email was inbound (trusted/untrusted) or outbound
- Version of the NoSpamProxy client
- Version of the applied 32Guards data model



From each of the areas mentioned (attachments, URLs, emails), only the worst rating is included in the calculation. Ratings from different areas are added up.

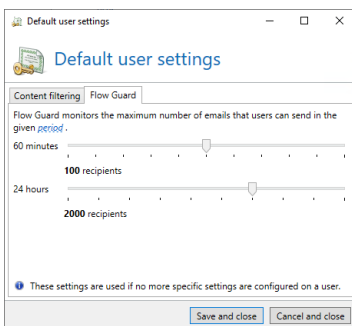
Updates to NoSpamProxy 14 and higher

When updating from older versions to NoSpamProxy 14 and higher, the **filter 32Guards** is automatically added to a rule if the following **two** conditions are met before the update:

- The **action 32Guards** is configured as part of a rule and
- on the **tab Filter** the option **Check the email with the filters** specified below is selected.

Flow Guard

Flow Guard makes it possible to control the volume of outbound emails. In this way, unwanted mass emails, whether generated by inexperienced users or triggered by malware, can be recognised before they are sent and the reputation of your own domain can be protected. Flow Guard assigns quotas for outbound emails to NoSpamProxy users. If the set threshold is exceeded, any further outbound email is rejected.



There are a total of two threshold values that can be set per user:

- Number of emails per hour
- Total number of emails per day



TIP: You can also assign the thresholds based on AD group memberships.



NOTE:

NoSpamProxy allows email addresses that are not assigned to any user to be used for sending. In these cases, Flow Guard proceeds as follows:

- If no user is assigned to the email address, licences are counted per email address.
- If several email addresses are assigned to a user, the emails from all email addresses are added together.

Setting threshold values

You set the thresholds either globally for all users or for individual corporate users. To do this you must

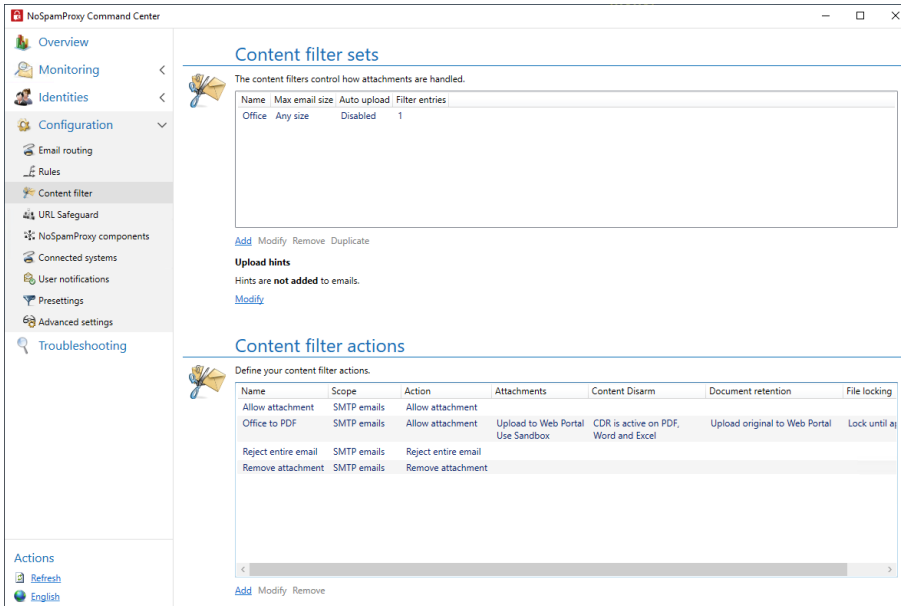
- configure the threshold values in the default user settings (see [Configuring default settings for users](#)) or
- configure the settings under **Identities > Corporate users** for the respective [Corporate users](#).

Content filters



This feature is available if you have purchased a corresponding licence.

Content filter sets enable the execution of content filter actions based on conditions. Both the content filter actions and the conditions are configured in content filter entries. A content filter can contain several content filter entries.



How a content filter works

When creating content filters, you determine

- the general instructions for handling attachments and dealing with archives,
- the content filter actions and
- the Bedingungen that trigger content filter actions.

You configure both content filter actions and conditions by assigning one or more content filter entries to a content filter. See Inhaltsfilter anlegen and Inhaltsfilteraktionen anlegen.

You can use the level of trust system to trigger various actions for a file type, for example

- completely block a Word document with macros (2007-2016, DOCM) from untrusted emails, but
- carry out a CDR action for trusted emails from your partners.

Related steps

Assigning content filters| To apply a content filter, you must assign it under **Partners** or **Corporate users**. See [Inhaltsfilter anlegen](#).

Creating content filter actions| Content filter actions are actions that are applied to attachments and to the emails that contain these attachments. They are triggered by the fulfilment of conditions. See [Inhaltsfilteraktionen anlegen](#)

Defining conditions| In order for content filter actions to be triggered, conditions that you have defined must be fulfilled. See [Bedingungen](#).

I Level of Trust

Level of Trust is a multi-layered concept that assesses the trustworthiness of a communication relationship or domain.

The quality of the connection history has the greatest influence on trust. A reliable and lasting communication relationship ensures that the level of trust increases; an unreliable and fragmented communication relationship ensures that the level of trust decreases.

NoSpamProxy includes various criteria in the calculation of the value:

Domain relationship| Regular outbound emails to a specific email domain are rewarded. So-called freemailers are excluded from this regulation by default. See [Level of trust configuration](#).

Address relationship between sender and recipient| Outbound emails to certain external addresses are rewarded with a high trust bonus. See [Level of trust configuration](#).

Combination of sender, subject and domain| Reply emails are rewarded if the subject and domain are unchanged.

Message ID| The message IDs contained in email headers are rewarded - similar to reply emails - if they are unchanged.

Delivery notifications| Valid notifications are rewarded, invalid notifications are penalised. See [Level of trust configuration](#).



NoSpamProxy rates an email as trustworthy if one of the bonuses described above is at least 40 points. The prerequisite for this is that the conditions mentioned at [Level of Trust](#) are fulfilled. If you want to ensure that emails from a specific partner are delivered, set the trust value fixed to 40 or higher. See [Editing partner domains](#). We also recommend that you make some form of authentication a pre-requisite for all bonuses. See [Authentication as a prerequisite for all bonuses](#).



NOTE: To protect the data, the relationship is not stored in plain text, but only in the form of a hash value (checksum).

Video: Level of Trust

Trust must be cultivated

If there is no outbound communication with a particular partner for a certain period of time, the level of trust is automatically reduced. This decrease in value occurs for both bonus and penalty values.



Automatic removal of partners

Partners are automatically removed when the Level of Trust value of the respective domain has dropped to 0 **and** the partner does not have any other properties that prevent this, such as stored users, passwords or certificates.

Points allocation for domains for Level of Trust

The bonus points for Level of Trust are assigned to the respective domains in two different ways:

- Automatically based on an outbound email.
- Manually via the user interface under **Partners** or via the PowerShell cmdlet `Set-NspPartnerTrustDetails`.

For an inbound email from this domain to receive the stored bonus points, at least one of the following conditions must be met in relation to the domain that has a certain trust level:

- The SPF check is successful.
- The DKIM check is successful.
- The DMARC check is successful.
- The email is signed using S/MIME or PGP and the signature is valid (and matches the domain in the email header).

- The IP address is mentioned in the properties of the domain. This list is automatically filled with the IP addresses that NoSpamProxy can read from the MX and A records of the respective domain. However, the addresses are only collected if there is no DMARC record for the sender domain.

No check for validity of the SPF entry is performed if the domain with trust set only appears in the header. Therefore, no DMARC validation can take place.

Consequently, if there is a difference between the MAIL FROM and Header-From domains, the email must have either

- at the partner entry a familiar subnet matches the submitting IP address or
- an S/MIME, PGP or DKIM signature belonging to the domain with the trust level set.



NOTE: In order for the above scenario to work, the Reputation filter must be enabled with checks for DMARC, SPF, DKIM and the sending IP address enabled in each rule where Level of Trust is active.

I Authentication as a prerequisite for all bonuses

To prevent attacks with fake email addresses, we recommend that you make some form of authentication a precondition not only for the domain bonus, but for all bonuses. See Level of trust configuration.

| Related steps

Related steps

How to activate Level of Trust| The Level of Trust system must be activated per rule. See [Steps in creating rules](#).

How to configure Level of Trust| The settings for Level of Trust are made under Level of Trust Configuration. See [Level of trust configuration](#).

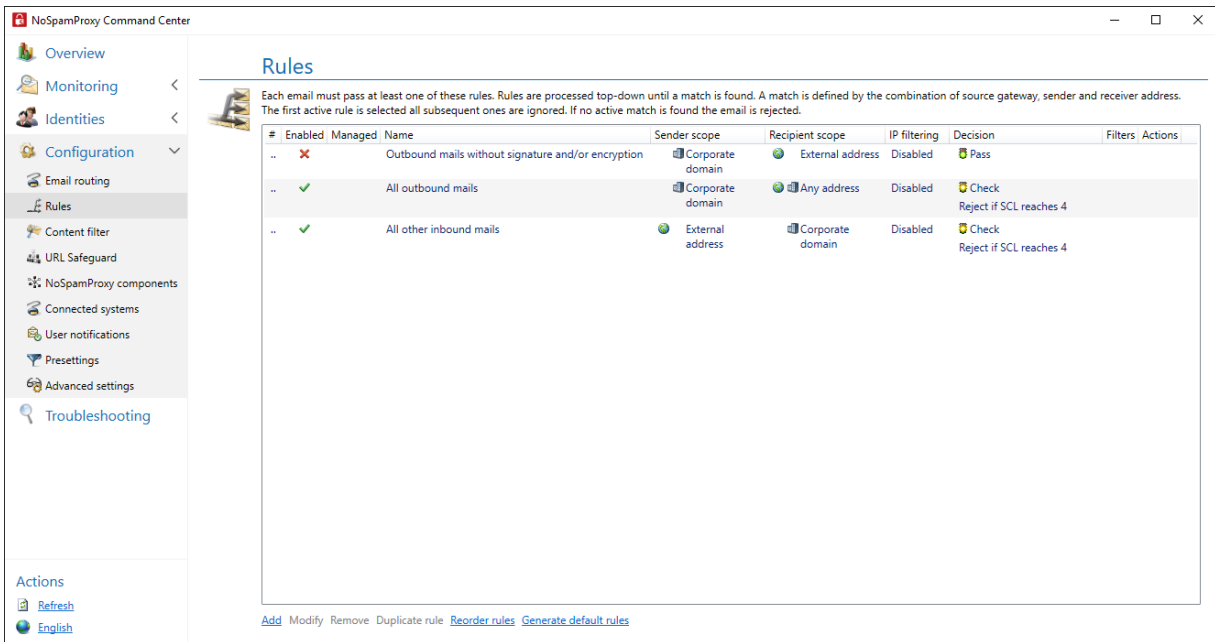
| See also

[Level of trust configuration](#)

[Spam Confidence Level \(SCL\)](#)

[How NoSpamProxy Protection classifies emails as spam](#)

Rules



What are rules?

NoSpamProxy applies rules when processing emails that you can configure individually. These rules are modular. You can create rules yourself and modify existing rules by selecting the desired filters for each individual rule from the available filters. Innerhalb jeder Regel können Sie diese beliebig mit einem Multiplikator gewichten und konfigurieren.

You can also specify that rules apply only to specific IP addresses or recipients, for example, only to senders with a specific TLD (Top Level Domain) or IP addresses from a specific subnet.



TIP: After reinstalling NoSpamProxy, you can create default rules. These enable the gateway to start functioning as quickly as possible with minimal administration effort. Nevertheless, you should check these rules and adapt them to your needs if necessary.

The order of the rules is crucial

If a rule is responsible for an email to be checked, it will be used. If more than one rule applies to an email, the rule that is highest in the list is applied.

How rules, filters and actions are related

To process emails, NoSpamProxy applies rules that you can configure individually. For each email, the individual filters of the applicable rule are executed. Filters evaluate how strongly the email meets a certain filter criterion and award corresponding penalty and bonus points. The awarded points are weighted with the multiplier of the filters and then added to a total value. If this value exceeds the set **Spam Confidence Level (SCL)** of the rule, the email will be rejected. You can set the allowed SCL individually for each rule. See [Filter konfigurieren](#) and [Filters in NoSpamProxy](#). [Actions in NoSpamProxy](#) are called up after the filters have determined whether the email is rejected or allowed to pass. Actions can, among other things, modify the emails, for example to add a footer or remove unwanted attachments. However, actions can also reject emails that would actually happen after they have been evaluated by the filters. This means that a virus scanner, for example, can still reject the email even though it has not been detected as spam. Actions are therefore higher-level settings with which filters can be overridden if

necessary. To find out which actions are available and how they work exactly, see [Actions available in NoSpamProxy](#).

Creating rules

For information on creating rules, see [Creating rules](#).

I Spam Confidence Level (SCL)

NoSpamProxy Protection rejects all emails whose Spam Confidence Level (SCL) exceeds a certain threshold. The administrator defines this threshold value in the individual [Rules](#).

Example 1

This example is based on the following filter configuration:

- Emails should be checked and rejected as soon as the SCL is greater than or equal to 4.
- Three filters are activated: Realtime Blocklists, Spam URI Realtime Blocklists and the word matches.
- The Word Matches filter is configured to search for the words Sex, Viagra, Cialis, etc. and to give two penalty points per hit.
- The two block list filters should give two points per hit.
- [Level of Trust](#) is switched off.

Now an email containing eight forbidden words and one forbidden link is processed. The link is included in a blacklist. Furthermore, the submitting IP address is represented on two blacklists.

Preliminary filter result

Filter	Spam Confidence Level
Realtime Blocklists	4 (Two hits times two penalty points per hit)
Spam URI Realtime Blocklists	2 (One hit times two penalty points per hit)
Word matches	16 (Eight hits times two penalty points per hit)

Basically, all filters - including the Level of Trust - always truncate the determined value to 10 if it is greater than 10. For negative values that are smaller than -10, the value is adjusted to -10.

"Net value" of the filters

Filter	Spam Confidence Level
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Word matches	10 (limited because the first value was >10)

Finally, the multiplier of the individual filters is taken into account. The filter Realtime Blocklists and Spam URI Realtime Blocklists have a multiplier of "2", the word matches have a multiplier of "1". The net value of the filters is now multiplied by the respective multiplier.

"Net value" and multiplier

Filter	Spam Confidence Level	Multiplier	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Word matches	10 (limited because the first value was >10)	1	10
Total			22

The email therefore receives an SCL of 22 and is thus rejected.

Example 2

In this example, the filter configuration from the first example is extended by the Level of Trust. It is the same email as in the previous example. However, we assume that this is a wanted email and that there is already an address pair and a domain bonus in the database from the sender and recipient address.

- Since the last email contact was already four days ago, the address pair bonus with 65 bonus points is not as high anymore. The domain, on the other hand, is trusted with a static 100 bonus points.
- The bonus points of the Level of Trust in the database are not directly the SCL value, but the so-called trust points. These are only used within the filters.

Evaluation by Level of Trust

Existing negative values as well as positive values are included in the calculation of the Level of Trust. Negative values can be caused, for example, by the intelligent DSN check or manually set values. In principle, negative values then take precedence over positive values. So if an email had received **+100** trust points for the domain, but had been assigned **-5** trust points for other reasons, these **-5** trust points would be used as the basis of the weighting.

To calculate the SCL, the resulting value is then divided by the value **-10** and results in an SCL of **-10** points in this example. As with all other filters, the determined value is clipped to **10** or **-10**. The table with the net values of all filters now looks as follows:

Filter	Spam Confidence Level
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Word matches	10 (limited because the first value was >10)
Level of Trust	-10

You can define the multiplier of the individual filters in the respective rule. The Level of Trust, on the other hand, determines its multiplier independently. For this purpose, the multipliers of all other filters are added and result in this example in the value **5**.

Result from Spam Confidence Level and Level of Trust

Filter	Spam Confidence Level	Multiplier	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime	2	2	4

Filter	Spam Confidence Level	Multiplier	SCL
Blocklists			
Word matches	10 (limited because the first value was >10)	1	10
Level of Trust	-10	5 (=2+2+1)	-50
Total			-28

The email would have been delivered in this example because the SCL is less than 4. To clarify the example, the Core Antispam Engine filter is also configured with the multiplier "3". This filter always assigns 4 points for a hit and this value is also not configurable.

The Core Antispam Engine filter also rates the email poorly.

Final result of the SCL calculation

Filter	Spam Confidence Level	Multiplier	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Word matches	10 (limited because the first value was >10)	1	10
Core Antispam Engine Filter	4	3	12
Level of Trust	-10	8 (=2+2+1+3)	-80
Total			-46

The multiplier of Level of Trust has automatically adjusted itself through the additional filter and can therefore have a greater impact on the result. This ensures that intended communication always reaches the recipient - regardless of the content of the email.

I URL Safeguard

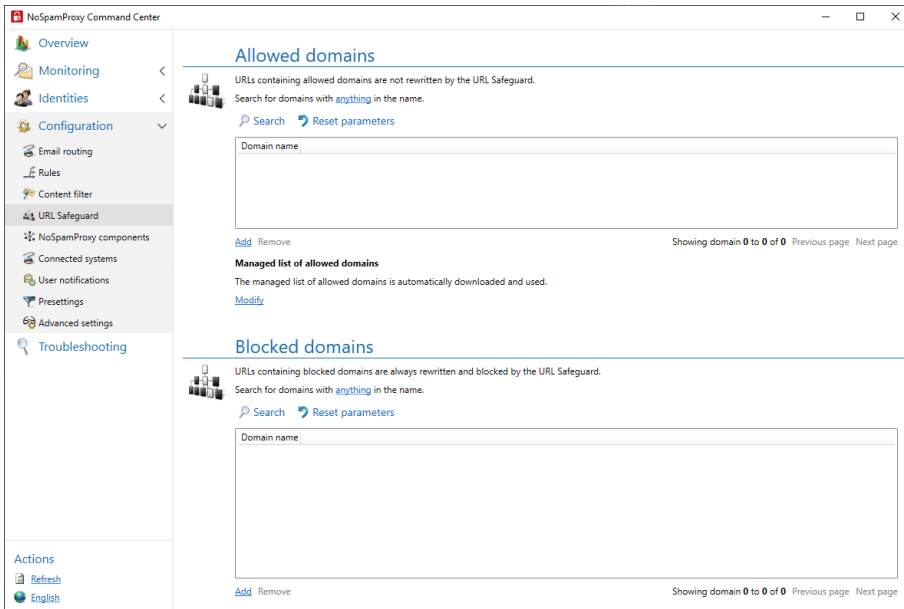
If configured accordingly, the URL Safeguard cross-checks the links in inbound emails against entries in the following lists:

- NoSpamProxy Allowlist, a list of known websites curated by NoSpamProxy.
- The local allowlist created by the administrator.

Domains that exist in one of these lists as well as your corporate domains will never be rewritten by the URL Safeguard.



NOTE: You can make settings for the NoSpamProxy Allowlist and the local allowlist under **Configuration > URL Safeguard** .



How does the URL Safeguard work?

If the domain contained in the link is not present in any of the lists, NoSpamProxy replaces the original link with a link that points to the Web Portal.

- NoSpamProxy replaces the original link with a link that points to the Web Portal.
- NoSpamProxy replaces the original link with a link that points to the Web Portal and blocks access to the original link.

In both cases, the e-mail delivered to the recipient contains only the rewritten link.

- If the link is classified as safe, access to the original URL is permitted and executed.
- If the link is classified as unsafe, access is denied. A notification about the incident will be added to the message tracking. Depending on the configuration, the administrator also receives a notification.



TIP: Blocked URLs can be unblocked by adding them to the local allowlist. The domain belonging to the blocked URL can be viewed on the Web Portal by the recipient of the e-mail after clicking on the rewritten link. The responsible administrator can then carry out the activation. A further delivery of the email by the communication partner is not necessary.

Frequently asked questions

What is a Protected Link?

The expression **Protected Link** is displayed instead of a URL if the display text contains a URL that can be copied into the browser and leads to a potentially harmful page.

Can the Protected Link tag be changed?

Yes. See [Anpassen des Tags Protected Link im URL Safeguard](#).

In which cases are URLs rewritten?

The URL or the display text in the email is rewritten if the domain of the URL of the display text or the actual link is not on the NoSpamProxy Allowlist or the local allowlist.

What can I do if links to the Web Portal cannot be opened due to their length?

A long link to the Web Portal may mean that it cannot be opened, as it exceeds the length limit of some browsers due to the rewriting. The original URL **cannot** be tracked in the associated message track, even if tracking has been activated. Only a shortened version is displayed there. You can view the Fully Qualified Domain Name (FQDN) in the associated Message Track, on the **URL Safeguard** tab, provided that tracking has been activated (see [Default partner settings](#)). To prevent links from this domain from being rewritten in the future, add the corresponding domain to the local allowlist. See [URL Safeguard einrichten](#).

See

[URL Safeguard einrichten](#)

[Anpassen des Tags Protected Link im URL Safeguard](#)

[URL Safeguard \(Action\)](#)

[Vorschaltseiten URL Safeguard](#)

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

Points allocation for domains for Level of Trust

The bonus points for Level of Trust are assigned to the respective domains in two different ways:

- Automatically based on an outbound email.
- Manually via the user interface under [Partners](#) or via the PowerShell cmdlet `Set-NspPartnerTrustDetails`.

For an inbound email from this domain to receive the stored bonus points, at least one of the following conditions must be met in relation to the domain that has a certain trust level:

- The SPF check is successful.
- The DKIM check is successful.
- The DMARC check is successful.
- The email is signed using S/MIME or PGP and the signature is valid (and matches the domain in the email header).
- The IP address is mentioned in the properties of the domain. This list is automatically filled with the IP addresses that NoSpamProxy can read from the MX and A records of the respective domain. However, the addresses are only collected if there is no DMARC record for the sender domain.

No check for validity of the SPF entry is performed if the domain with trust set only appears in the header. Therefore, no DMARC validation can take place.

Consequently, if there is a difference between the MAIL FROM and Header-From domains, the email must have either

- at the partner entry a familiar subnet matches the submitting IP address or
- an S/MIME, PGP or DKIM signature belonging to the domain with the trust level set.



NOTE: In order for the above scenario to work, the Reputation filter must be enabled with checks for DMARC, SPF, DKIM and the sending IP address enabled in each rule where Level of Trust is active.

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](tel:+495251304636)
- by email at support@nospamproxy.de.

