Net at Work
Building IT-Excellence.

NoSpamProxy 13.2

Manual

- Protection
- Large Files

Imprint

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

Trademarks

27 July 2020

Contents

1. NoSpamProxy

NoSpamProxy Protection

Spam and spam protection

Spammers are applying increasingly elaborate methods in order to disable existing protection systems and spread their messages among recipients. Unfortunately, thorough inbox hygiene does not prevent spammers from reaching their goals. Meanwhile, spam has become a serious economic burden on many companies.

Spam interferes with business processes and binds employees as well as system resources. Moreover, unwanted emails can have a devastating effect on your email servers. These emails may carry harmful contents and attachments aimed at attacking and spying out your company data, thus posing a threat to the security of your company.

Furthermore, spammers often try to misuse your system as a relay. In these cases, emails are sent in your name, and at the cost of your capacity. As a result, reliable email partners may classify your domain as a spam sender which then leads to important business connections getting blocked.

The attack scenarios are complex, and not all spam is the same. The interests of companies differ, as do the classifications of emails. Therefore, you should be able to classify certain types of emails such as junk email, newsletters or emails containing Chinese characters as spam. This is where NoSpamProxy Protection comes into play.

Rejection instead of sorting

Response times of spammers have dropped significantly, and the responses themselves have reached a new level of sophistication. Static spam filters might work successfully for a short period of time but are often useless in the long run.

In order to be effective, spam protection systems must work intelligently and flexibly, and they must be able to adapt to the situation at hand.

A spam protection system must be able to protect you from unwanted emails and at the same time be able to classify safe emails as such. A 99% quota for blocked spam emails sounds fine; but it may create more damage than good if important emails are accidentally blocked or moved to the wrong folder. In addition, protection should be specific and adjusted to the requirements of your business processes. The size of your organisation is irrelevant; in the end, a protection system should not only protect your organisation from spam emails but also from unnecessary burdening of the system, as the conservation of your resources is central.

These requirements for intelligent spam protection were our incentive to develop NoSpamProxy Protection. The basic idea is simple; in contrast to other filters, NoSpamProxy Protection rejects spam emails before they enter your system: rejection instead of sorting.

How can I report a False Positive as a user?

False Positives are safe emails which are accidentally classified as suspicious and subsequently rejected. As mentioned above, this is one of the major threats to filter solutions. The more spam you

need to sort out, the more likely it is for you to accidentally remove safe emails, and the consequences might be very serious.

Assuming you receive information from a customer via phone that an email sent to you did not get through, was classified as spam and rejected. You can solve this unpleasant situation easily with NoSpamProxy Protection. You do not need to be an administrator, implement specific system settings or modify NoSpamProxy Protection. Instead, simply send an email to the customer, and the issue is solved.

The next email sent by the customer will automatically be classified as safe by NoSpamProxy because it is a reaction to your email, even if the sender does not use the "Reply" function.

This also means that a second try usually gets through without any problems, and no further False Positives are created. The email address of the sender is classified as trustworthy by NoSpamProxy Protection.

Proxy instead of relay

NoSpamProxy is, as its name suggests, designed as a proxy. Simply put, a proxy is a stop-over point between the Internet and your system. Similar to a firewall, your internal network is protected from unfiltered contact with the Internet.

For emails sent to owned domains, an external connection to NoSpamProxy is established. Then, NoSpamProxy will establish a second connection to your email server.

NoSpamProxy collects the data, extracts the relevant SMTP information and reconstructs the email based on the data and information gathered. The email is then delivered to the configured filters for inspection. If an email is identified as spam, NoSpamProxy Protection rejects it. This forces the incoming email server to send a non-delivery report to the sender. A proxy is perfectly suited for realising early spam rejection.

Advantages of proxy

Many functions of the internal email server remain usable. For instance, the server will still reject emails in case the inbox is full or does not exist. In turn, NoSpamProxy Protection rejects the connection externally.

Your system will not be loaded with unnecessary data. Many connections can be identified as origins of spam at a very early stage and do not burden the internal email server.

Protective function

You server is unavailable externally. Thus, 'Denial of Service'-attacks do not interfere with internal communication.

NoSpamProxy Large Files

With Large Files, users can transmit files of any size to recipients via their Outlook client without straining the organisation's email system. Instead of sending the file itself, a link is attached to the email. This link can be used to safely download the files via TLS. Additionally, you can send the invitation link for the Large Files Web Portal, enabling recipients to send you large files.

Please do not hesitate to contact us at info@netatwork.de if you are interested in NoSpamProxy Large Files. We will be happy to provide advice and support in extending your existing licence.

NoSpamProxy Disclaimer

NoSpamProxy Disclaimer automatically integrates configurable email disclaimers into your emails during their composition. The configuration consists of two parts; the NoSpamProxy administrator that prepares values and settings for the disclaimers, and the administrators for the disclaimer creation that can use these values and settings on the disclaimer website in their created templates and rules.

A detailed description of the value configuration can be found in chapter Disclaimer.

Advantages of NoSpamProxy Encryption

Since NoSpamProxy Encryption is based on the technologies of the tried and tested AntiSpam gateway NoSpamProxy, its functions can easily be activated through a licence extension. The confidential communication with partners can be realised on one gateway only and with a consistent administration.

If you want to connect NoSpamProxy with systems not based on SMTP such as De-Mail, E-Postbrief, Deutschland-Online infrastructure and POP3 inboxes, you can implement this by installing an extended licence with NoSpamProxy Encryption.

2. Help and support

Net at Work offers many forms of help and support for the installation and the operation of NoSpamProxy.

- **Training videos**
  Training videos provide an overview of different areas and include step-by-step configuration tutorials as well as practical examples.
- **Blog**
  The Blog provides daily updated alerts for new product versions, suggested changes to your configuration, warnings on compatibility issues and more help. To make sure you do not miss any important advice, you can also find the latest news from the blog on the start page of the NoSpamProxy configuration console.
- **Knowledge Base**
  The Knowledge Base contains additional information on specific issues.
- **Support**
  If you require additional support, please visit our support website.

3. System requirements

Information about system requirements and the supported software can be found in the Knowledge Base.

4. The roles of NoSpamProxy

NoSpamProxy comprises several roles which are described below.

Gateway Role

The Gateway Role is the core component of NoSpamProxy. Depending on your environment, this role can either be installed in a demilitarised zone (DMZ) or the intranet. To ensure high availability of your system without downtime, this role can be installed on multiple servers.

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

Intranet Role

As its name suggests, the Intranet Role is usually installed as part of your company intranet.

Web Portal

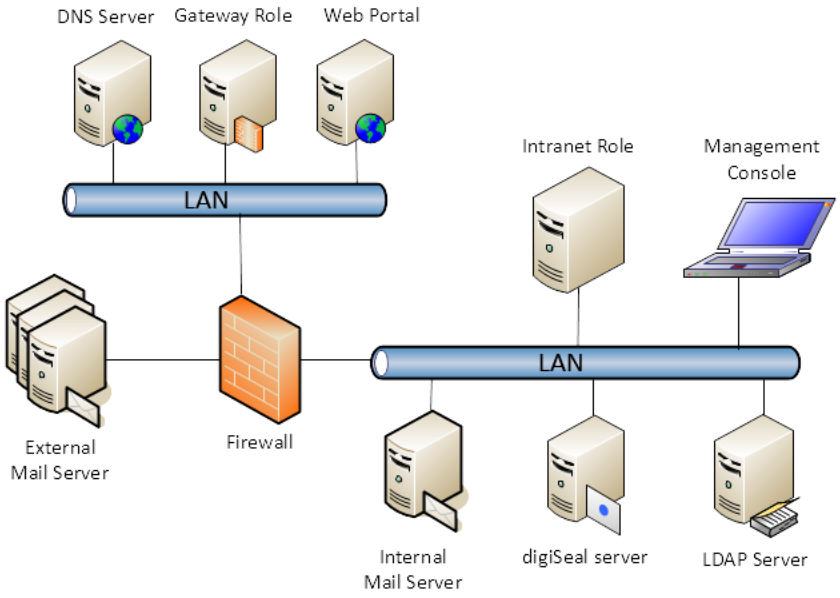
If you have activated Large Files, users can transmit large files via the Web Portal.

In order to set up a highly-available system, this role can be installed on multiple servers.

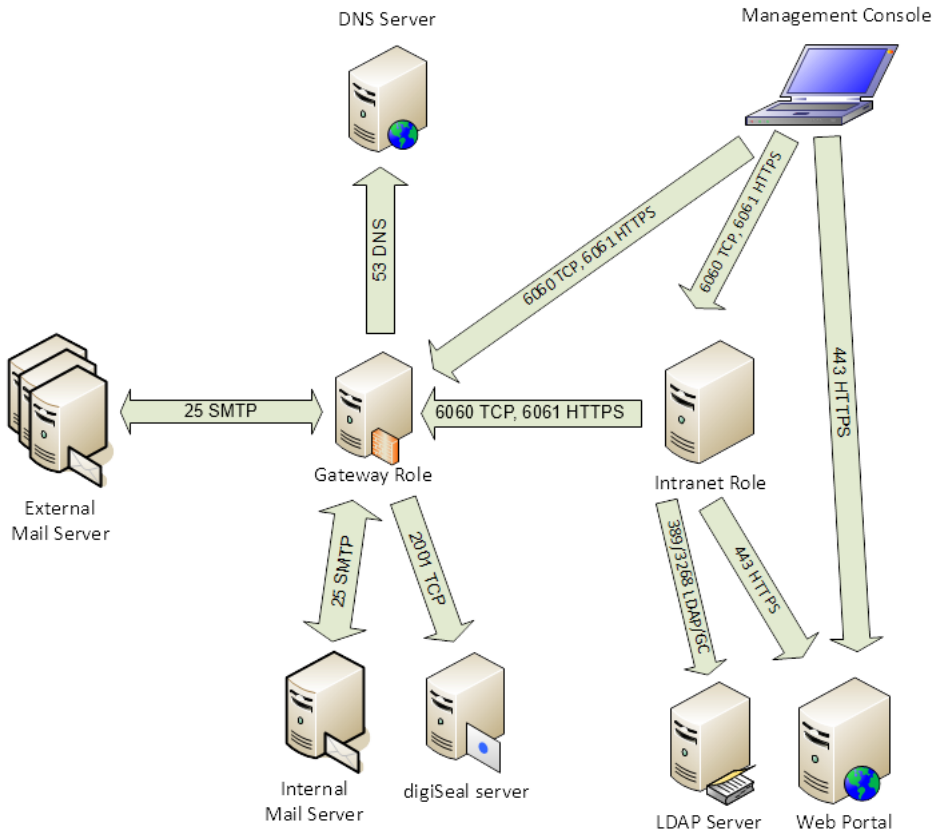
5. Functionality and infrastructure integration

NoSpamProxy communicates with other infrastructure components within your environment (Picture 1).

All components of the system can be operated on the same server. In small environments, NoSpamProxy can be installed along with a firewall and your email server on one single server. In addition to the individual components, the TCP Ports which are used between the components are documented as well (Picture 2).



Picture 1: NoSpamProxy components



Picture 2: NoSpamProxy infrastructure integration and communication

Firewall

To ensure successful operation of NoSpamProxy, all necessary network connections must be available at all times and remain unblocked by network configurations. The SMTP protocol on port 25/TCP and the DNS protocol on port 53 TCP/UDP are particularly relevant. If the NoSpamProxy roles are installed in different network segments, the communication for TCP on port 6060 and for HTTPS on 6061 must be allowed on the firewall. Both the management console and the Intranet Role use port 443/HTTPS to access the Web Portal.

SMTP Mail Server

To enable the Level of Trust system get to know the communicative relations of your organisation, emails to external addresses should be sent via NoSpamProxy.

SQL Database

NoSpamProxy saves the data required for its operation in a Microsoft SQL database. For this, Microsoft SQL Server 2008 or later is required. The free Express Edition can be used as well.

Domain Name System (DNS)

Your system should feature Domain Name System (DNS) lookup. The DNS name under which the respective email server communicates must also resolvable via DNS. If a server communicates as "mail.netatwork.de", it should also be resolvable as "mail.netatwork.de" in the DNS. If it is not resolvable, the domain name is either incorrect (which suggests a misconfiguration of the DNS server) or the DNS name is not maintained in the DNS.

Directory Service, Active Directory

NoSpamProxy can reject emails to non-existent or non-entitled recipients upon receipt. This requires a list of valid SMTP addresses to be maintained in the gateway. For example, this can be realised via automatic synchronization with Active Directory or Lotus Domino data. Alternatively, users can also be maintained manually.

Examples of implementation

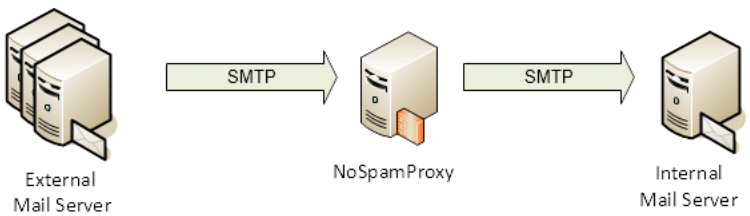
General information on the application of NoSpamProxy

Whether the email originates from a provider or directly from the sender; NoSpamProxy is at the forefront all email communication as it is placed before the first email server or relay of the recipient.

If this is not the case, neither the IP address of the incoming gateway can be checked nor can the connection be terminated. Instead, the incoming gateway will send a non-delivery report. The fundamental advantage of rejecting emails and saving data offered by NoSpamProxy could not be utilised.

Upstream NoSpamProxy

The simplest setup design is to place NoSpamProxy as an individual system upstream to your own email server (Picture 3).

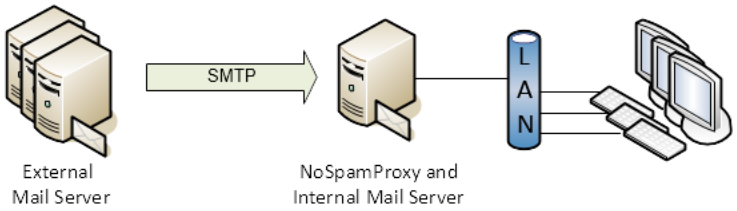


Picture 3: NoSpamProxy placed upstream to your own email server

NoSpamProxy on the Mail Server

Providing a separate server for NoSpamProxy in small environments might be too laborious and time-consuming. In this case, the gateway can be installed on an existing email server.

This requires changing the configuration of the existing email server as follows: Instead of receiving emails on port 25, you configure another port for doing so (e.g. 2525). Subsequently, you configure a smarthost in NoSpamProxy for emails to local addresses for host 'localhost', port '2525'.

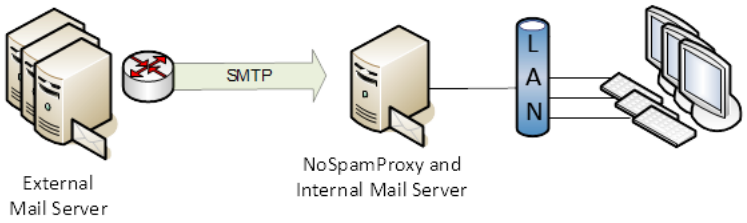


Picture 4: NoSpamProxy on the email server

NoSpamProxy now receives the connections on port 25 and transfers them to the email server via 'localhost:2525'.

NoSpamProxy with NAT router

If the server itself does not have its own official IP address, a system located in front of the server is responsible for the implementation. With smaller installations, this is mostly a router with Network Address Translation (NAT).

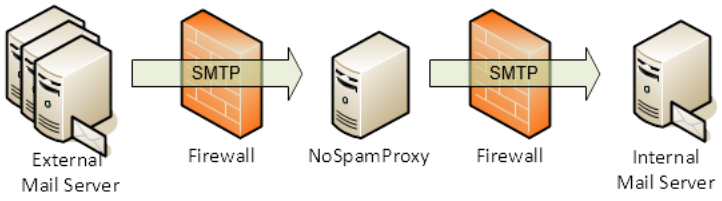


Picture 5: NoSpamProxy with NAT router

This router must be configured for NoSpamProxy in such a way that it transfers all connections which are received on the official IP address to NoSpamProxy at port 25. The configuration of NoSpamProxy is identical to one of the two previous examples.

NoSpamProxy with firewall and DMZ

Larger installations often use a multi-level firewall or a so-called "demilitarised zone" (DMZ) which makes it possible to gain better control over the data traffic between the systems.



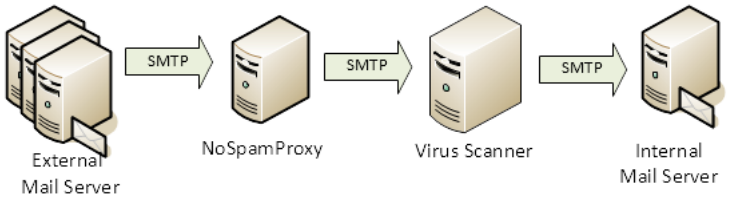
Picture 6: NoSpamProxy with firewall

In this case, NoSpamProxy is installed on a dedicated server in the DMZ. The firewall permits connections from the outside to the server, to port 25 of NoSpamProxy. To enable this configuration, you should only install the Gateway Role in the DMZ. The Intranet Role should be installed in the intranet.

NoSpamProxy and SMTP virus scanner

NoSpamProxy can take multiple approaches to virus identification, as described below.

- **Cyren AntiSpam**
  Emails can be checked for viruses and malware through the Cyren AntiSpam service. This service is automatically installed along with NoSpamProxy.
- **On-access virus scanner on the NoSpamProxy server**
  A virus scanner installed alongside NoSpamProxy can check emails with the help of the action File based virus scanner.
- **SMTP virus scanner as SMTP relay**
  An SMTP virus scanner usually works as an SMTP relay and must therefore be installed between NoSpamProxy and your intranet



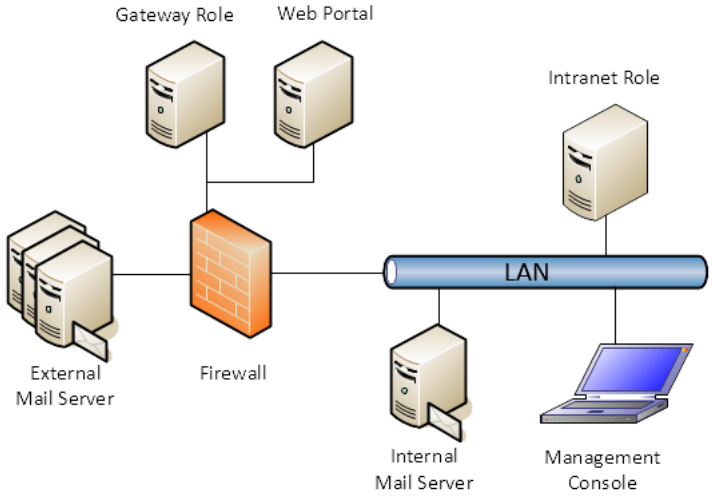
Picture 7: NoSpamProxy with virus scanner

An SMTP virus scanner usually works as an SMTP relay and must not be integrated between the Internet and NoSpamProxy.

Installation of the roles on different servers

In very small environments, it is recommended to install all roles on one server. NoSpamProxy offers full functionality even when installed on a Small Business Server.

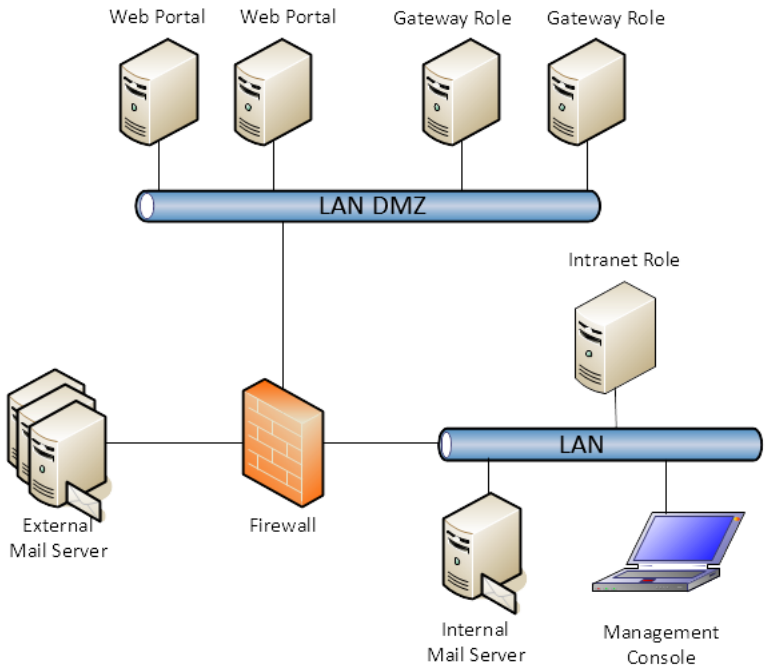
The following chart shows a possible distribution of roles for larger environments which include a DMZ. (Picture 8).



Picture 8: Installation of NoSpamProxy in the DMZ

A server with the installed Gateway Role is located in the demilitarised zone (DMZ). Here, the emails are processed, filtered and subsequently forwarded to the internal email server. A server on which the Intranet Role is installed runs in the LAN. On the firewall, only port 6060 for TCP and port 6061 for HTTPS must be opened from the LAN into the DMZ for data transfer between the Gateway Role and the other two roles. The only mandatory connection from the DMZ to the LAN is port 25 for email communication.

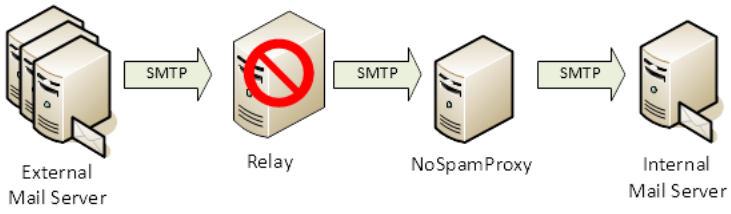
In environments where large amounts of emails are exchanged it is possible to install multiple servers with the Gateway Role in the DMZ. This ensures high availability of your system. The NoSpamProxy management console can be installed on the PC of the administrator from which all other roles in the LAN and the DMZ can be managed (Picture 9).



Picture 9: Roles of NoSpamProxy on distributed servers

How not to do it: creating a faulty configuration

This figure shows a non-permissible installation.



Picture 10: Example of a faulty configuration - NoSpamProxy is inoperational

As mentioned before, emails are received completely by the relay before they are sent to NoSpamProxy. As a result, NoSpamProxy will not function properly. Neither is data volume conserved nor can NoSpamProxy reject existing connections. It is impossible to check the IP addresses of the incoming gateways.

Emails to external addresses

The success of the Level of Trust system depends to a large extent on emails being sent to external addresses via NoSpamProxy.

For outbound emails, NoSpamProxy can use an external smarthost or deliver emails directly. If you send via a smarthost, you can, for instance, use the smarthost of your provider or an email relay especially installed for this purpose.

If you do not have a static IP address, you should send emails to external addresses via your provider. Dynamic IP addresses will be categorically refused by many companies and email providers.

6. NoSpamProxy management console

NoSpamProxy is managed via a Microsoft Management Console (MMC). The installation of the console is described in the NoSpamProxy installation manual. Please follow the instructions given in this manual before activating NoSpamProxy.

The management console of NoSpamProxy is divided into the following areas:

- **The dashboard**
  Beneath the top node of the management console named **NoSpamProxy** you will find the dashboard. It provides a quick overview of the entire gateway with all connected roles. It also lets you perform different tasks which are described in the chapter of the dashboard.
- **Monitoring**
  The **Monitoring** provides an overview of the receipt and delivery of emails. You can also access the event viewer of all connected roles.
- **Peoples and identities**
  The area **Peoples and identities** lets you manage your owned domains and corporate users but also external communication partners. You can determine settings regarding confidence and security for these identities.
- **Configuration**
  The nodes beneath **Configuration** serve the configuration of NoSpamProxy. Here you define send and receive connectors for emails, your rules and messages but also the connections to NoSpamProxy components or components of third party providers.
- **Troubleshooting**
  The area **Troubleshooting** lets you analyse potential issues with NoSpamProxy and its configuration. You can create log files of individual NoSpamProxy components or have settings corrected automatically.

Changing the client language

The NoSpamProxy client is automatically set to the system language. To change the language, click on the node **NoSpamProxy** and select **Action** / **Change language**. Alternatively, you can access this function by right-clicking on **NoSpamProxy**. The client must be restarted for the change to become effective.

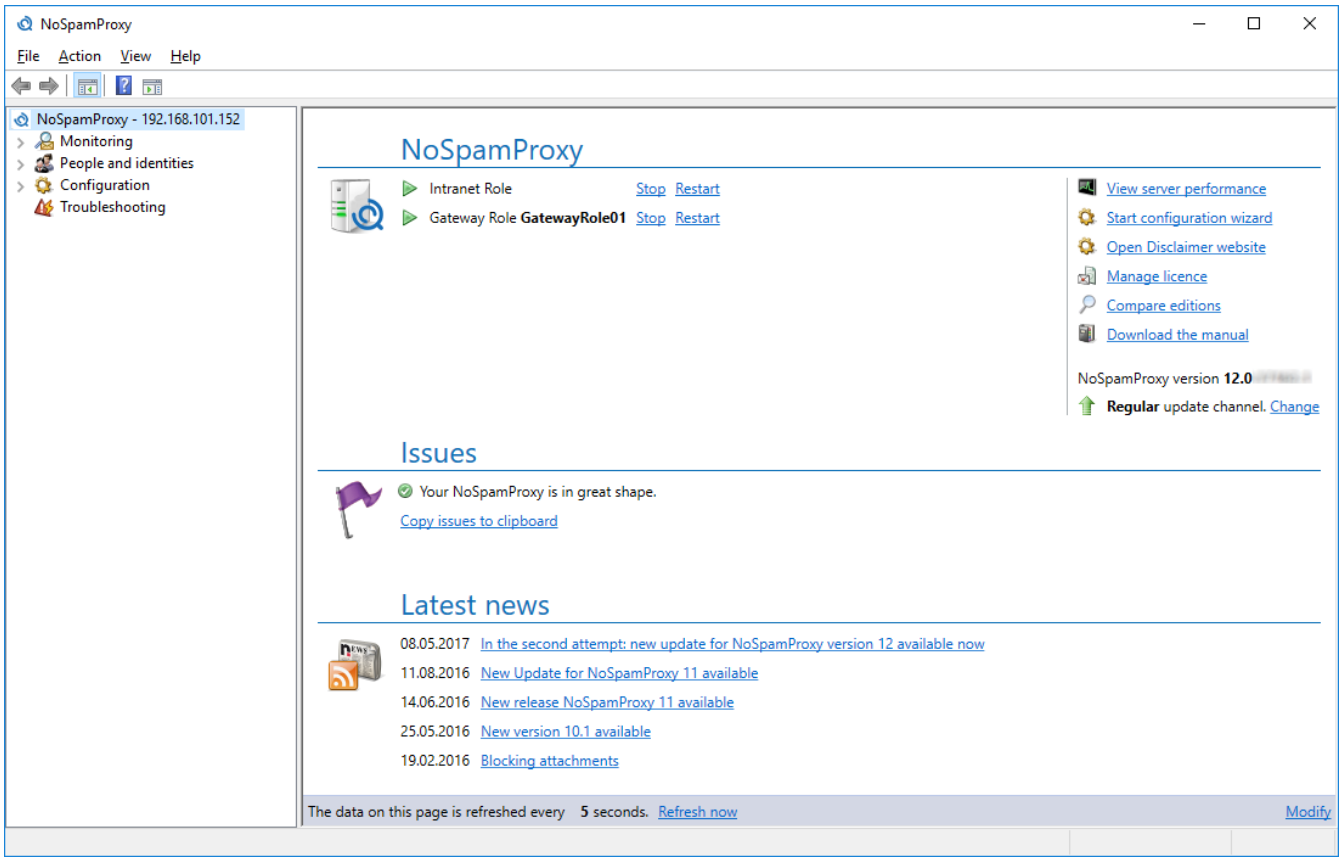
Establishing a connection to the Intranet Role

After completing the NoSpamProxy installation, the connection of the management console is set to `localhost`. To install the console on a workstation other than the one used for the Intranet Role, you need to adjust the connection. Go to **Action** / **Change server**. Enter the name of the server (for example: "mail.example.com") and the port (usually "6060"). Alternatively, you can access this function by right-clicking **NoSpamProxy**. The client must be restarted for the change to become effective.

If the gateway is operated in a DMZ and you want to remotely control the service from the LAN with the NoSpamProxy MMC, you just need to activate the TCP port 6060 and for HTTPS the port 6061 on the firewall. This connection is encrypted based on the certificate.

7. Dashboard

The page under **NoSpamProxy** (Picture 11) provides you with a quick overview of the status of the installed roles.



Picture 11: The overview of the Gateway Role configuration

Upon initial activation, NoSpamProxy is largely unconfigured. The missing configuration options appear in the list **Incidents**. Instead of working on each incident individually, we recommend using the configuration wizard. The wizard supports you in quickly and completely activating NoSpamProxy in most environments. It identifies and creates the recommended configuration based on the licenced functions.

List of the roles

All connected roles are directly listed beneath the heading **NoSpamProxy**. The list indicates for each role whether it is started or stopped. Additionally, you can also start, stop and restart the roles manually. After installing the licence, a summary of the licence is shown beneath the list

Area for actions

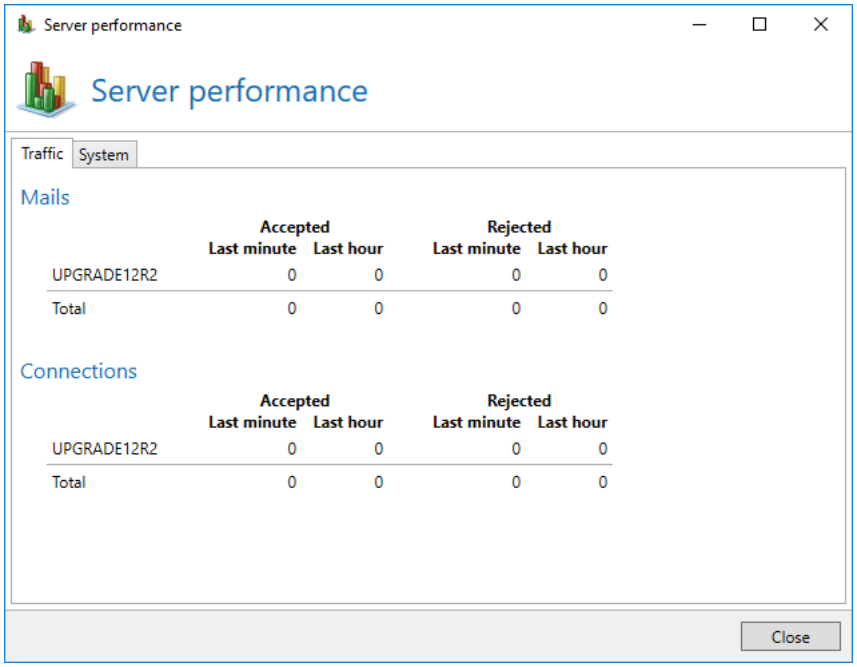
Available actions are shown at the top right corner. The action **open disclaimer website** leads you to the templates and rules for the Disclaimer. The installed version of NoSpamProxy appears beneath the list with the actions.

View server performance

The action **View server performance** offers you a quick overview of the current processing of emails and the currently available resources.

Data traffic

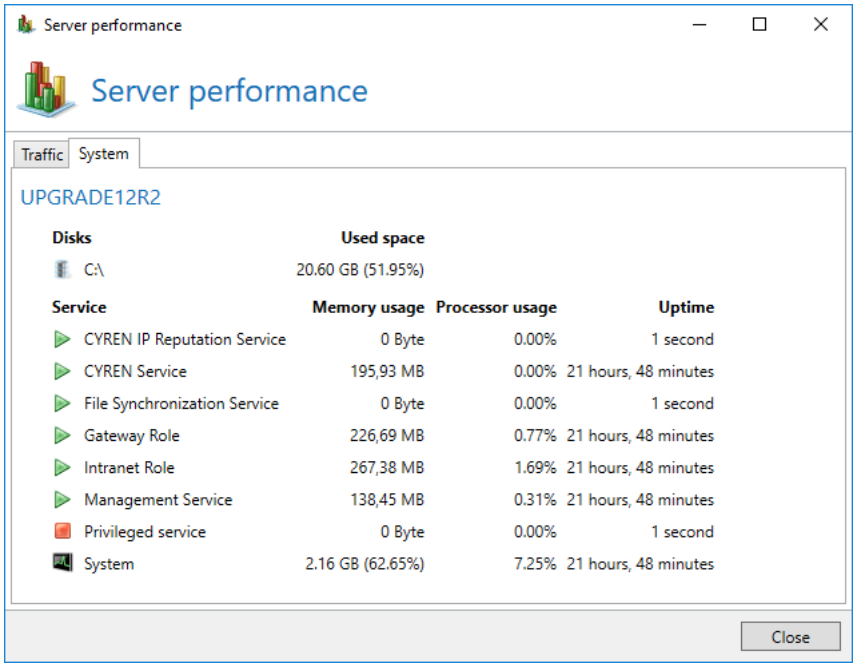
The page **Data traffic** shows a moving average of the processed emails of the last minute or hour. The page is updated automatically and shows whether NoSpamProxy is currently receiving emails (Picture 12).



Picture 12: The currently processed messages

System

The page **System** shows the installed services for each system with intranet or Gateway Roles, their status and the used resources (Picture 12).



Picture 13: The used and available resources

In addition to this view, the Performance counters are also available to you on the server.

Starting the configuration wizard

The **Configuration Wizard** guides you through all necessary steps of the NoSpamProxy configuration:

- **Licence**
  Install a licence or alter the existing Licence. If you have not yet created any rules, you can automatically create Default rules based on your licenced functions.
- **Connection to the Gateway Role**
  If no Gateway Role has yet been connected, you can connect your Gateway Role here. After adding the role, please set the DNS name for the Server identity of this Gateway Role.
- **Owned domains**
  Configuration of Owned Domains. If the gateway has not yet entered owned domains during the execution of the wizard, the primary domain of the licence is added to the list of owned domains in this step.
- **Local email servers**
  Configuration of the local email servers.
- **Local delivery**
  Configuration of inbound delivery of emails to corporate email servers.
- **External delivery**
  Configuration of outbound delivery of emails to external email servers.
- **Administrative notification addresses**
  Configure the administrative email addresses.

- **Sensitive data protection**
  Set a password to protect your sensitive data.

After the completion of the wizard, please perform a check:

- Check the configuration of the Receive connectors.

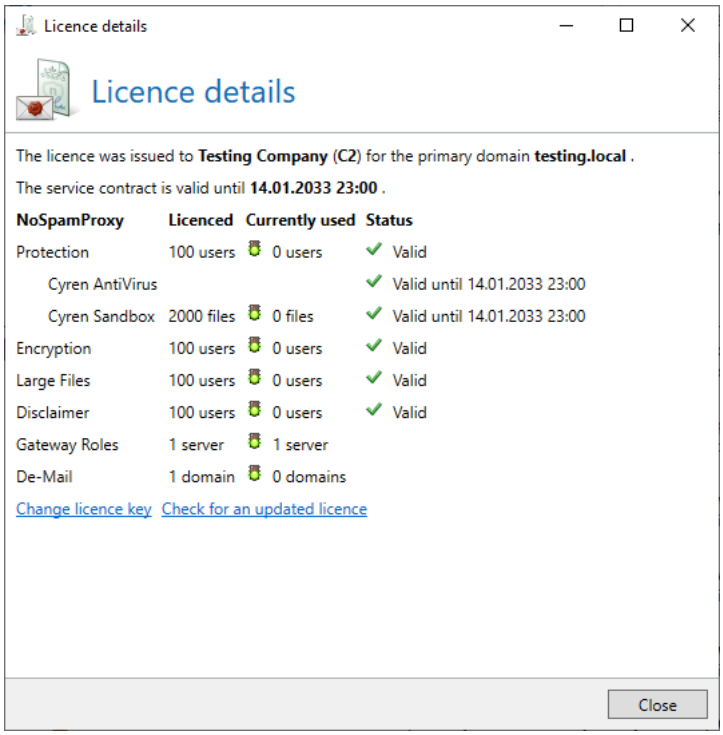
Following these steps ensures that NoSpamProxy is fully operational.

NoSpamProxy manual

Click to download the current user manual. If you have already activated your NoSpamProxy licence, the respective version of the manual will be downloaded.

Licence management

This action opens the dialog for the licence currently used. It shows you all relevant licence information and generates alerts in case issues with the licence emerge (Picture 14).



Picture 14: The currently installed licence

Here, you see your C number, domain as well as all licenced functions along with their validity period. Click **Change** to load another NoSpamProxy licence file. This requires a maintenance agreement which is valid at least as long as the currently used licence.

How to compare editions

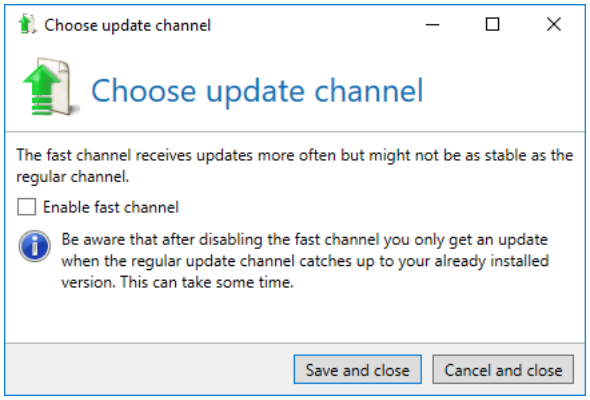
This link opens a document which lets you compare the licences available for NoSpamProxy.

Software updates

This action is shown in case a new NoSpamProxy version is available. It lets you download the NoSpamProxy installation file; you can initiate the installation manually.

Select update channel

Updates for NoSpamProxy are distributed via two update channels. The **regular channel** and the **fast channel** (Picture 15). The regular channel is the default setting and will provide updates with a long test history and the highest stability for NoSpamProxy. In contrast, the fast channel will provides updates earlier. The updates available on the fast channel have also passed all automatic tests have been successfully installed, but may suffer from stability issues.



Picture 15: Settings for the update channel

If you switch from fast to regular channel, you will only be offered updates if the version number of the respective update is higher than the one currently installed.

Incidents

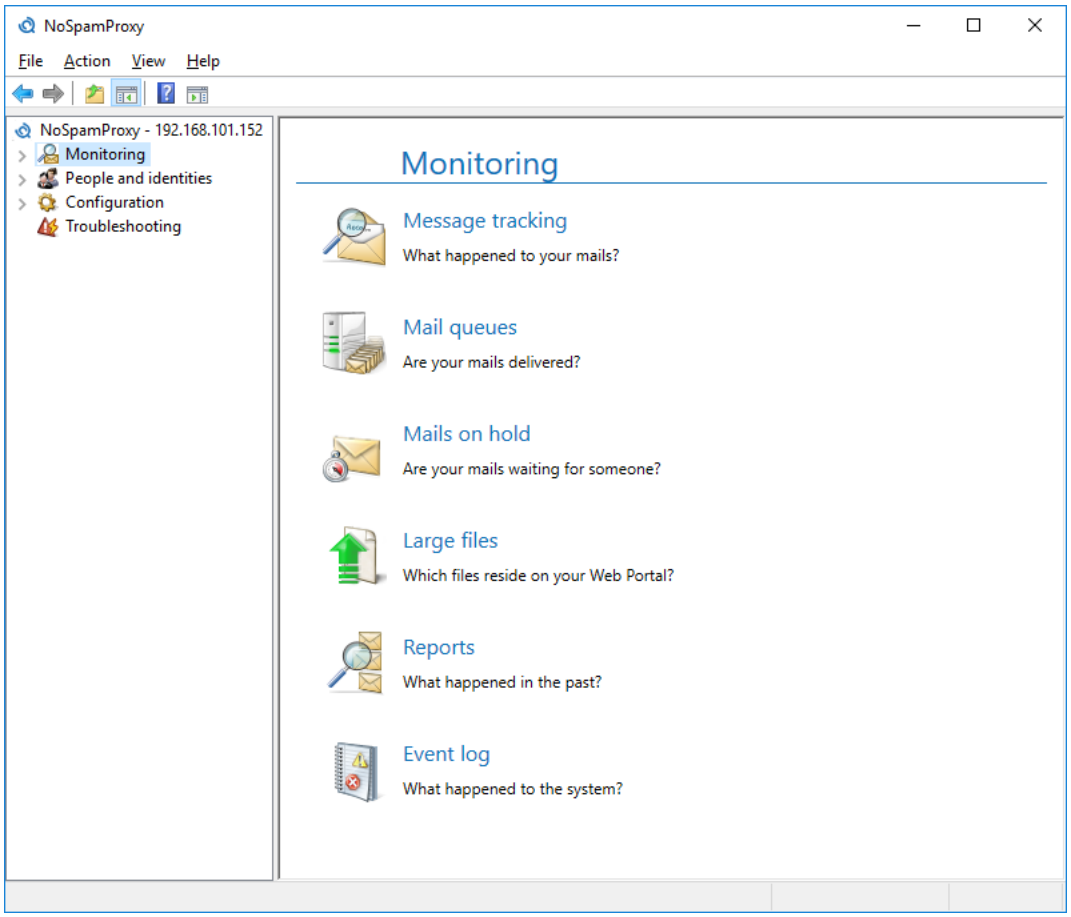
The list of **Incidents** shows you missing or misconfigured settings relevant for the operation of NoSpamProxy (if any).

Latest announcements

These announcements inform you about product updates or general suggested improvements concerning the configuration of NoSpamProxy. Click the headings to read the corresponding article in the NoSpamProxy blog.

8. Monitoring

The nodes under Monitoring (Picture 16) inform you about the receipt and dispatch of your emails. Moreover, status information on the system and the email traffic are shown.

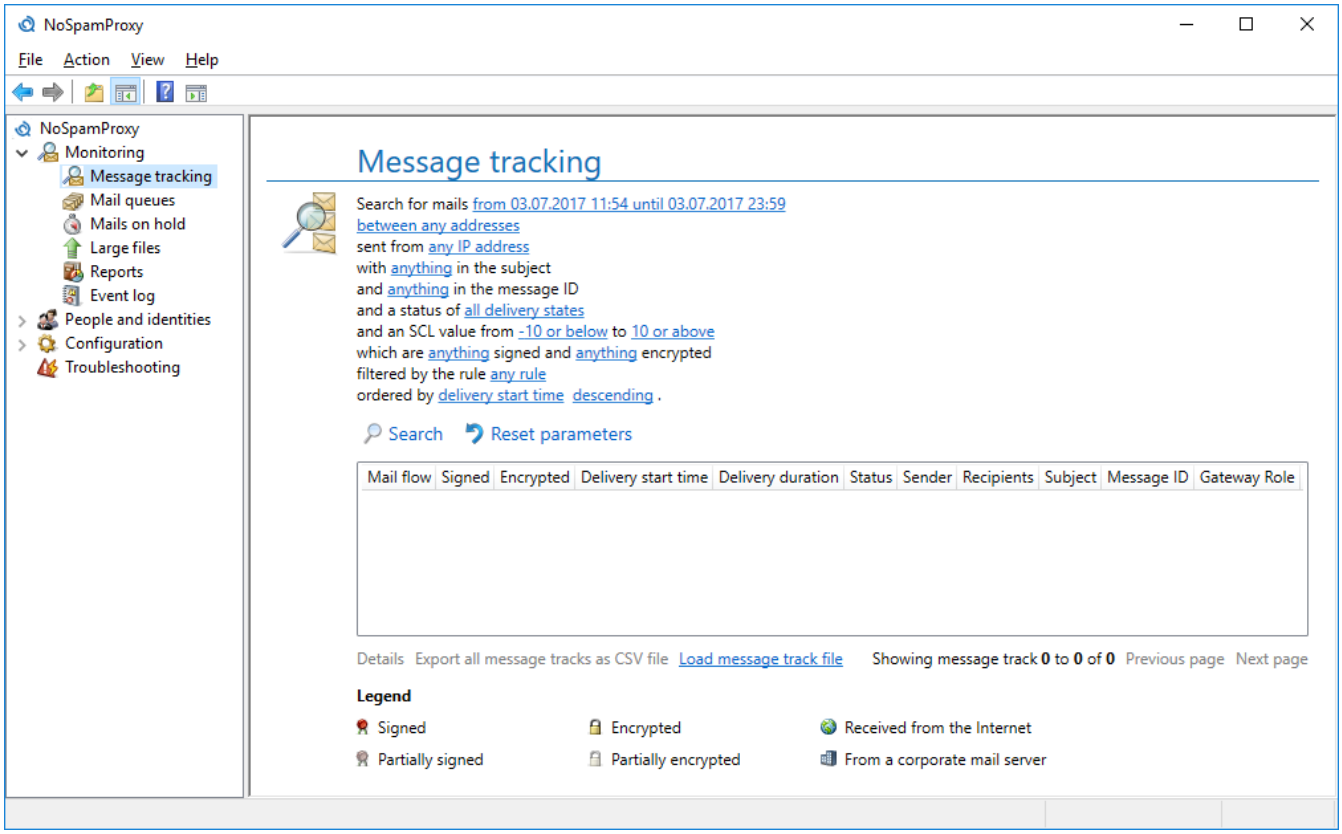


Picture 16: Monitoring

Message tracking

Message tracking allows you to gain an overview of blocked and unblocked emails. (Picture 17). You can adjust the search criteria based on sender, receiver and subject as well as concrete time intervals and the status of the email.

You can also access details on the email processing and the time at which an event occurred. As a result, you can follow the actions of NoSpamProxy and the functioning of the rules .



Picture 17: Message tracking datasets

For email tracking, various search criteria are available which can be used individually or combined. In either case, a time frame must be set. By default, the start time is set to the current system time - 1 hour and the end time to the respective day at 11:59 pm.

You can apply filters based on the characteristics listed below. When entering a text, you can always enter the entire text to be searched for or just parts of it.

- Time period of dispatch: Via the option **time frames** frequently-used search items can be selected quickly.
- Sender and receiver address: The email addresses of the communication partners. You can filter these addresses based on local and external addresses. The search type can be 'exact match' for complete addresses or 'contains' for address fragments. The search for exact matches will yield results much quicker.
- Subject: The content of the subject line.
- Message ID: Internal ID of the email.
- Delivery results: The status of delivery.
- SCL value: Restriction to the calculated SCL value.
- Rule: The name of the rule which processed the message.

All emails matching the search criteria appear in the list of the message tracking datasets. They are displayed with the indications **Direction**, **Security**, **Connection start time**, **Transfer duration**, **Status**, **Sender**, **Recipient**, **Subject**, **Message ID** and **Gateway Role**.

Emails are listed based on their delivery date in descending order.

Checking the details

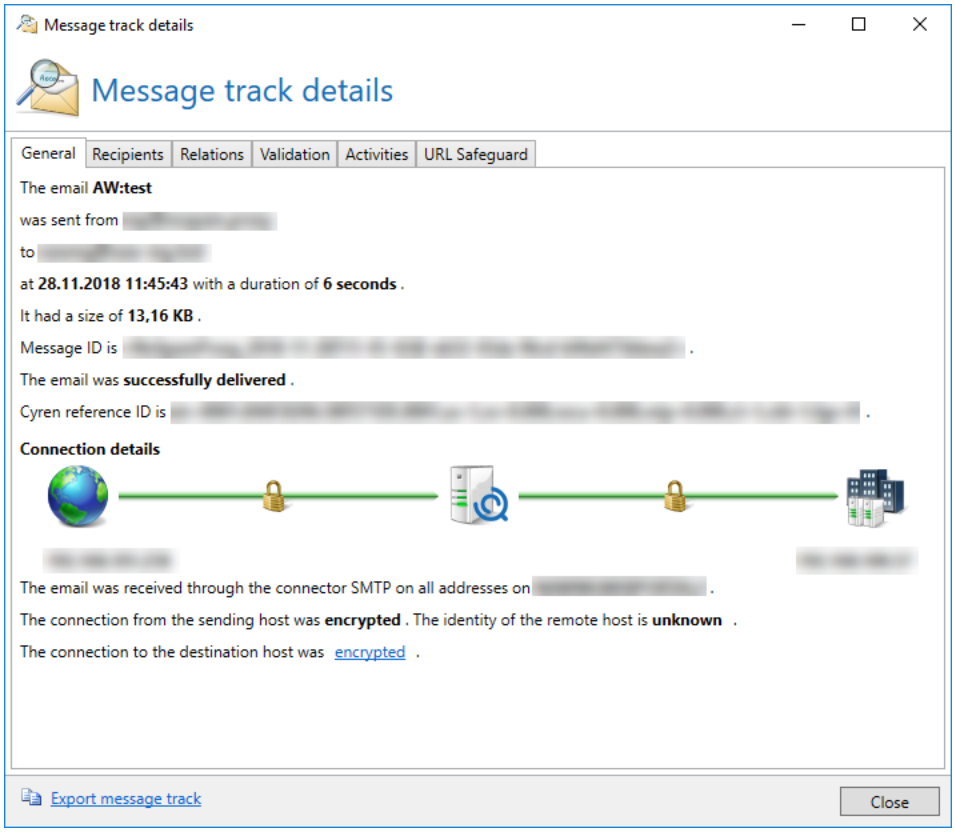
This view provides you with detailed information on the delivery status of emails. Information on signing and encryption of emails is also displayed .

Select a dataset and click **Details** to access detailed information. Alternatively, double-click the dataset.

The dialog **Message track details** appears. (Picture 18).

From the start to the end of the connection, you will find all the editing steps and details for the selected dataset here. You can see at a glance whether the connection was encrypted and which certificate the SMTP server or SMTP client used. On the remaining tabs, filter results and general processing errors are displayed, allowing you to track at any time whether the email delivery is working properly.

The **Validation** tab displays, among other things, details about the validation of the email, the calculation of the Spam Confidence Level for the Level of Trust rating, and the filters and actions applied to the email. The **URL Safeguard** tab contains information about URLs changed by the URL Safeguard.

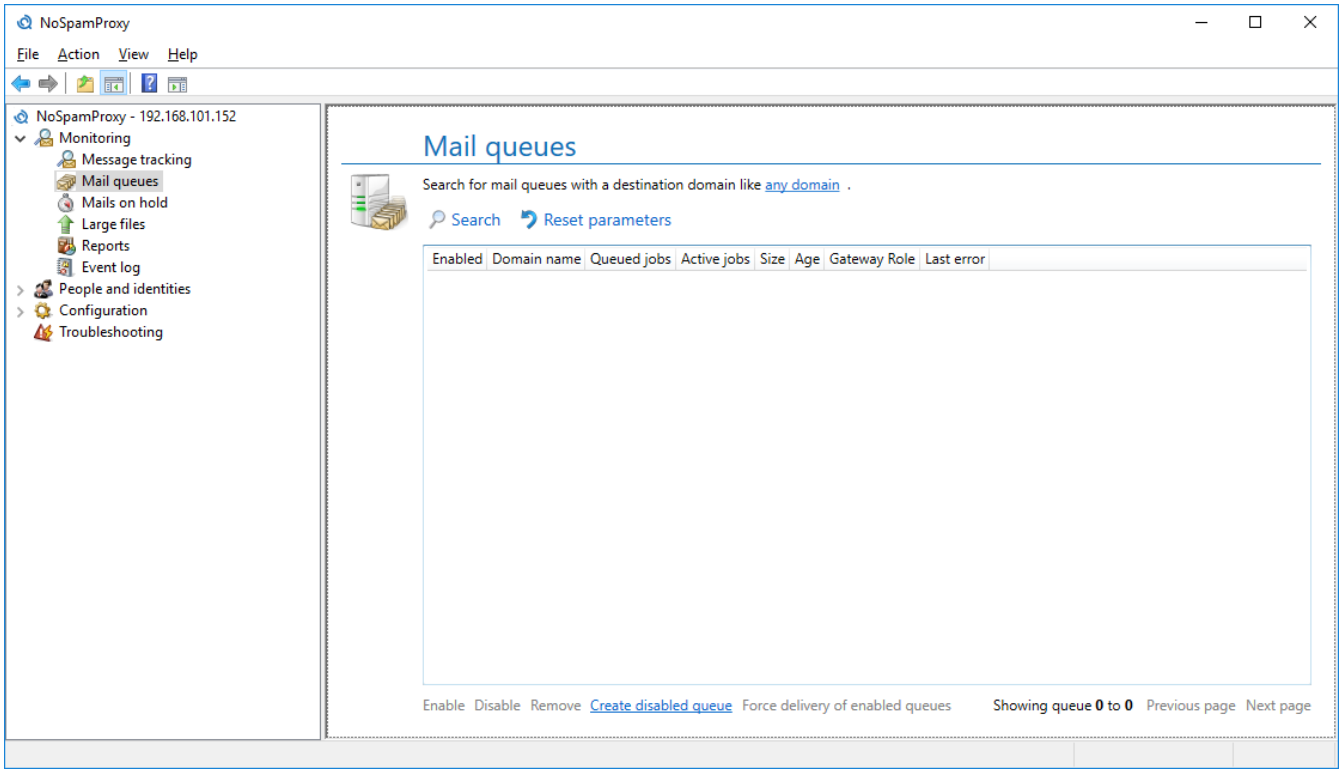


Picture 18: Email delivery results in detail

You can save the datasets shown in Message tracking on your local hard drive or access saved datasets. This function is very helpful in case you need support in analysing a specific dataset. To export datasets, click **Export message tracking** at the bottom-left corner of the dialog. In order to access the details, click **Load message tracking file** in the list of all found datasets.

Email queues

Emails to external addresses are enqueued according to their domain. There is one queue per domain. All active email queues are shown to you under the menu item **Email queues**. (Picture 19). A list of target domains for pending emails - emails that have not yet been sent - is displayed. You can also pause any email transfer to one or more specific domains.



Picture 19: All pending emails are arranged in queues according to their domain name

You can also search for specific queues. Enter the search term and click **Search**. All entries containing the search term are displayed.

The column **Active** shows whether emails are currently delivered for this domain.

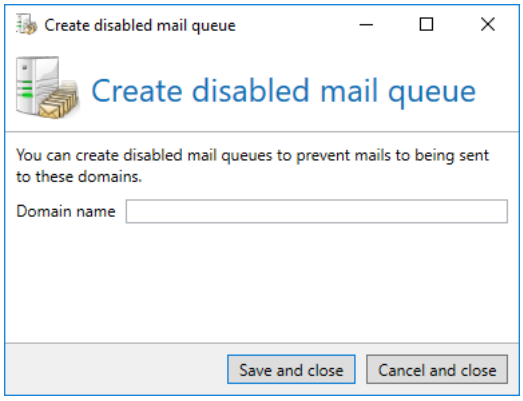
The **Domain name** corresponds to the name of the target domain.

The **Queue length** corresponds to the number of pending emails.

The column **Active connections** shows currently open SMTP connections to the target domain. This is particularly useful in cases where a large number of emails are sent to the same domain.

Via the action **Activate selected queues** and **Deactivate selected queues**, you can start or pause email delivery to the respective domains.

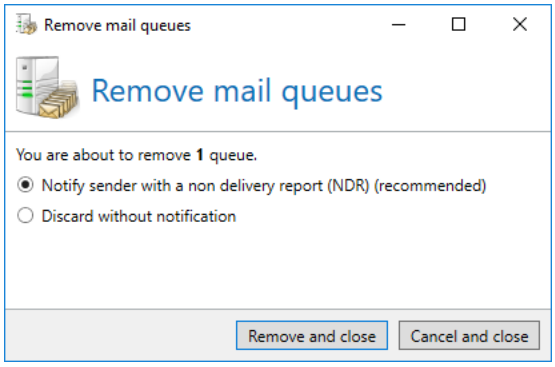
You can also create inactive queues to disable connections to specific domains proactively. To do so, select **Create deactivated queue**. The dialog (Picture 20) opens.



Picture 20: Domains to which no emails should be sent can be created as "deactivated queues"

State the domain name (e.g. "netatwork.de") beneath **Domain name for queue** and save the setting afterwards to create the deactivated queue. Afterwards, all emails to "netatwork.de" in the queues of NoSpamProxy are paused until you reactivate the queue.

A queue can also be deleted. During the deletion, you can decide whether a non delivery report (NDR) is sent or not.



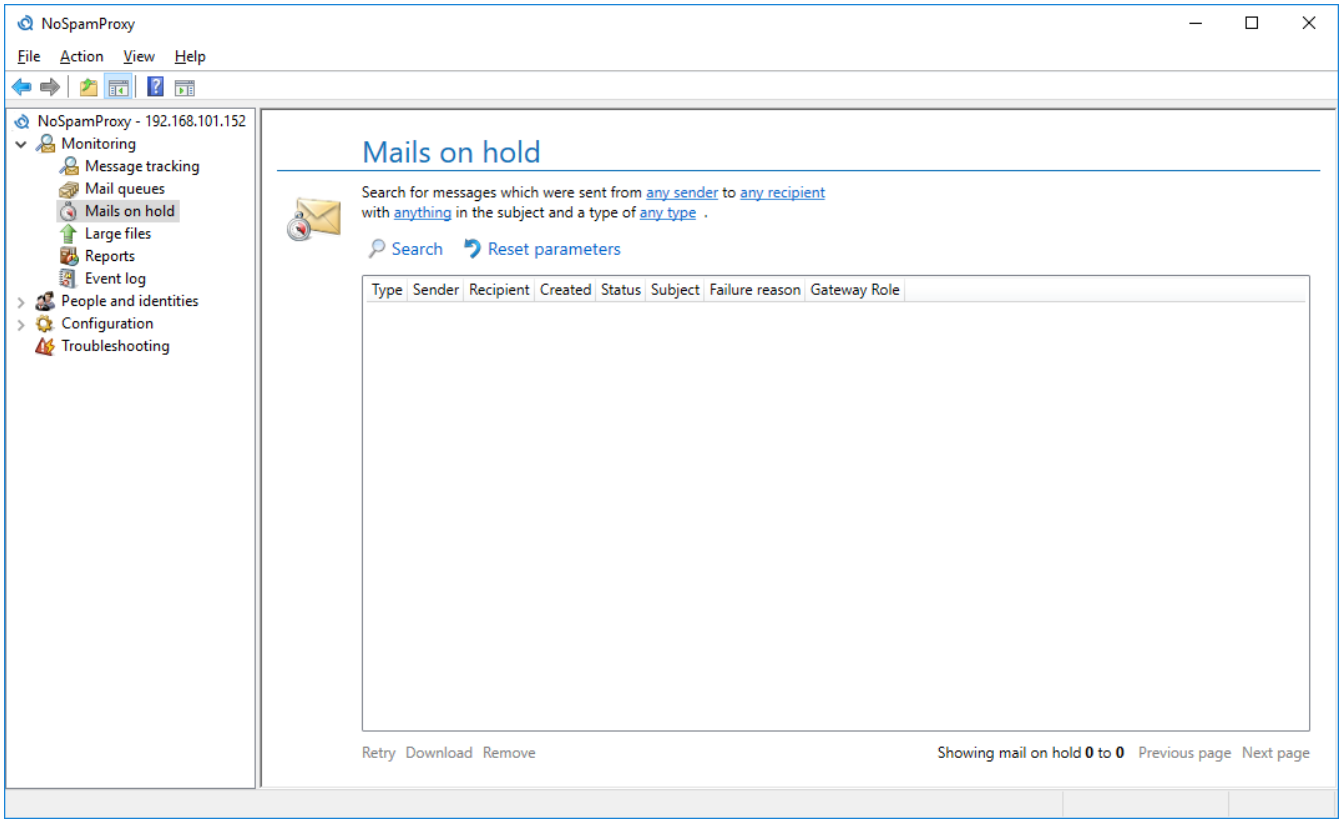
Picture 21: Deleting queues

Mails on hold

If you use NoSpamProxy Protection without NoSpamProxy Encryption, the node is only displayed if Large Files is also licenced.

Under certain conditions, emails can also be put on hold. This means that emails are neither delivered nor rejected until certain conditions are met. Mails on hold are caused by missing encryption keys,

incidents due to file attachments and issues concerning qualified signatures or De-Mails. These emails are listed under 'Mails on hold' (Picture 22).



Picture 22: All list of mails on hold

You can search for and filter emails on hold based on direction, sender and recipient address, subject line and email status. Concerning addresses and the subject lines, the search term only needs to be entered partially; results for all addresses and subject lines containing the search term are displayed.

If you have licenced Large Files, files affected by uploading failures are displayed in this list.

You re-initiate the processing of selected emails by clicking on **Try again**. In case issues persist, the affected emails are re-entered into the list.

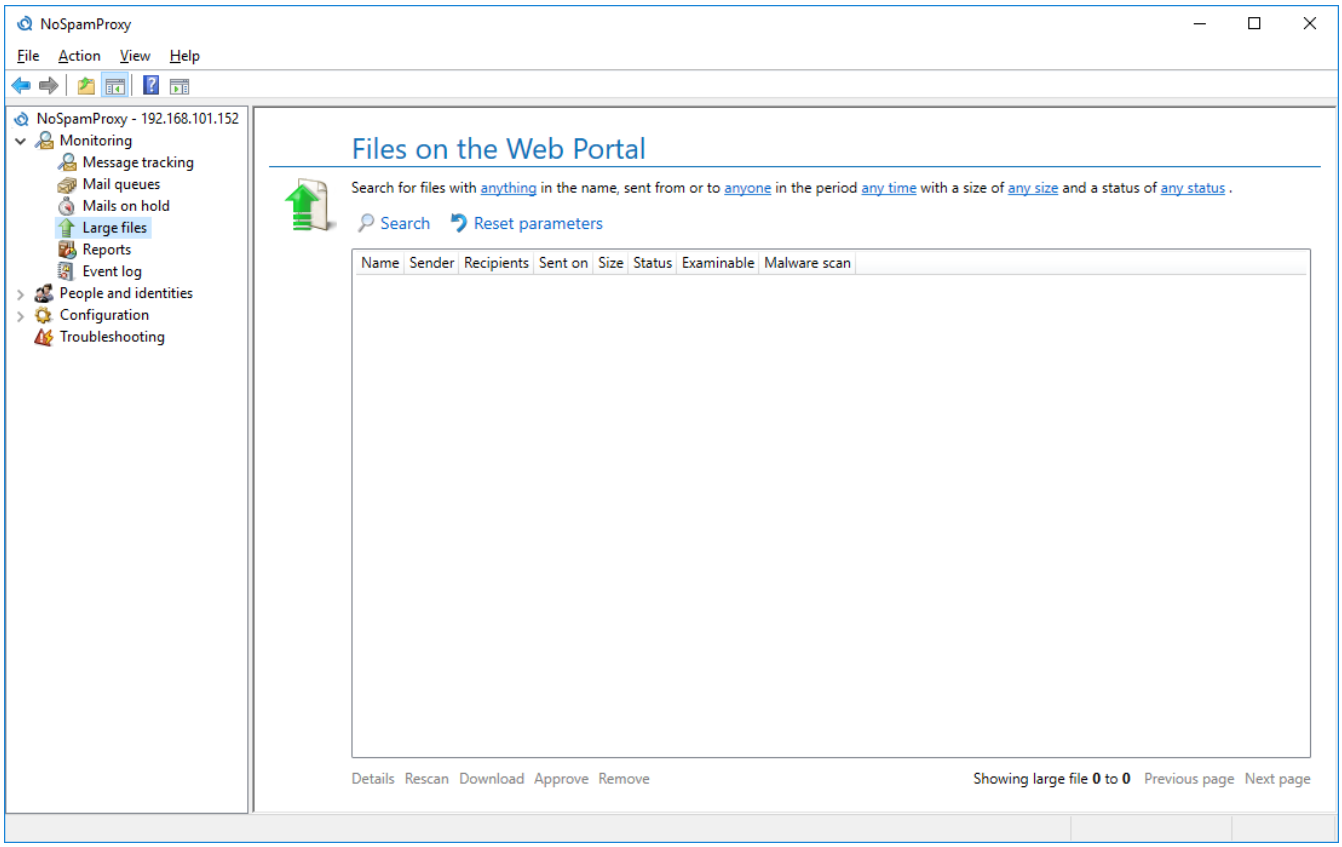
You can download and save the entire email including all corresponding documents to the workstation which runs the user client. To do so, select an incident and choose **Download**.

Moreover, you can delete emails on hold. You can choose here whether the sender is notified or not.

Large Files

The node is available if Large Files is licenced.

The section **Files on the Web Portal** (Picture 23) shows all files which are currently saved on the Web Portal. You can delete files which are no longer required here. Files which require clearance by an administrator can be cleared for download. Files marked as **Examinable** which have not yet been cleared can be downloaded by the administrator to facilitate a content check. Examinable files can be scanned for malware via **Check again**. If malware is found, the file is deleted and the recipient is informed about the result. The column **Malware check** shows the date and time of the last check.



Picture 23: Files on the Web Portal

You can filter the search based on the following properties:

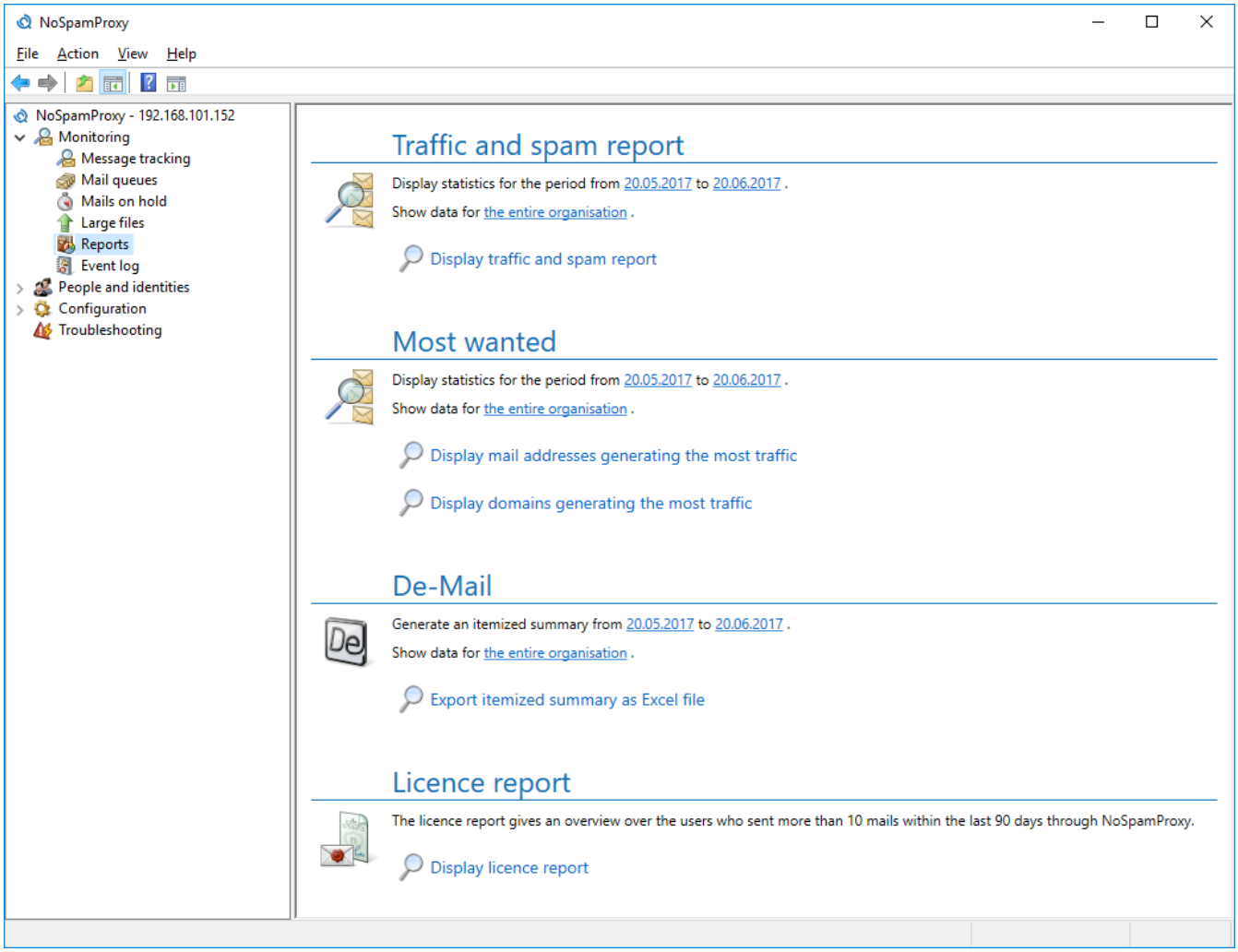
- **File name**
  Provide the file name or parts of it.

- **Sender or receiver address**
  Provide an email address or parts of it. The overview shows only the the recipient address while all addresses are include in the search.
- **Dispatch period**
  The time period can be restricted. If you do not want to apply a restriction, deactivate the check box in front of **From** and **Until**. Via the option **Timeframes** frequently-used search terms can be selected quickly.
- **File size**
  Restrict the file size with the sliders. Deactivate the restriction using the check boxes in front of the sliders.
- **Status**
  Select either all files or files with certain properties, such as never or partially downloaded or downloaded by all recipients. You can also search for files which have not yet been approved or files whose malware scan produced errors.

The link **Details** displays additional recipients of the selected file as well as details on errors which may have occurred during the malware scan.

Reports

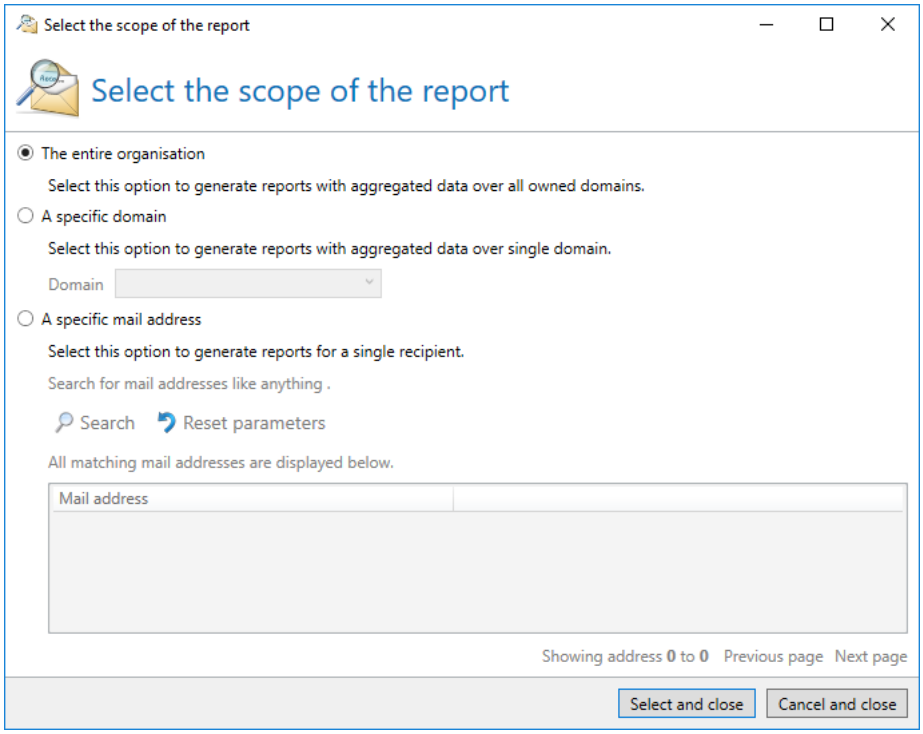
The reports of NoSpamProxy provide you with a history of your email correspondence (Picture 24). With a few clicks, you can see how spam volume has developed over time. You can also determine email addresses or domains with high spam output.



Picture 24: Evaluation of message tracking data

Data traffic and spam report

The paragraph "Data traffic and spam report" lets you create a report on the email correspondence history. The report not only shows the history of the number of emails but also the history of the data volume. To create the report, select the time period to be covered by the report. Now determine the scope of the reports. To do so, click on the link for the entire organisation.



Picture 25: The scope of the data traffic and spam reports

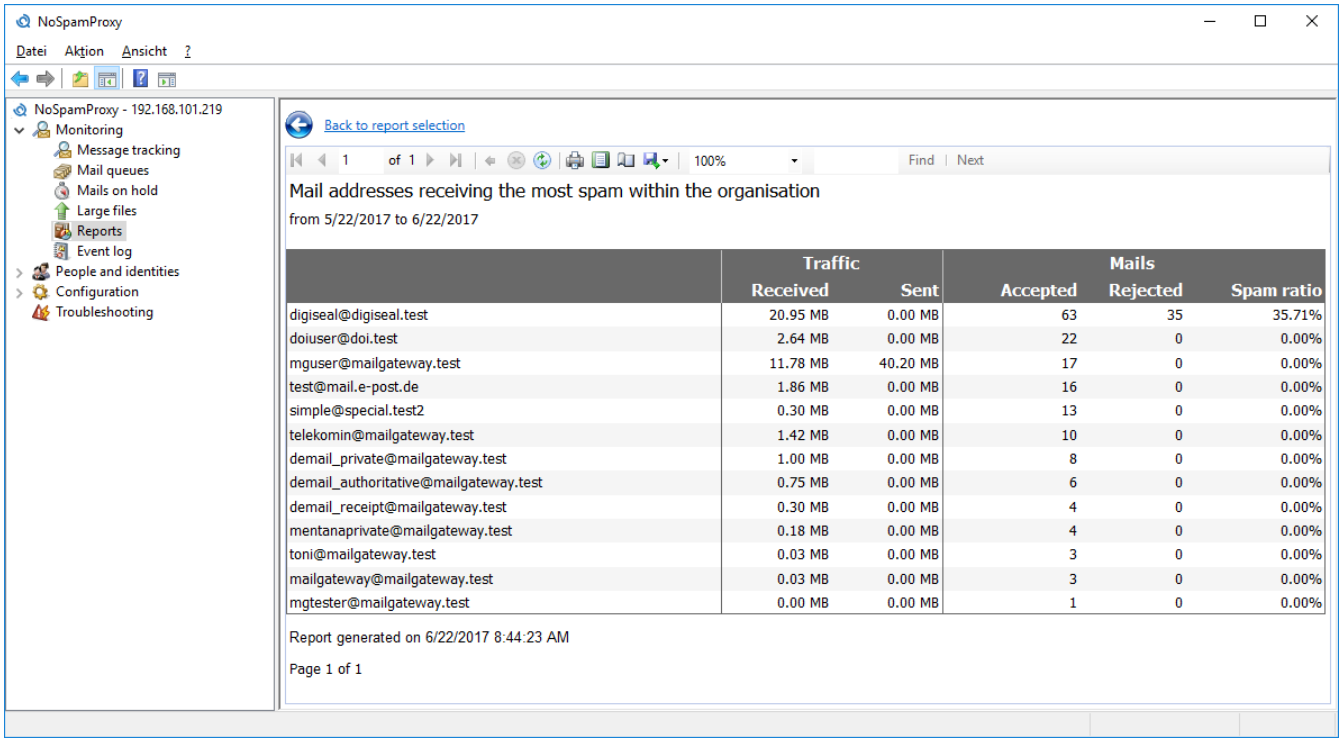
A dialog (Picture 25), lets you determine whether you want to create the report for the entire organisation, for a specific domain or for a specific email address.

You can only select domains and email addresses which have already received emails and thus appear in the message tracking database. No access to the configuration of the Gateway Role is effected.

Click on **Select and save**, to save the settings. Then click on **Show report**, to create the report.

Most wanted

In the section **Most wanted**, NoSpamProxy offers you four reports which, for example, contain the email addresses or domains with the highest spam ratio. Furthermore, there are reports showing you which email addresses or domains produced the highest amount of data (Picture 26) Just like in section **Data traffic & Spam report**, you can determine the time period and the scope covered by the respective report.



Picture 26: The addresses with the highest spam ratio

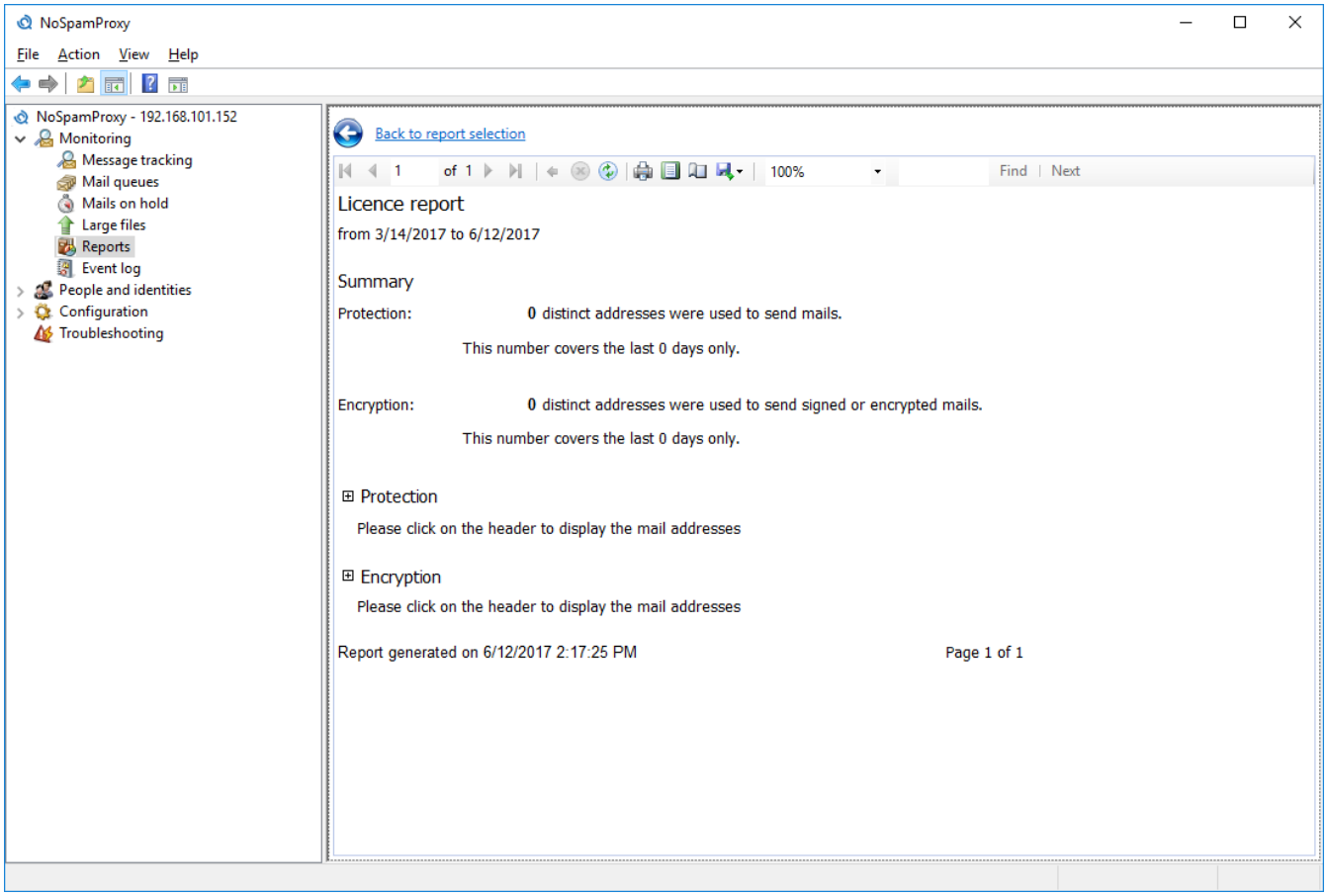
The available reports are the following:

- Show email addresses which receive the largest amount of spam.
- Show email addresses which create the largest volume of data.
- Show the domains which receive the largest amount of spam.
- Show the domains which create the largest volume of data.

You can decide whether you want to create the report for the entire organisation, for a specific domain or for a specific email address. Subsequently, click on the desired report to generate it.

Licence report

The licence report lets you adjust the number of licenced users of the individual features to the number of licences required (Picture 27).



Picture 27: The report of the used licences

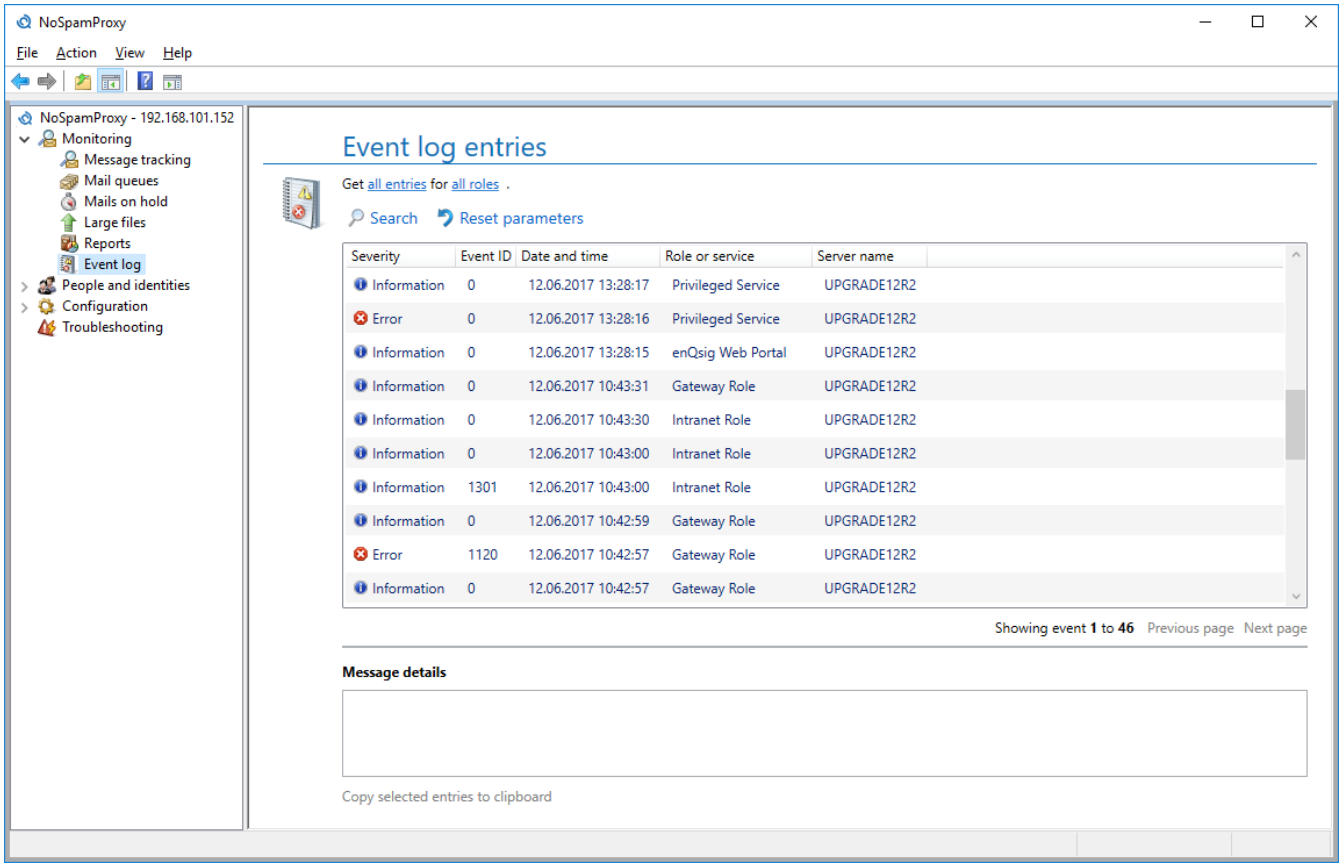
The licence report totalises all users who have received more than 10 emails during the last 90 days.

The user numbers included in this report let you continually adjust the number of NoSpamProxy licences to a growing number of user in your company.

If you have questions, please do not hesitate to contact our team at info@netatwork.de.

Event view

The server events relevant for NoSpamProxy are available in the client under "Event view" (Picture 28).



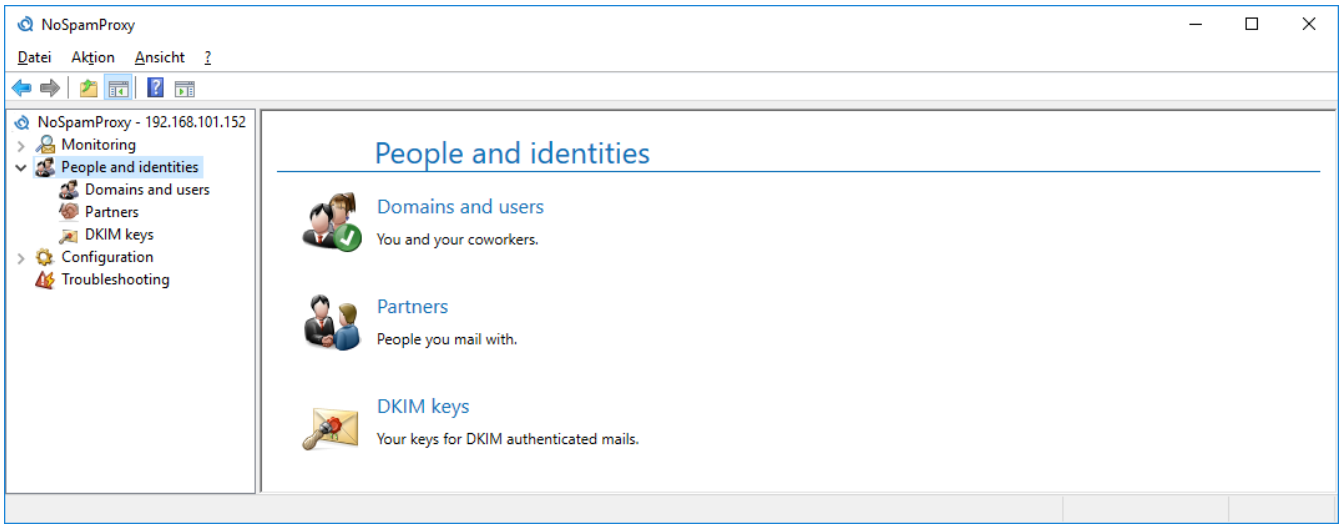
Picture 28: The event view shows the events for all NoSpamProxy roles.

You can filter the entries shown here according to roles or services. You can also restrict the type of the displayed events. The selectable categories are **Errors**, **Information** and **Warnings**. To view older entries, you can browse through the search results by using the functions **Back** and **Next**.

Select an entry to view its details. The details are displayed at the bottom of the page.

9. People and identities

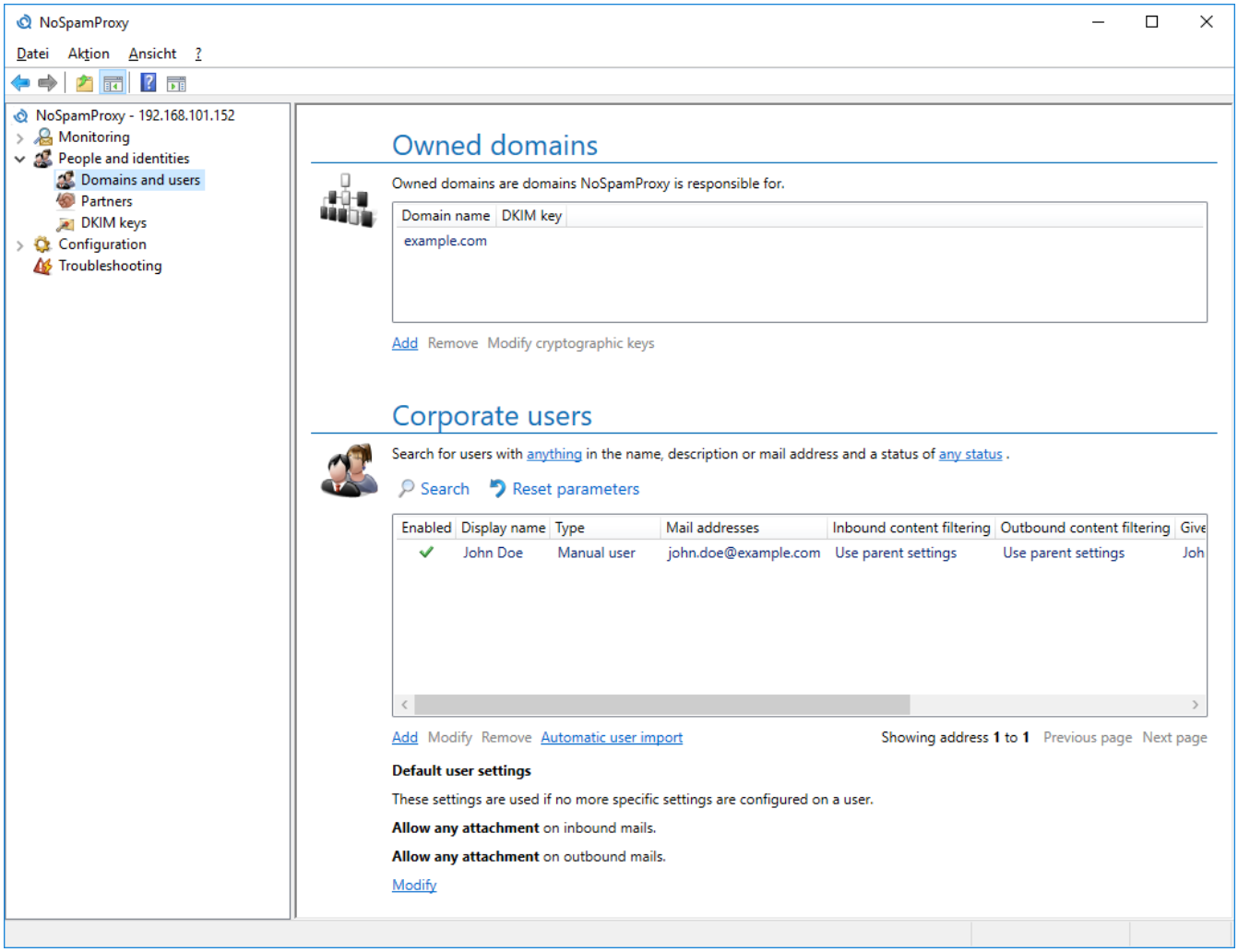
People and identities contains all external and internal companies and persons as well as their email addresses (Picture 29).



Picture 29: The areas beneath People and identities

Domains and users

Under **Domains and users**, you can maintain your owned domains and a list with valid email recipients and the corresponding addresses (Picture 30). This list is used if you filter the rules by "Local addresses" instead of "Owned domains". Additionally, you can configure the automatic import of user data here.



Picture 30: The list of the owned domains and the corporate users

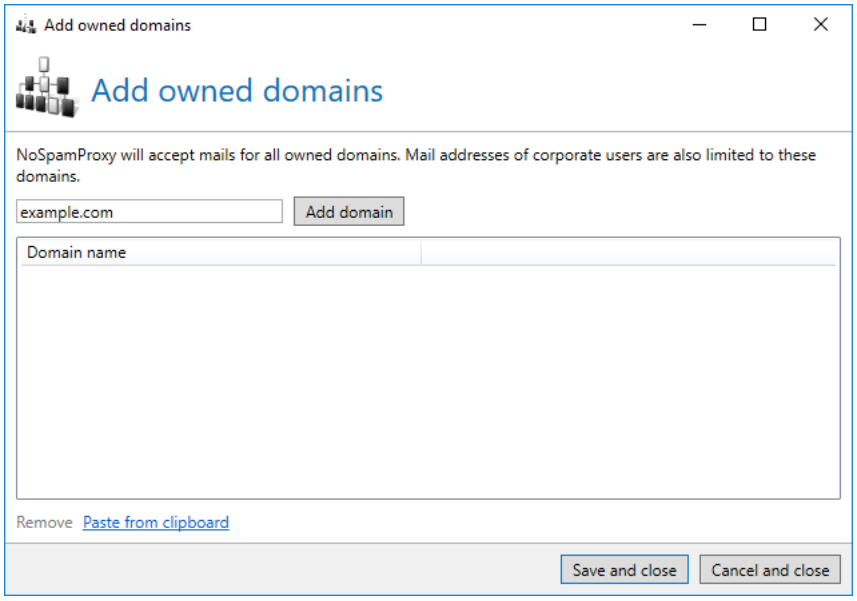
Owned domains

Enter all domains for which you wish to receive emails into the list of owned domains. You can also use this list in the rules. Otherwise, NoSpamProxy classifies these connections as relay misuse and rejects emails.

All owned domains must be entered. Otherwise, local emails cannot be identified as such and will be rejected due to suspected relay misuse.

Add owned domains

The action **Add** opens the entry dialog (Picture 31).



Picture 31: Dialog for new owned domains

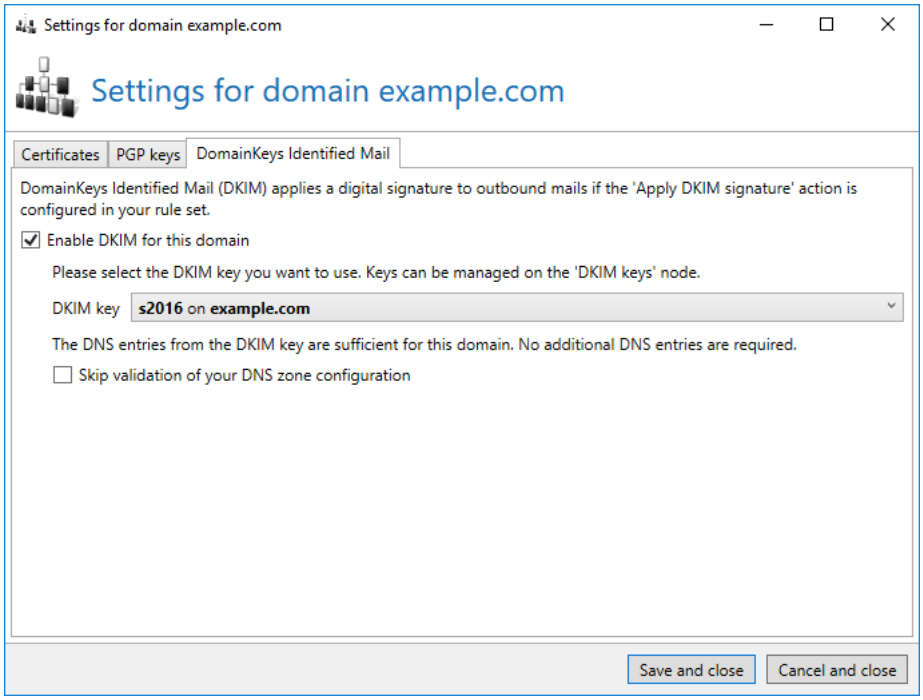
Enter all your owned domains here.

When deleting owned domains, all email addresses of this domain are deleted from the corporate users as well. If the user does not own any email addresses afterwards, it is deleted as well.

DomainKeys Identified Mail

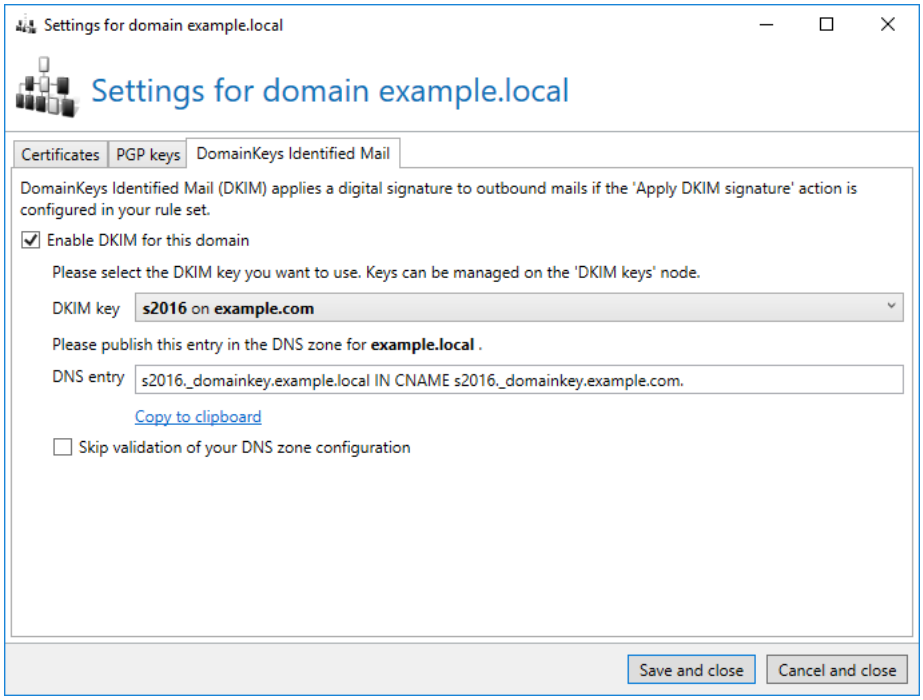
DomainKeys Identified Mail (DKIM) secures outbound emails by equipping them with a digital signature. This signature lets the recipient determine whether the email was sent from the correct domain (ensuring its authenticity) and whether it was changed during the transport (ensuring its integrity). DKIM-signed emails can also be read by recipients who cannot evaluate the DKIM signature. To those recipients, DKIM-signed emails appear similar to non-DKIM emails.

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



Picture 32: Selecting a DKIM key for the current owned domain

On the tab **DomainKeys Identified Mail**, the keys created can be mapped to the domain (Picture 32). To do so, activate DKIM for the domain and select one of the keys created from the list of the **DKIM keys**. If the domain of the DKIM key is identical to the domain being configured, the DNS entry which you published during the creation of the key suffices. If the domains differ from each other, the configuration page shows another necessary DNS entry (Picture 33). If you need to publish additional DNS entries, NoSpamProxy prepares the required entry; you can then copy it to the clipboard and publish it to the DNS zone. Afterwards, the DKIM configuration for this domain must be interrupted temporarily. You only need to interrupt the configuration if DNS entries are missing. Otherwise, you can proceed with the configuration without interruption.



Picture 33: Selecting a DKIM key of another domain

If all necessary DNS entries have been published and are known throughout the internet, restart the selection of the DKIM key. Select the key for which you published the DNS entries. During saving, the DNS configuration is checked. If validation fails, discrepancies are shown.

After successful validation you have to map this DKIM key to one of your owned domains to use it.

When publishing DNS entries it may take some time until all DNS servers on the Internet receive these changes. Please wait at least 24 hours before you check and apply the entries. If you activate DKIM and your DNS configuration is incorrect, emails to recipients who evaluate DKIM signatures can no longer be delivered.

The DKIM signature requires the action **Apply DKIM signature**. This enables you to deploy DKIM for one part of your emails and suppress DKIM for another part.

Corporate users

As with owned domains, NoSpamProxy can check the individual recipients and directly reject emails to non-existent recipients. For doing so, it is required that the gateway knows all internal recipients. If you use an Active Directory, you can import the corporate users in a simple way.

The list of the **Corporate users** is used if you filter the rules by **Corporate email addresses** instead of **Owned domains**.

In order for NoSpamProxy to use the **Corporate users** list, in the respective Rules for email correspondence on the tab **Recipient** the radio button for the **Recipient type** must be set from **Owned domains** to **Corporate users**. Only then will the gateway use the list of corporate users for the determination of valid email addresses.

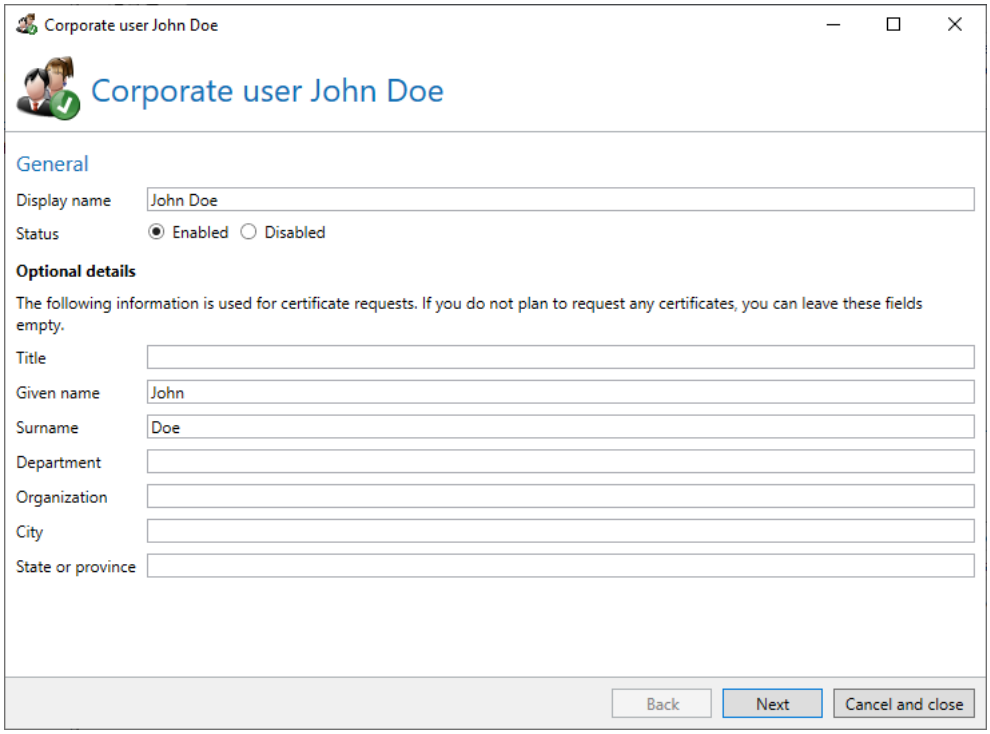
The list of the corporate users can contain two different **Types** of users:

- **Manually entered user**
  You can manage all features in NoSpamProxy in manually entered users. These users can be changed and deleted at discretion.
- **Replicated user**
  Replicated users are imported from a directory service such as Active Directory. The features of the user must be changed in the original source since NoSpamProxy only makes a read only view of most of the features for available for replicated users. All changes are applied during the new run of the User imports. In replicated users, you can not only change the activity status of the entire user but also the activity status of individual email addresses.

Search for users by searching for words or parts of words in names, descriptions or email addresses. You can also differentiate between activated and deactivated users during the search.

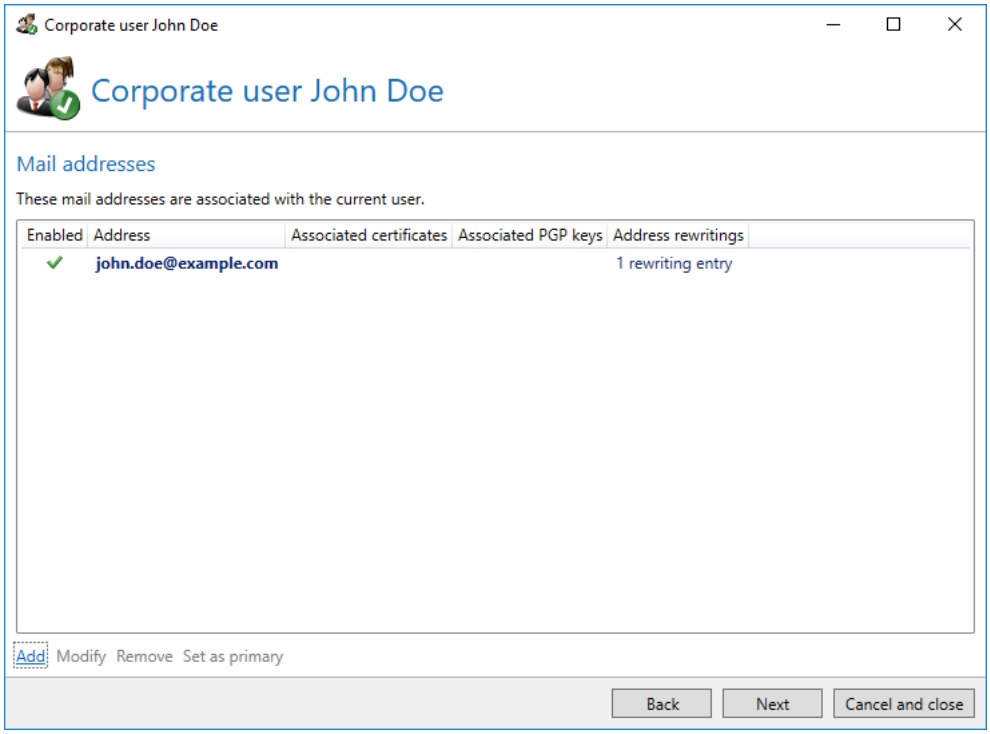
Add user

A wizard supports you in adding new users. Enter the name (Picture 34) first. The optional details are required only for certificate requests.



Picture 34: The name and additional user data

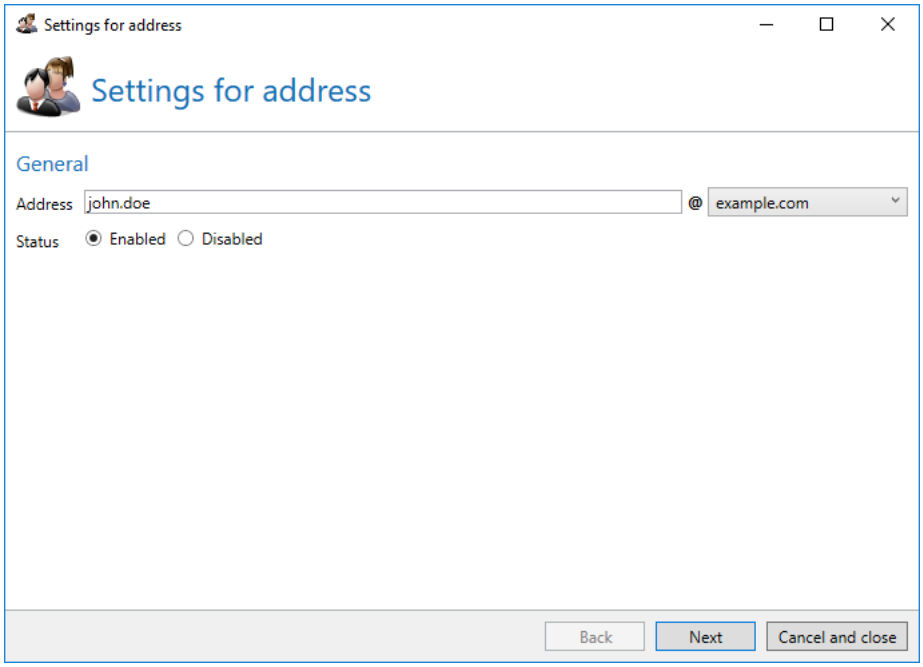
In the next step, all email addresses of the user are entered (Picture 35).



Picture 35: All email addresses assigned to the user

Enter the local part of the email address and select the domain from the drop down list of your already entered owned domains. Via the **Status**, the address can also be deactivated (Picture 36).

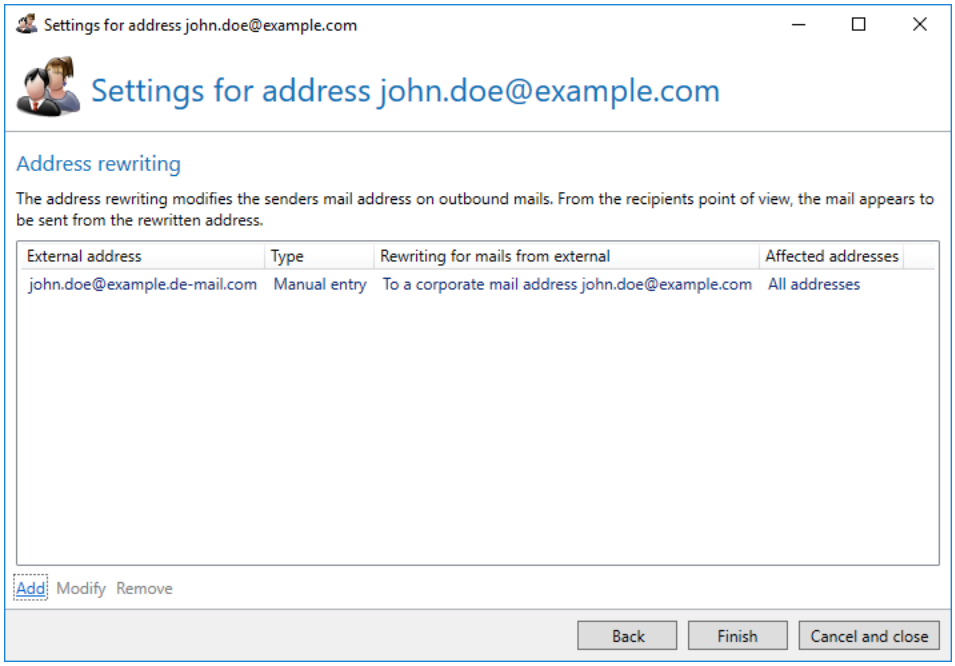
The first entered address is marked as the primary one. You can change this in the list of the email addresses via the action **Set as primary address**. The primary address is used for other functions such as De-Mail.



Picture 36: Entering a new email address

If you own a licence for NoSpamProxy Large Files or NoSpamProxy Protection, you can now select a content filter. If no specific content filters should be assigned to the user, you can also use the Default settings for users. The content filters are defined under Content filter.

The last step (Picture 37) determines all Address rewriting for this email address.



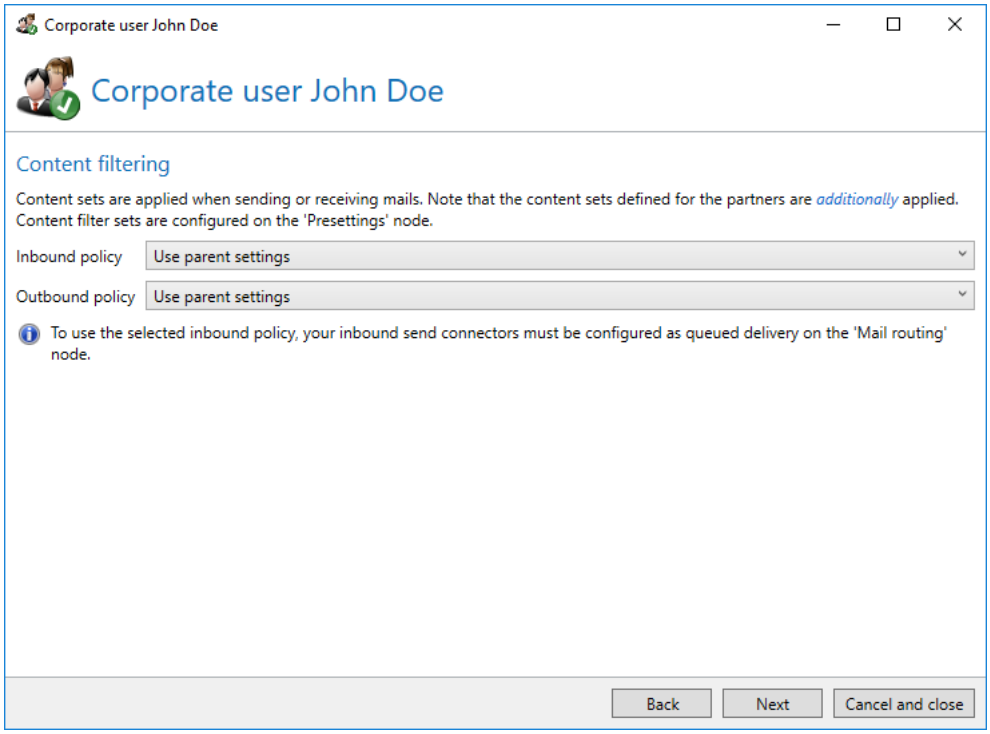
Picture 37: The list of all address rewritings

Additional user fields

Values for **Additional user fields** can be entered by the administrator.

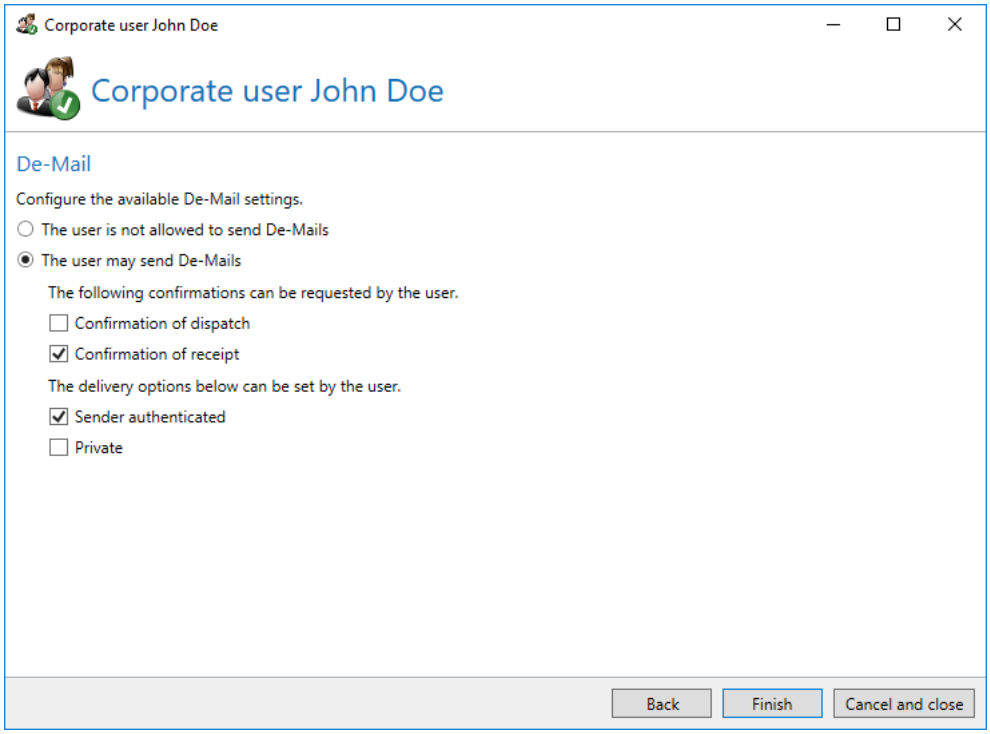
See Disclaimer for information on the configuration of **Additional user fields**.

If you own a licence for NoSpamProxy Large Files or NoSpamProxy Protection, you can select the content filters to be applied on the following page. You can either use the global settings, allow all attachments or select a configured content filter under **Presettings**.



Picture 38: Configuration of the content filters for the user

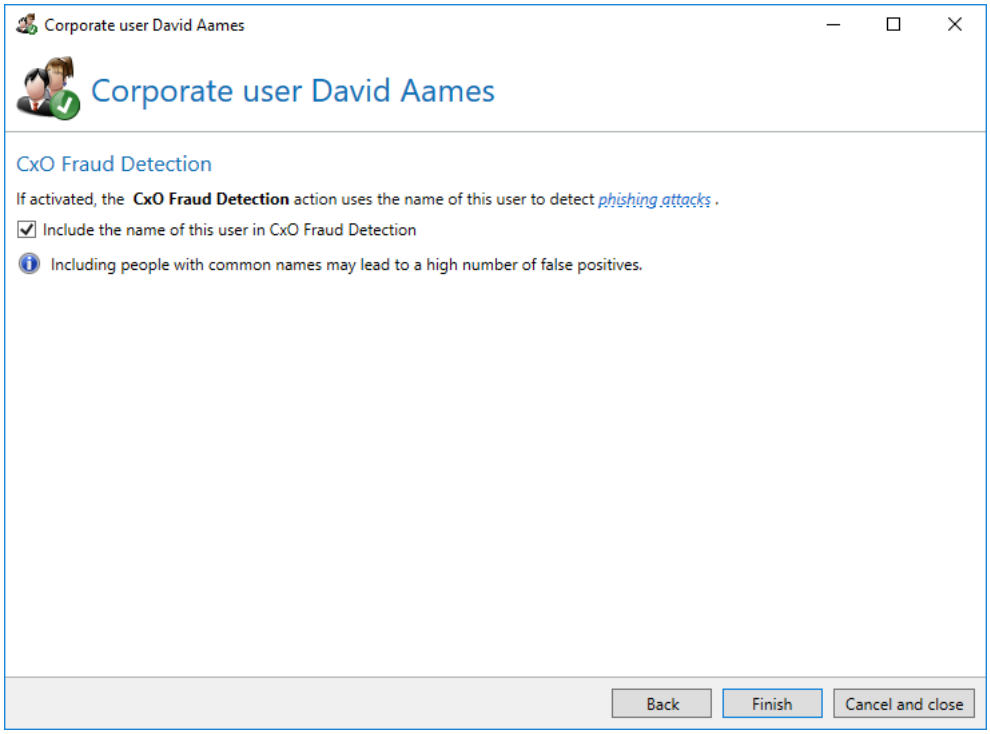
On the page **De-Mail** (Picture 39) you determine which De-Mail functions are available for this manually created user. First, set whether the user is generally permitted to send De-Mails and, if required, configure all confirmations and delivery options this user can request afterwards.



Picture 39: Available De-Mail functions for the user

CxO Fraud Detection

On the **CxO Fraud Detection** page, specify whether this user's name will be used for CxO Fraud Detection. Tick the checkbox **Include the name of this user in CxO Fraud Detection** to compare this name with the sender name of inbound emails.



Picture 40: Include this user in CxO Fraud Detection

More information about CxO Fraud Detection can be found here.

URL Safeguard

The **URL Safeguard** action prevents access to harmful content accessed via links. URLs contained in emails are matched against whitelist entries and, if necessary, rewritten or rewritten and blocked. Rewritten URLs point to the Web Portal, where they are checked and blocked or allowed depending on the check result.

Blocked URLs can be unblocked by adding them to the local whitelist. The domain belonging to the blocked URL can be accessed on the Web Portal by the recipient of the email after clicking on the rewritten link. The administrator responsible can then perform the activation. A further delivery of the email by the communication partner is not necessary.

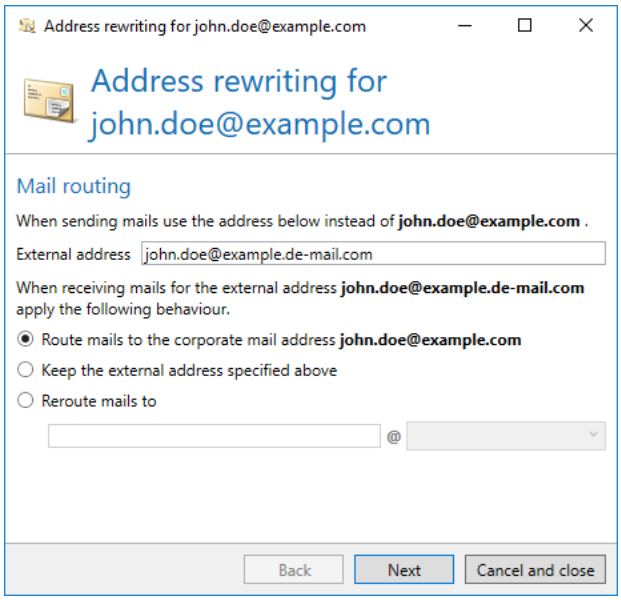
You can find further information under URL Safeguard.

New address rewriting

The address rewriting rewrites the email address of a corporate user to a different email address. As a result, a corporate user can contact an external email recipient by using an email address other than their own. The email appears to have been sent from the rewritten address. In the case of emails sent

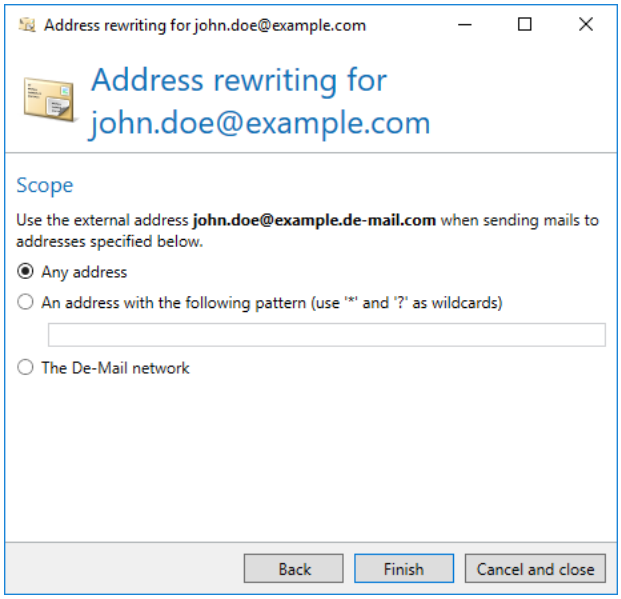
to corporate email addresses, however, the list is used to check whether the recipient is an entry from the external addresses of the address rewriting. Then, the address is sent to the corporate email address of the entry. Another use case is the so-called group mailbox. In this case, different corporate email addresses are rewritten to a single address (e.g. info@example.com).

For an address rewriting, first determine the **External address** to be used in case the email address is rewritten (Picture 41). Then, select how emails to corporate email addresses should be dealt with.



Picture 41: External and corporate email addresses

In the next step you determine the recipient addresses this applied to (Picture 42). If the recipient address does not correspond to your selection, the address rewriting is not implemented. In the selection **An address with the pattern** you can use the placeholders ('*' and '?').



Picture 42: Selected recipient addresses of this rewriting

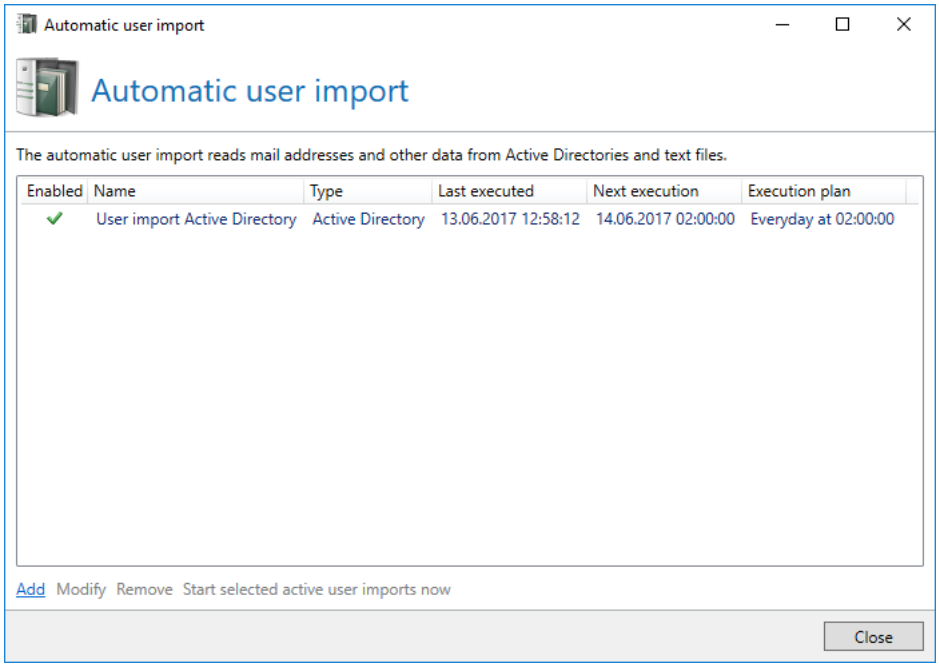
Replicated users cannot be deleted.

Default settings for users

If you own a licence for NoSpamProxy Large Files or NoSpamProxy Protection, you can select a content filter in the default settings. This filter is applied by default in case no deviating settings exist for the user. The content filters are defined under Content filter.

Automatic user import

Configure automatic user import lets you automate the import of user data. (Picture 43).



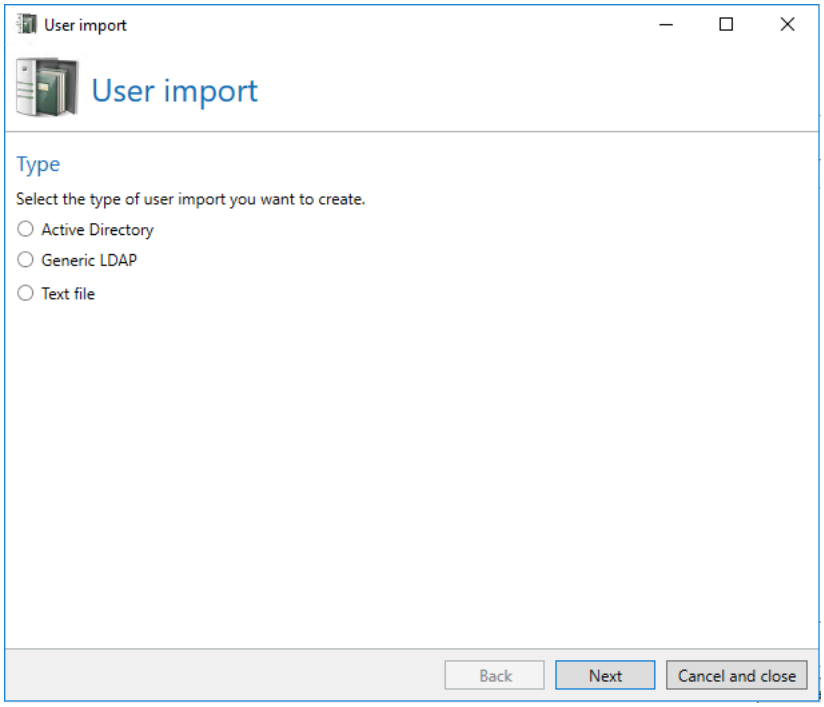
Picture 43: List of user imports set up

You can set up multiple user imports for the intranet role. This enables you to keep the corporate users in the NoSpamProxy Gateway Role up to date. For example, you can set up imports which transfer all active users from the Active Directory to corporate users. This way you ensure that only desired addresses are available from the Internet.

New user import

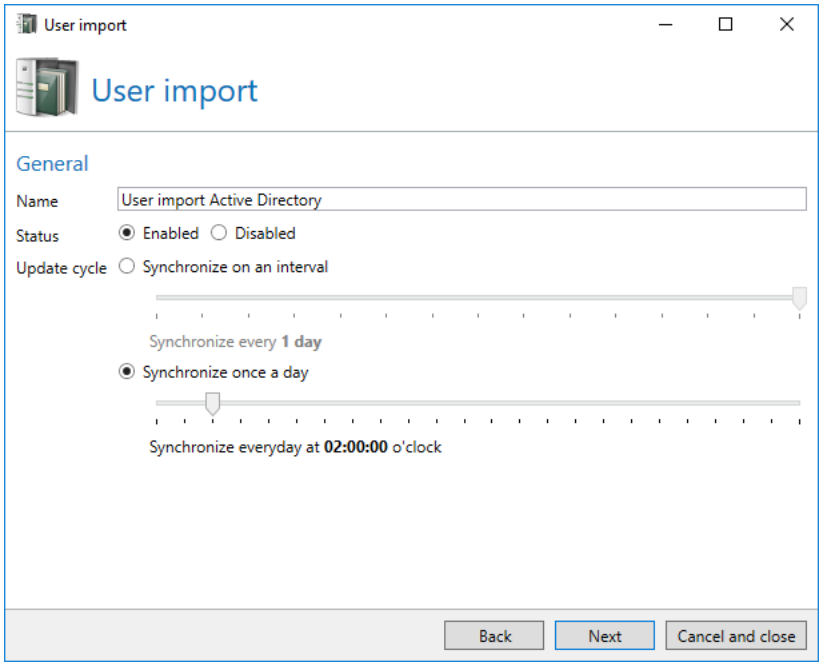
A user import determines which email addresses are imported. You can either provide an Active Directory or a text file as source. Moreover, you determine the point in time or the intervals in which imports should be executed.

The first step in creating new user imports is to determine the type. (Picture 44). An Active Directory, a generic LDAP source such as Lotus Notes, or a text file can be used as source.



Picture 44: Selecting the type of user import

Under **General** (Picture 45) you enter a unique name the user import. Under **Update interval** you schedule the user import. In addition, you can deactivate the import without deleting it using the **Status** option.

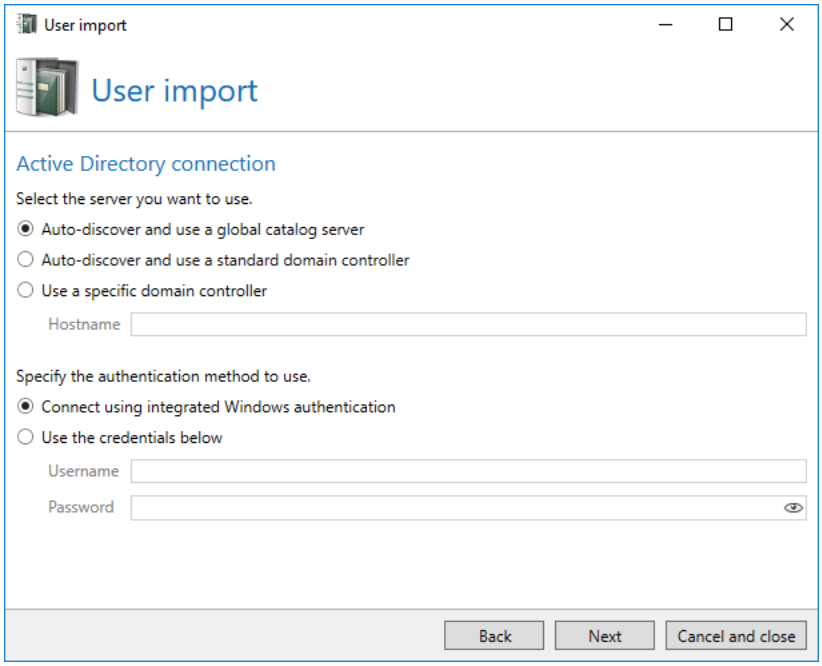


Picture 45: General settings

Depending on the type selected, please continue reading in chapter Active Directory, Generic LDAP, or Text file.

Active Directory

Under **Active Directory connection** you establish the connection to your domain controller (Picture 46). Select the server type and the user allowed to access it. If you want to enter a specific domain controller, enter an IP address or a server name. When selecting Windows authentication NoSpamProxy uses the network service if installed on a domain controller; otherwise, the workstation account is used for authentication.



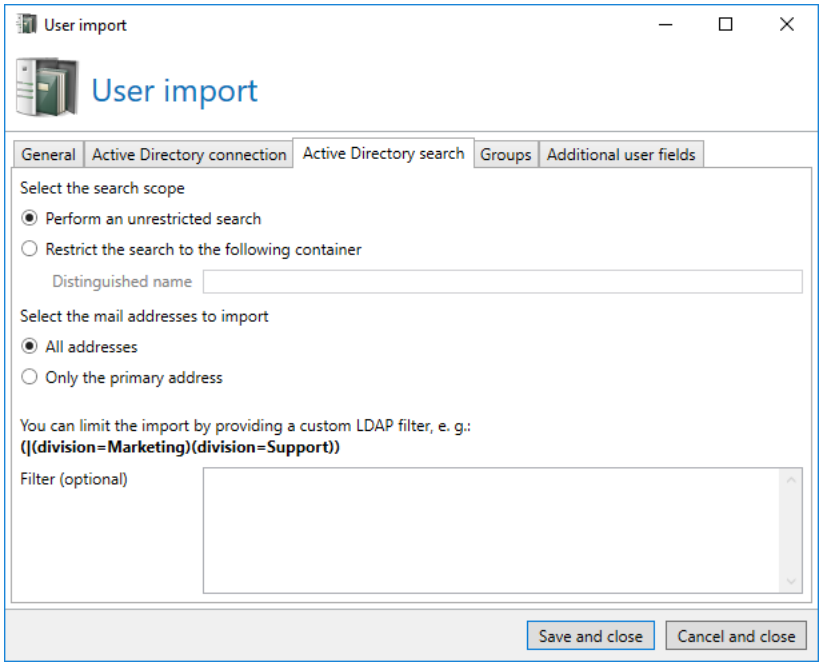
Picture 46: The directory connection

The **Active Directory search** selects the users to be imported. You can filter by certain containers, e.g.

`OU=Sales,OU=User,DC=domain,DC=DE`.

When using this example, make sure to replace "Sales", "User", "domain" and "DE" with the respective values.

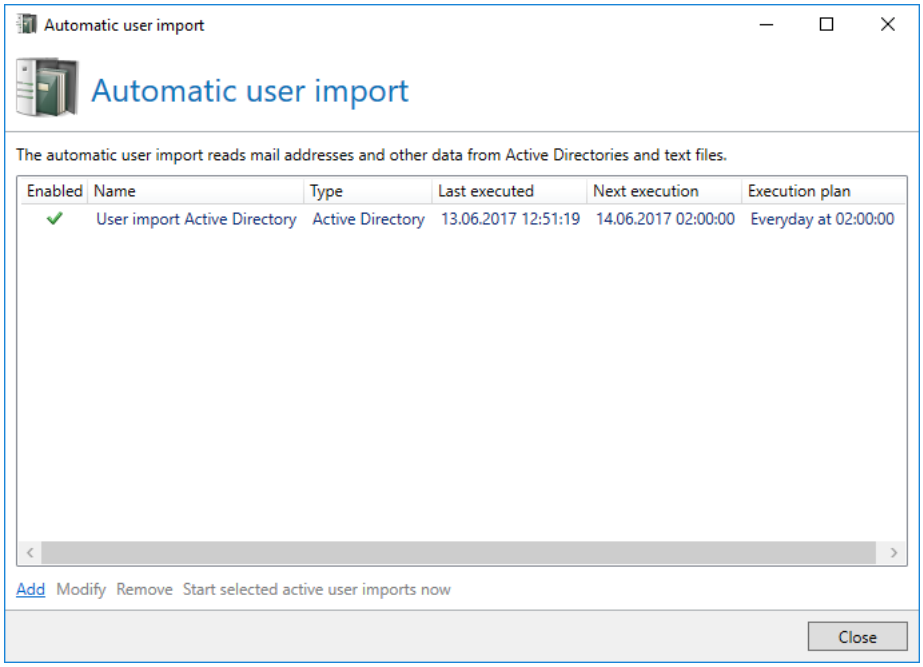
In most cases you will import all email addresses. However, you can also limit the scope of the import to include only the primary address by selecting the option available at this page.



Picture 47: Selecting the Active Directory users to be imported

You can also set an additional LDAP filter to import only users which have entered specific values for certain attributes.

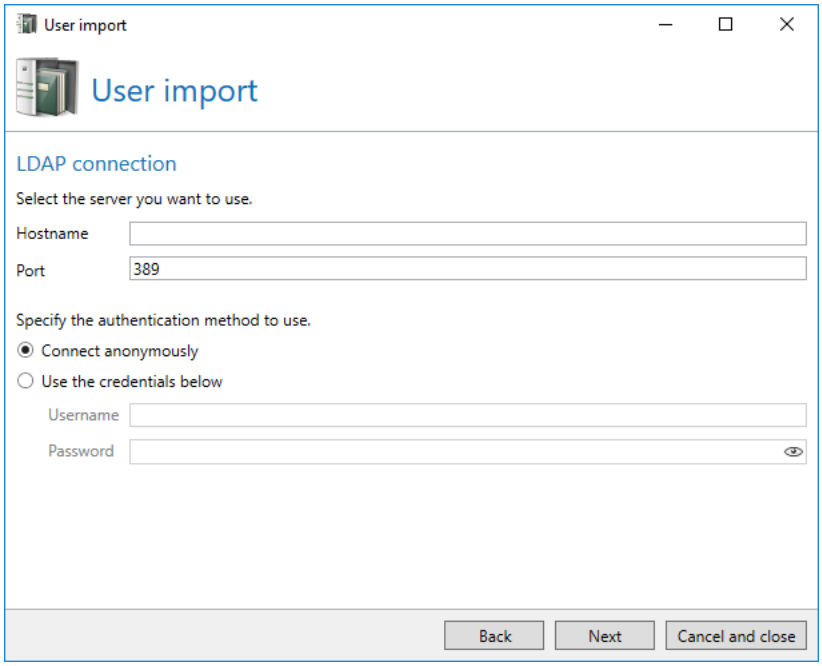
In **Groups** (Picture 48) define which functions can be used by each imported corporate user. These functions depend on the user's group membership.



Picture 48: Authorised groups for De-Mail

Generic LDAP

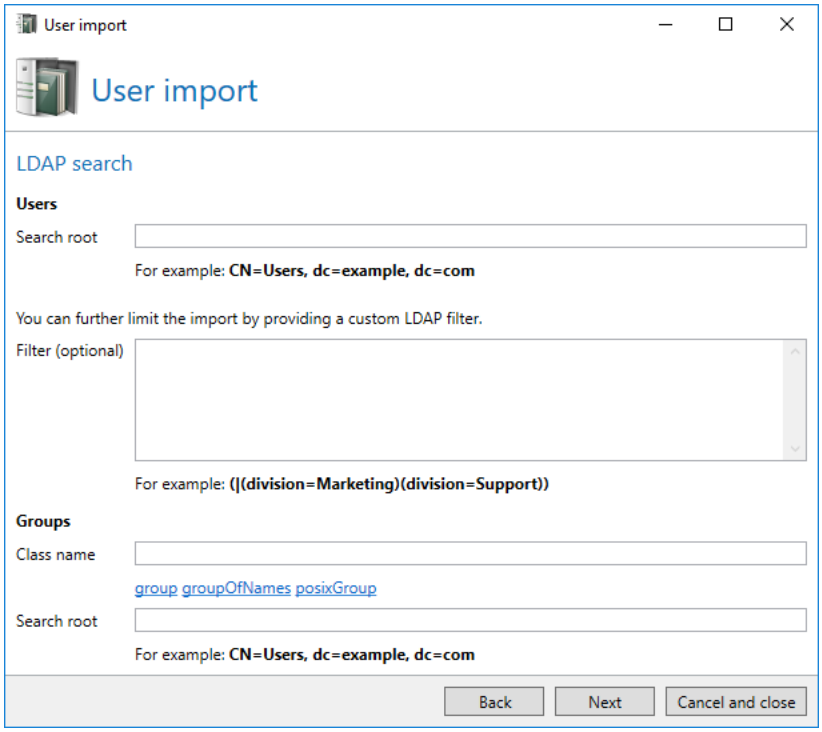
The **LDAP connection** (Picture 49) establishes the connection to your server. Enter the server and the necessary credentials.



Picture 49: LDAP connection

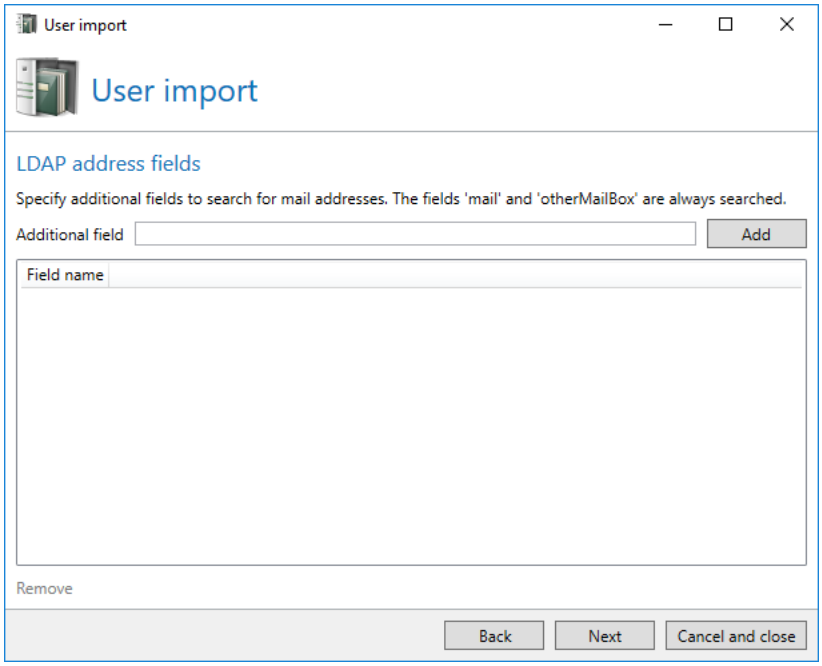
The SSL-protected LDAP variant LDAPS is currently not supported by NoSpamProxy.

In the **LDAP search** (Picture 50) you can restrict the directory search to specific containers. Please enter the search root as well as the class names under which the groups can be found. You can also restrict the search to users with specific features by using a filter.



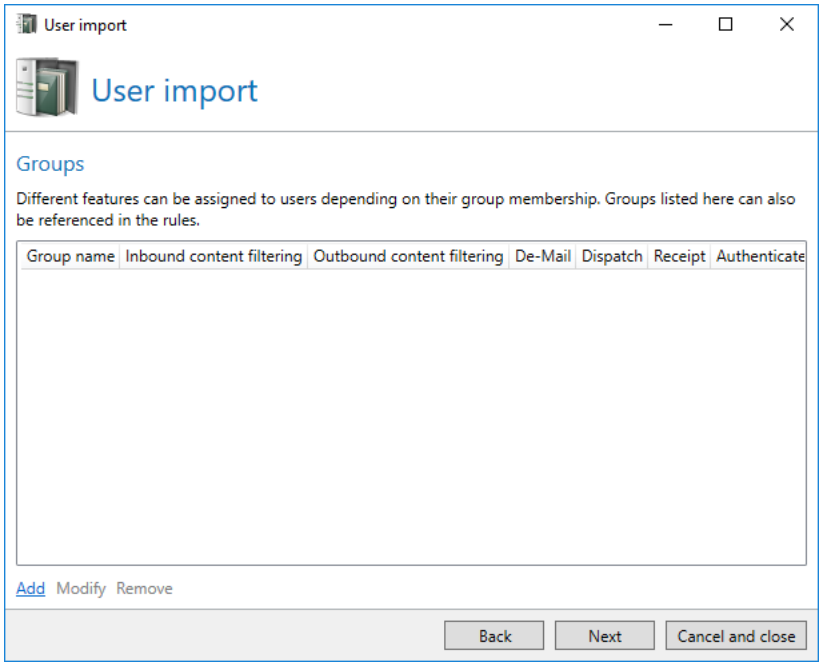
Picture 50: Customising the LDAP search

On the **LDAP address fields** page you can provide further LDAP fields to be included in the search for email addresses. (Picture 51). This is required if your system does not save email addresses in the default fields 'mail' or 'otherMailBox'.



Picture 51: Configuring additional address fields

Under **Groups** you define which functions can be used by individual imported corporate users (Picture 52). The functions depend on the user's group membership.



Picture 52: Authorised groups for De-Mail

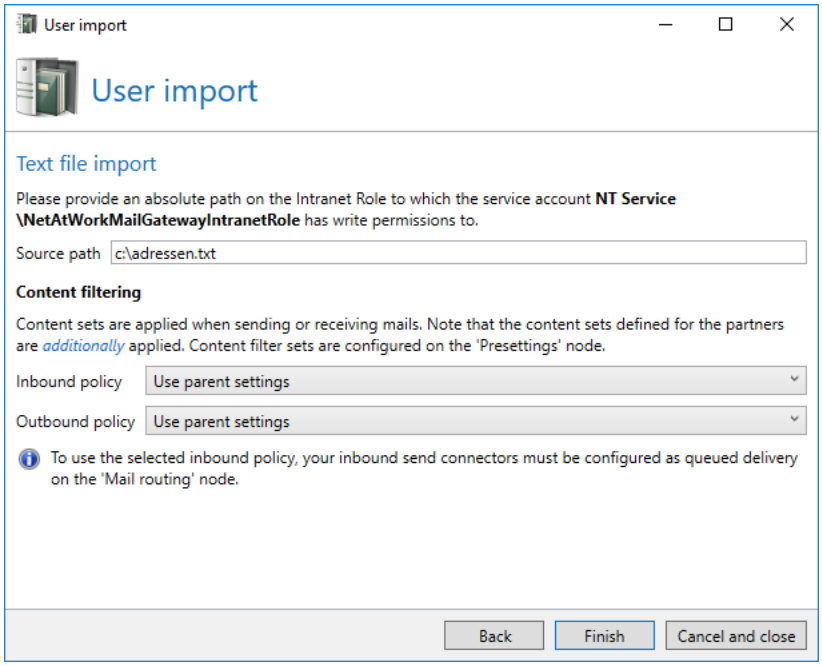
Additional user fields

The **Additional user fields** can automatically be assigned values through the user import.

See chapter Disclaimer for information on how to configure **Additional user fields** as part of automatic user import.

Text file

In the settings for user import by way of text files, enter the path to the file which contains the user addresses (Picture 53).



Picture 53: Specifying the path to the text file

The text file does not require any specific format. All email addresses are imported, irrespective of the file format.

If you own a licence for NoSpamProxy Large Files or NoSpamProxy Protection, you can select a content filter for all users to be imported. The content filters are defined under Content filter.

Email addresses are imported only if the domain is also deposited in the Owned domains of NoSpamProxy. Remaining email addresses are not imported.

Partner

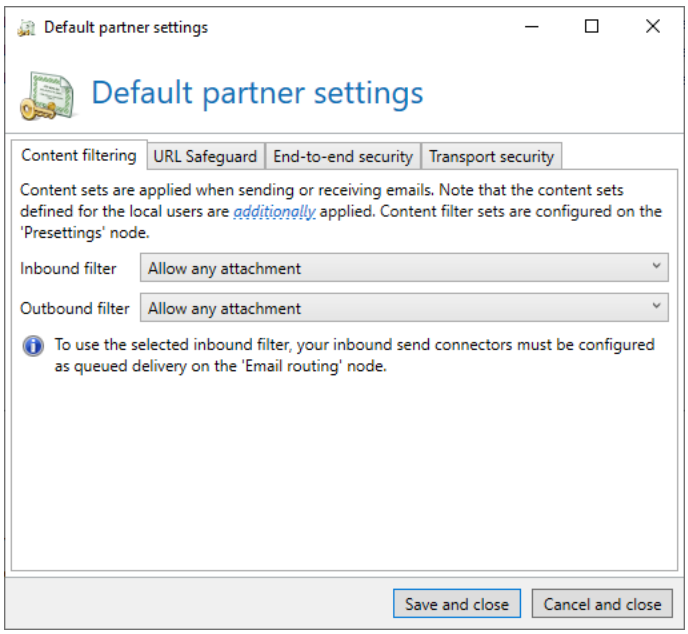
Partner topic

A partner entry defines the exchange process for email communication with external communication partners. These settings can be applied to all partners, to partner domains as well as to a partner email address. The settings made for an email address will have priority over domain settings, the domain settings will have priority over partner settings.

Default partner settings

To each of the settings types **Default partner settings**, domain settings and email addresses, one content filter for email attachments (Picture 54) can be applied. Content filters are defined under Content filter.

A valid licence for NoSpamProxy Encryption or NoSpamProxy Large Files is you want to use content filters.



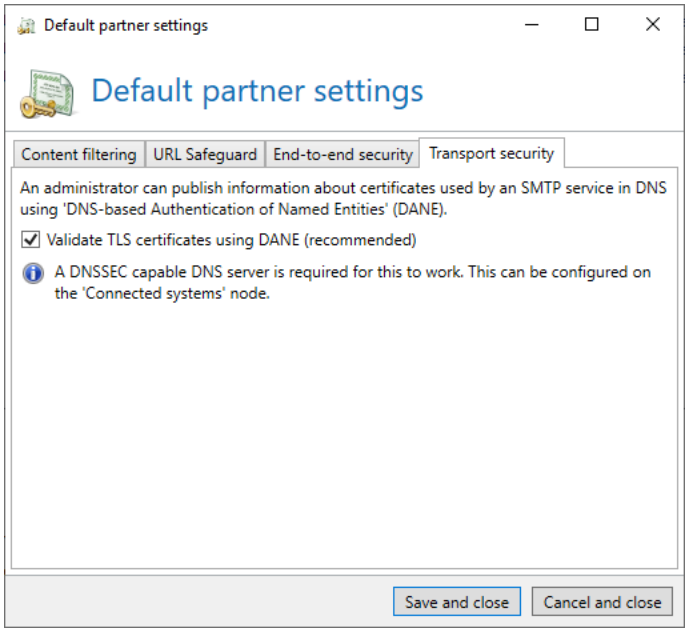
Picture 54: Default settings for content filters

The URL Safeguard prevents you from accessing malicious content that can be reached via links.

In the default settings for partners, you configure the basic behaviour for trusted and untrusted emails. You can also enable or disable tracking. Tracking allows you to see which users have accessed URLs that have **subsequently** turned out to be malicious.

For the use of 'DNS-based Authentication of Named Entities' (DANE), the use of a DNSSEC-enabled DNS server must be configured in the **Default setting for partners** (Picture 55). Through the use of DANE, the TLS certificates of the transport encryption are checked. This way, only certificates classified as trustworthy by the recipient of the email are accepted. More information on the concepts of DANE can be found at https://de.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities.

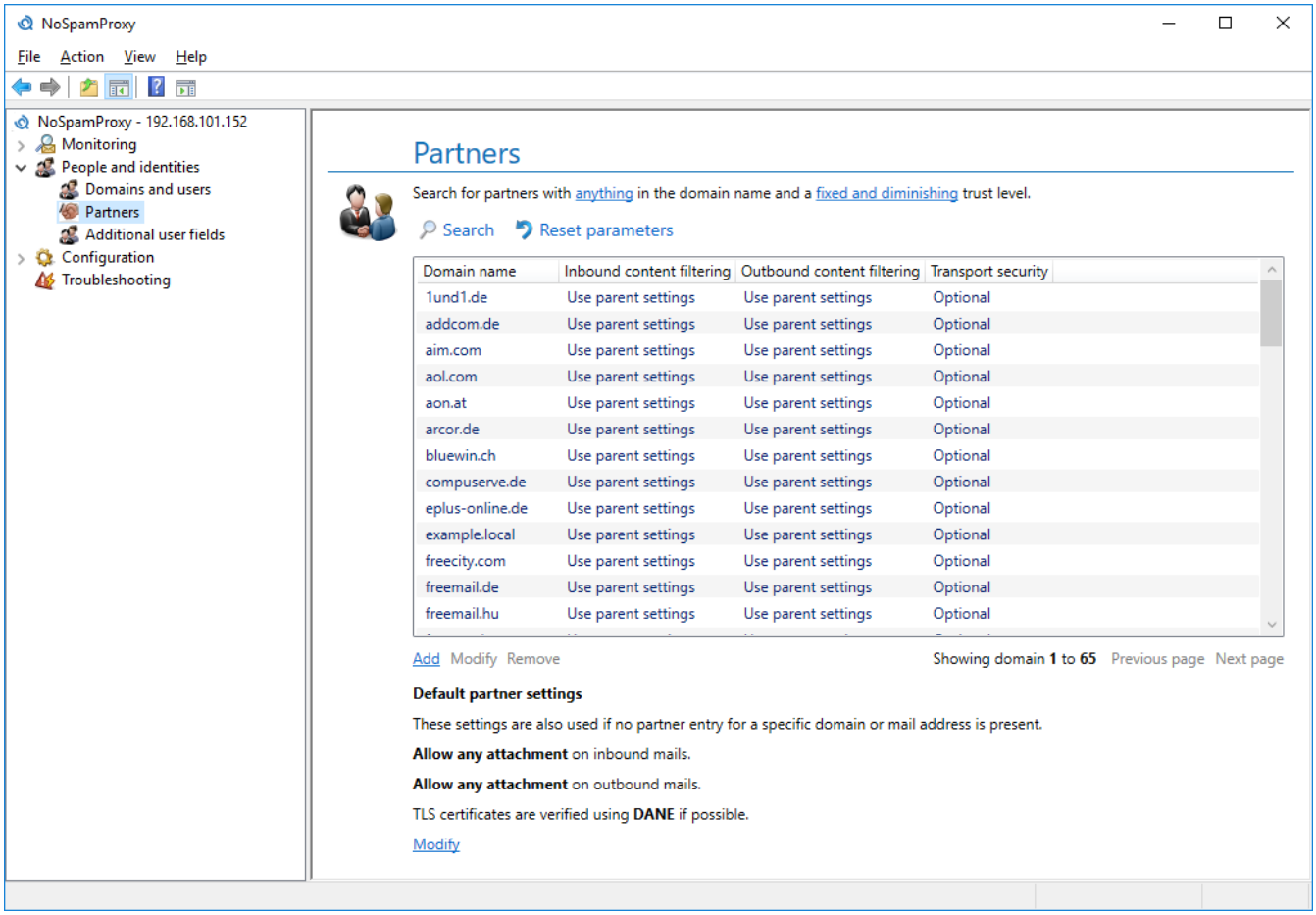
To secure the TLS certificates via DANE, you must configure a DNSSEC-enabled DNS server under Connected systems in the section DNS server.



Picture 55: Settings for DANE with TLS certificate

Partner domains

The list of the partners is grouped based on domains (Picture 56). Each domain contains settings for content filters, the required transport security and the trust between the domains.



Picture 56: The overview of all partners

The domain level settings apply to all partners that have not configured deviating settings for their email address in the **User entries**. Settings contained in user entries have priority over domain settings.

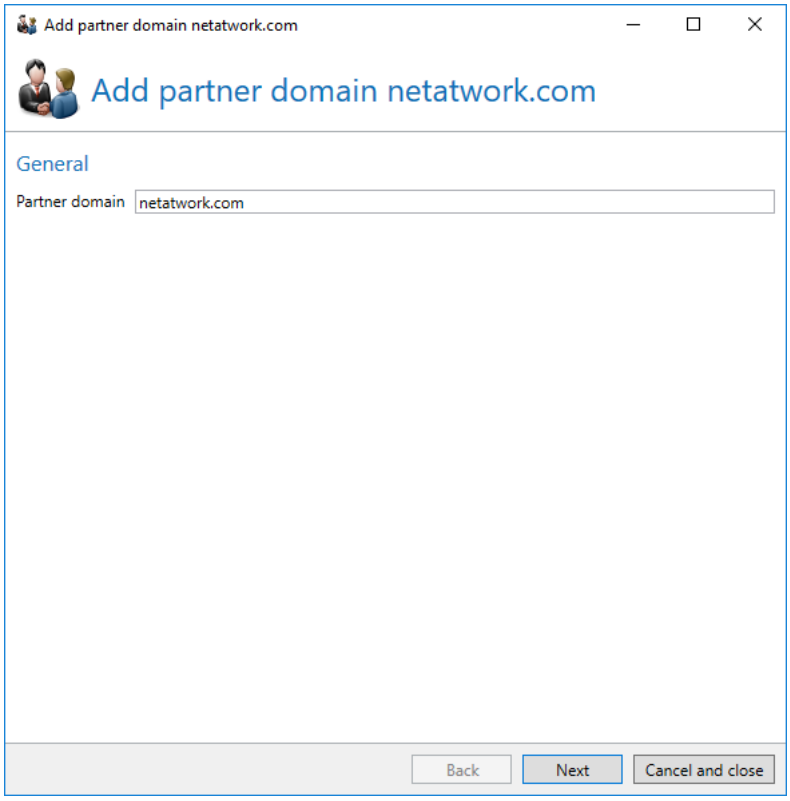
When creating a new partner domain, the default partner settings are applied to the entire domain. Settings for most partner addresses need only be configured once. Deviating settings for partner addresses have priority over partner domain settings.

Required transport security determines whether emails must be encrypted during their transport between servers. You can also add for the certificate used and provide additional certificates. The required transport security is applied to the entire domain.

NoSpamProxy Protection lets you configure the **Trust** in this domain. Trust is built automatically through email communication with partners. Trust is determined for the entire domain.

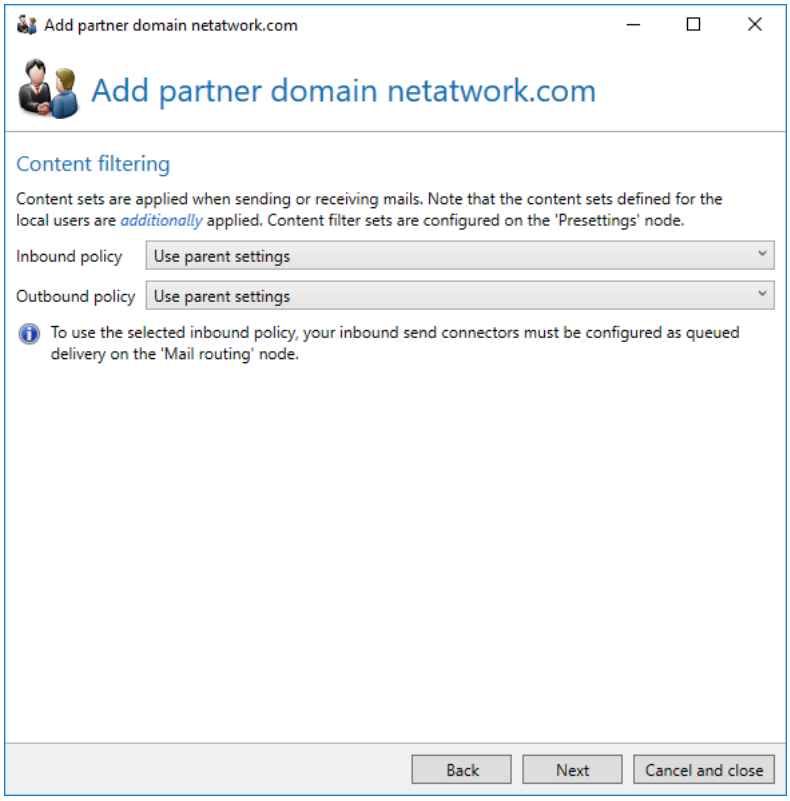
New partner domain

When adding new partner domains, first enter a domain name (Picture 57). The domain name must be entered in US-ASCII characters.



Picture 57: The domain name

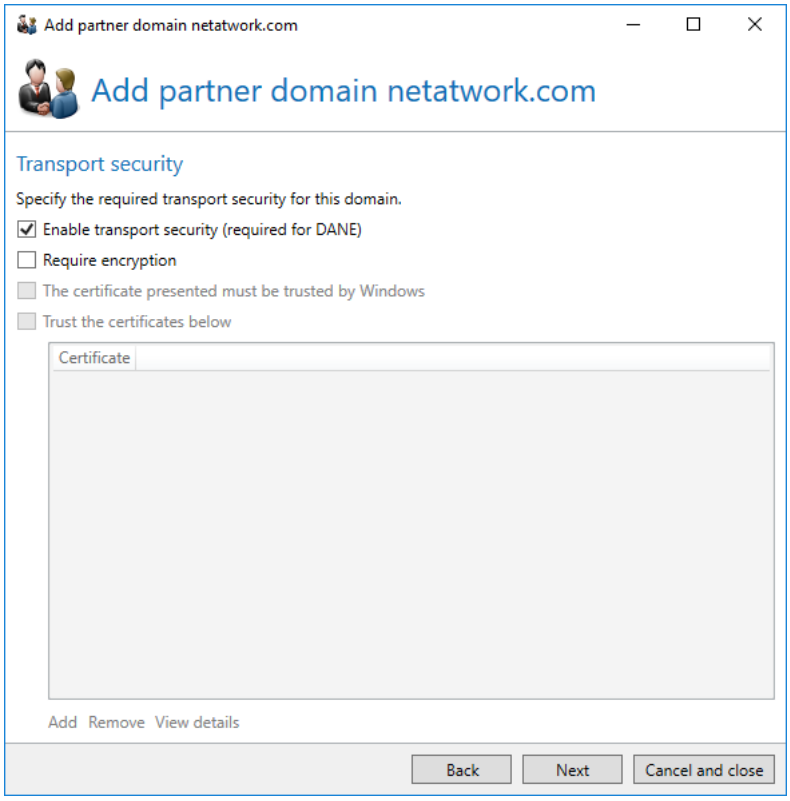
If you own a licence for NoSpamProxy Large Files or NoSpamProxy Protection, you can select the used content filters on the following page. The content filters are defined under Content filter.



Picture 58: Configuring the content filters

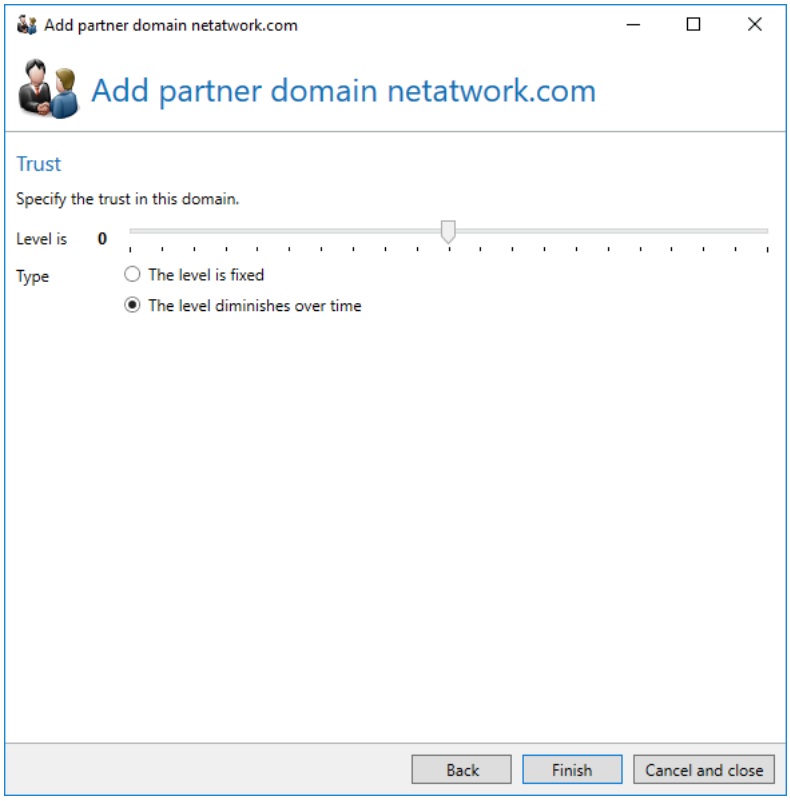
Transport security determines whether the communication to servers of the partner domains must be encrypted, if so, which certificates are trusted (Picture 59). You can also provide additional certificates which can be used for transport encryption to the target server. To deactivate transport security, you must deactivate all check boxes.

If you have selected **Delivery via a special server** in the Email routing as delivery method for external addresses for SMTP and **Require encryption** in the settings of the partner domains, the dispatch to this domain will fail. In this case, NoSpamProxy cannot ensure that the communication is encrypted all the way to the email server of the recipient.



Picture 59: Transport security

The **Trust** in a domain (Picture 60) is strengthened by emails sent to the domain. It will gradually approximate the value "0" in case no further email communication occurs. You can also set the trust to a fixed value. In this case, a positive value represents trust (bonus points), and a negative value mistrust (minus points).



Picture 60: The trust in a domain

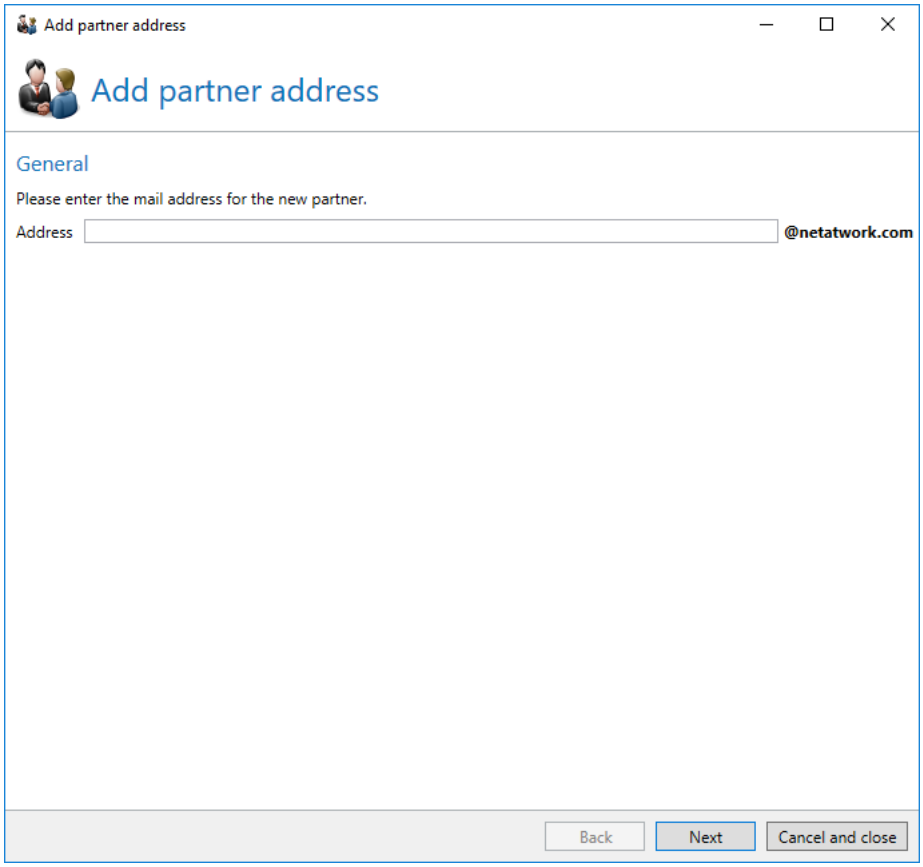
Edit partner domain

When editing a partner, the domain settings Domain can be adjusted. Additional areas are available when editing a partner.

User entry of a partner domain

Creating a user entry is identical to the creation of a Domain. A user entry is mapped to an email address and overrides the settings for the domain if communication with this email address occurs.

First, enter the email address (Picture 61). Please enter the local part (left to the @ character) of the email address into the field **Partner address**. The domain part is displayed next to the input field.



Picture 61: Adding a partner email address

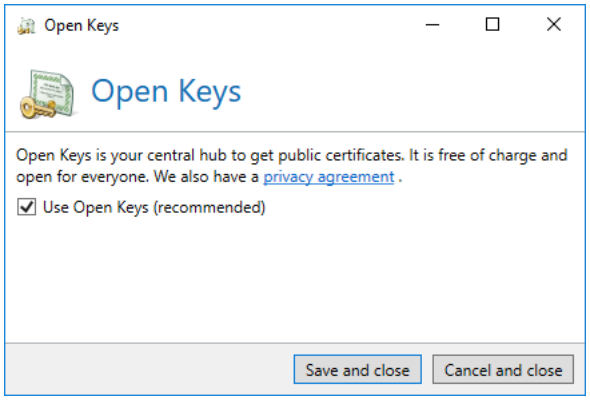
In the next step, you determine a content filter.

Open Keys Web Service

The Open Keys Web Service is the central hub for public certificates and the easiest way to request and retrieve public certificates. We recommend using Open Keys.

By default, the Open Keys Web Service is used to request and retrieve public certificates. In case the service deactivated, proceed as follows:

Under **Public key servers/Open Keys**, click **Edit**.



Picture 62: Using the Open Keys Web Service

Tick the checkbox next to **Use Open Keys (recommended)** and click **Save and close**.

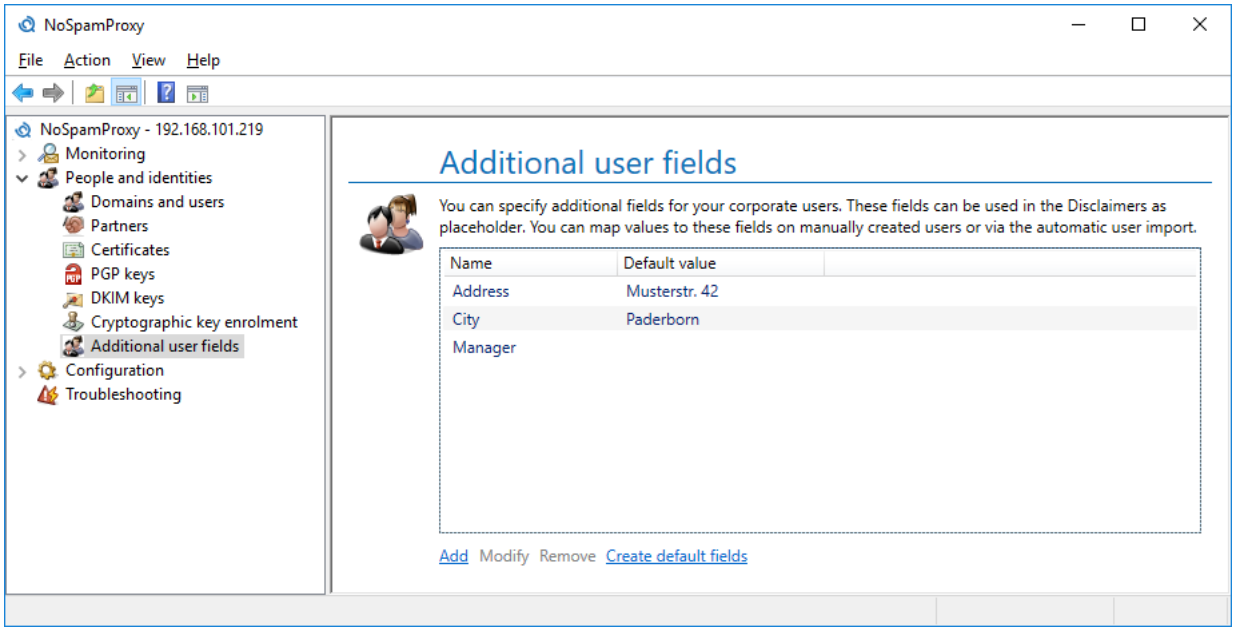
Additional user fields

To use the "Additional user fields" a valid licence for the Disclaimer feature is required.

You can add to the data of your corporate users by adding additional fields. Subsequently, you can insert these fields into your disclaimer templates as placeholders. These will be replaced by sender data.

For manually created users, you can edit the user fields defined here directly for the respective user. If you import your users from a system which has been removed, you can determine how these fields are filled via the Automatic user import

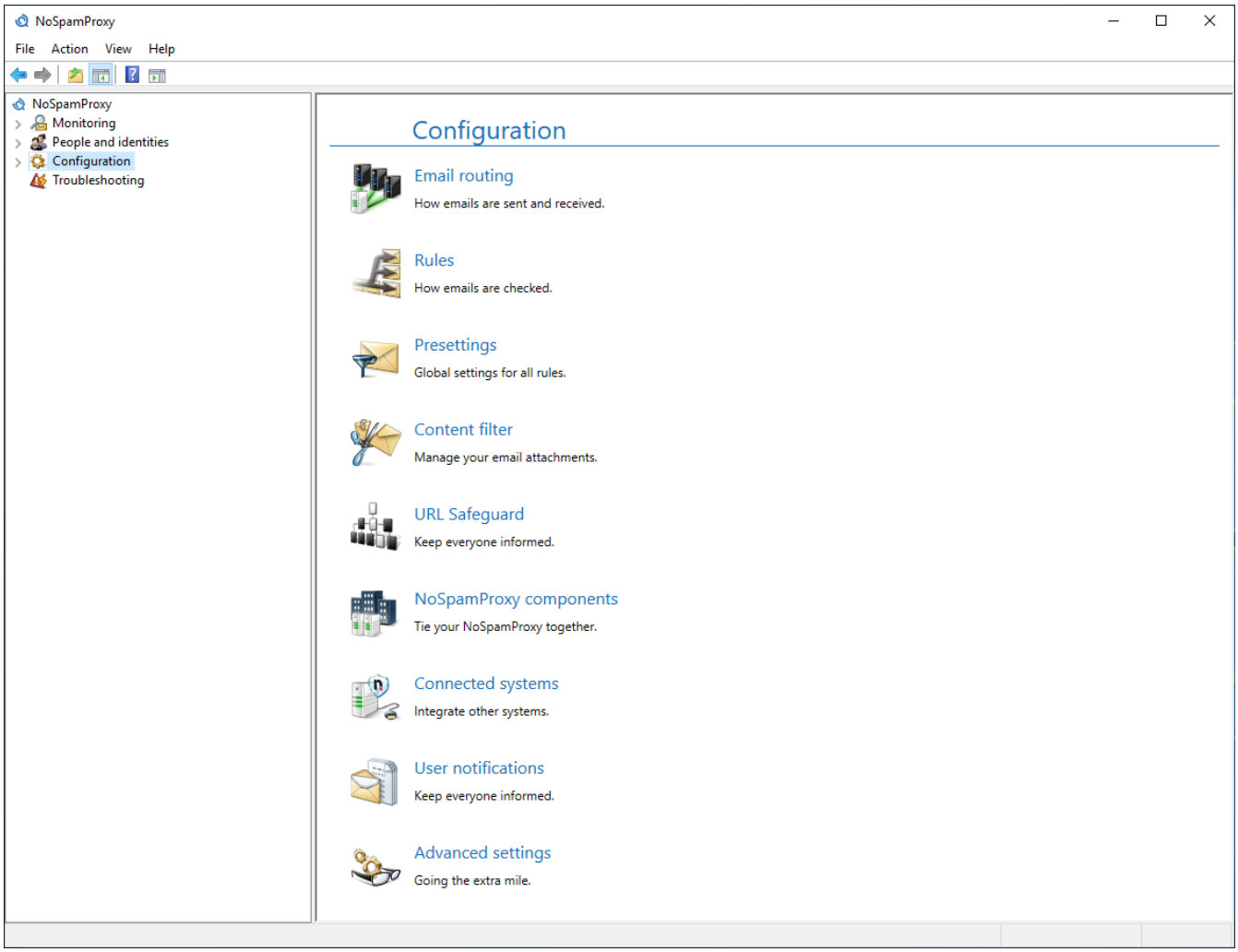
You can also define a default value for each field. This value is used if no value is set for the respective user.



Picture 63: List of all custom fields

10. Configuration

Under **Configuration** (for the Intranet Role) you can find the settings for the connection to other roles, settings of the database as well as notification addresses. (Picture 64).



Picture 64: Intranet Role Settings

Email routing

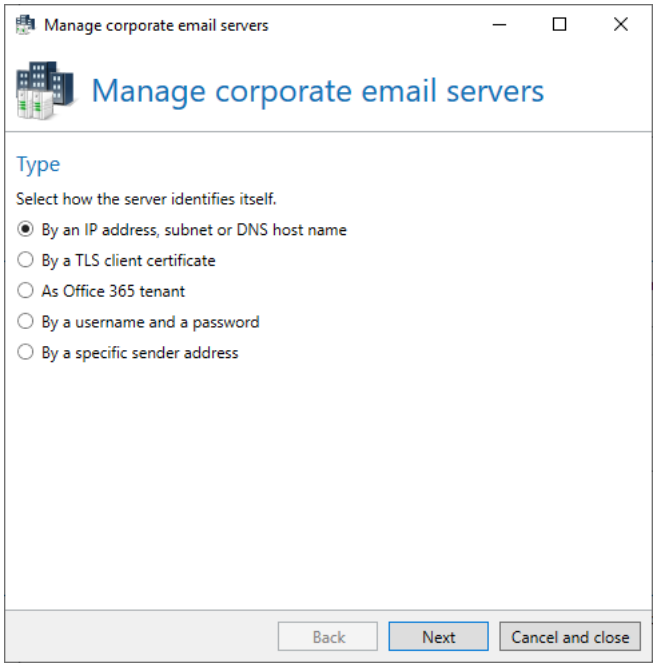
Under **Email routing** you can find the connectors for the delivery of inbound as well as outbound emails. Under Receive connectors, you can configure how NoSpamProxy receives emails. Additionally, you can configure the local servers here.

Local email servers

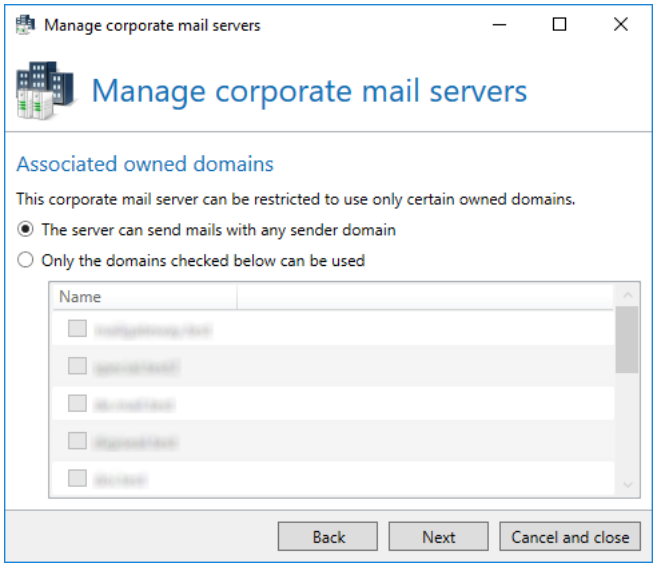
Here, you list all email servers allowed to use owned domains as sender domains for emails. Local servers are identified in multiple ways:

- **IP address**
  A server is regarded as local if it sends from the given IP address.
- **Subnetwork**
  A server is regarded as local if it sends from an address in the given subnet. A subnet is provided in the CIDR representation, e.g. 192.168.100/24.
- **DNS domain name**
  A server is regarded as local if the DNS host name configured here references the address of the server.
- **TLS certificate**
  A server is regarded as local if it executes TLS authentication using a client certificate during the connection. If a root or intermediate certificate is entered, the server must report with a certificate which contains the configured certificate in its certificate chain. If an end certificate is entered, the server must report with the exact same certificate.
- **Office 365**
  Here, you can enter Office 365 as local server. A server is regarded as local if it is an official "Office 365" server.

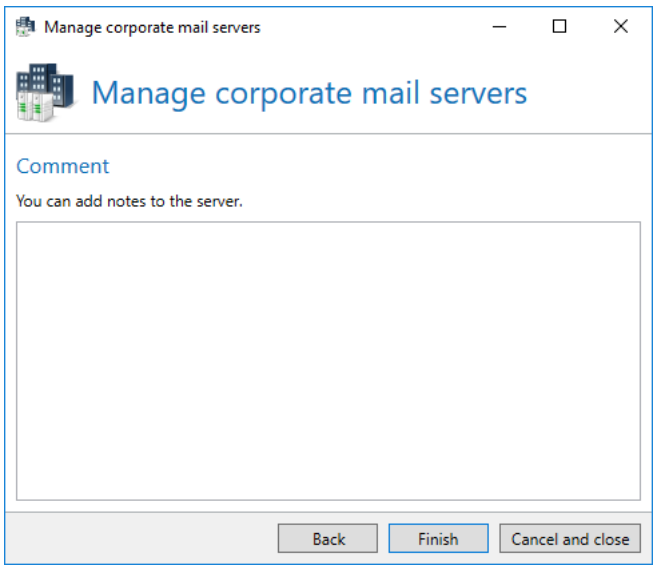
When adding new local email servers, select the type of the server first (Picture 65). Then, configure the specific settings specific for this type. Now you can select whether the connector is only responsible for specific domains or for all (Picture 66). Afterwards, you can also add a comment (Picture 67).



Picture 65: Server type selection



Picture 66: Indicate with which corporate domains the server is allowed to send emails



Picture 67: You can also add a comment

Multiple used settings of connectors

Some settings are used multiple times for certain connectors. The settings are explained in the following chapters.

Name

Use the field **Name** to give each connector an unique name. The name must differ from other connectors of the same area. The name ensures that you can distinguish the different connectors and can be used to briefly describe the function of the connector.

Connection to Gateway Roles

Depending on its type, the connector can either be used on several Gateway Roles simultaneously or on one single role only. Select the Gateway Roles on which you wish to operate the connector.

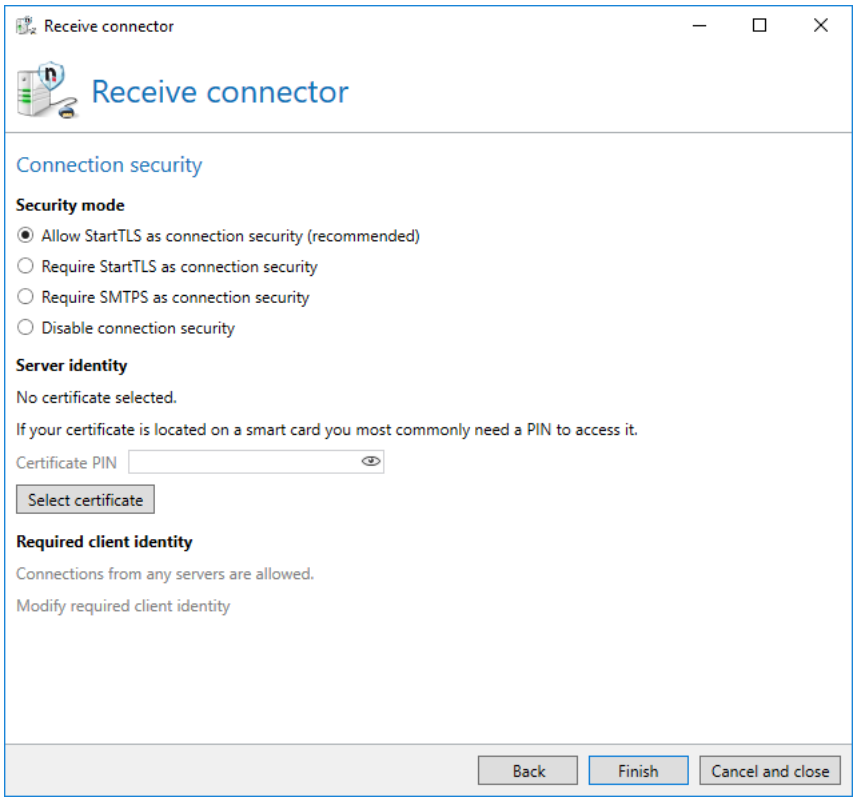
Costs

The **Costs** are used if multiple send connectors can be used for email delivery. In these cases the connector with the lowest costs will be used. If delivery of the email via this connector fails, the email delivery definitely failed. In this case, no further connectors with higher costs are used.

Connection security

The connection security (Picture 68) determines the encryption of the transport connection. The dialog described here is used several times for the different connectors. For some connectors, individual configuration options are hidden.

This concerns the encryption on the transport route. This does not refer to an end-to-end security.



Picture 68: Settings for the connection security

SMTP Security settings

In the section **Security settings**, you can determine the security level for the transfer of emails to local addresses. The following settings are available:

- **Allow connection security through StartTLS (recommended)**
  If this mode is used, encryption of the connections is possible but will not be forced. The encryption of the connection via StartTLS is optional for the inbound server. A certificate in the area Server identity for receive connectors is required. As an option, you can provide a certificate in the area Client identity for send connectors to ensure the identity of the send server for the receive server.
- **Demand connection security through StartTLS**
  If you want to make sure that all connections via the corresponding receive connector are encrypted, you must select this option. NoSpamProxy will then demand an encrypted connection from the inbound server via StartTLS. If this mode is used, you need to provide the gateway with a certificate in the section Server identity.

- **Use TLS as connection security**
  If set, an SMTP connector expects a connection establishment via SMTPS. A POP3 connector expects POP3S. Use this setting only if absolutely necessary. The StartTLS procedure is the state-of-the-art and most widely-used procedure in connection encryption. Usually, a separate port (normally 465) is used for SMTPS since the connection is automatically expected in encrypted form similar to HTTPS via the port 443.
- **Deactivate connection security**
  If set, connections are never encrypted. Thus, NoSpamProxy does not offer connection security to inbound servers.

SMTPS on port 25 does not comply with RFC. Use an own receive connector which you locate on port 465 instead.

The encryption level necessary for the connection by StartTLS or SMTPS amounts to at least 128 Bit. Connections with a smaller encryption level are not accepted. Moreover, only TLS connections are accepted. SSL connections are not supported since they are no longer considered as safe.

Server or client identity

SSL certificates are required for the encryption of the transport connection. The receiving email server requires a certificate as server identity to enable the encryption of the connection. The sending email client can prove its own client identity through a certificate.

- **Server identity**
  An SSL certificate in the receive connector is used to be able to provide connection security. The certificate as server identity for the receiving email server facilitates the encryption via StartTLS or TLS. Without certificate, the encryption for connections must be deactivated.
- **Client identity**
  An SSL certificate in SMTP send connectors is used to ensure the identity of the sending email server. Since the certificate of the server identity of the receiving server suffices for the encryption of the transport connection, the connection security via StartTLS or TLS can be used without a certificate as client identity.

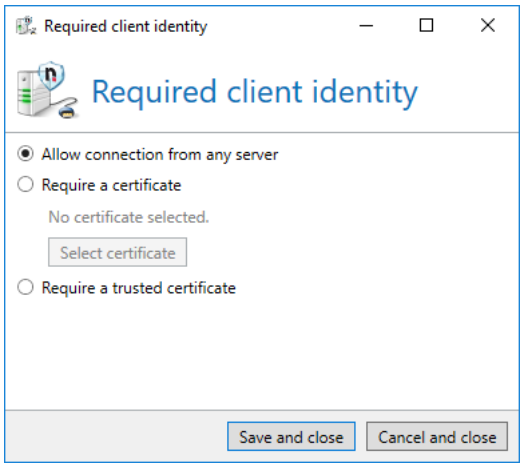
When adding a certificate for the transport encryption via StartTLS, the Gateway Role requires read access to the private key. Access to this role is granted automatically. However, you must restart the Gateway Role in order for the change to become effective and to enable read access for the Gateway Role on the private key of the used certificate. A corresponding alert message is also displayed.

After selecting the certificate, you might be asked to enter a PIN code into the field **Certificate PIN (optional)** if the certificate store has protected the certificates with a PIN.

Please make sure to enter the correct PIN code. Many of the certificates protected by PIN codes are irrevocably destroyed by entering the wrong PIN code three times.

If SSL is forced for connections, you can determine which clients are permitted to connect in the section **Required client identity** by only allowing access if the counter device authenticates with a corresponding certificate (Picture 69):

- **Allow connections of every server**
  Every server may connect.
- **Require certificate**
  The certificate to be provided by the counter device depends on the certificate selected here: For intermediate or root certificates, the counter device must authenticate itself with a certificate which contains the selected certificate in the certificate chain. for end certificates, the counter device must authenticate itself with the exact same certificate.
- **Require trusted certificate**
  The certificate chain of the presented certificate must be terminable via the certificates of the Windows certificate store.

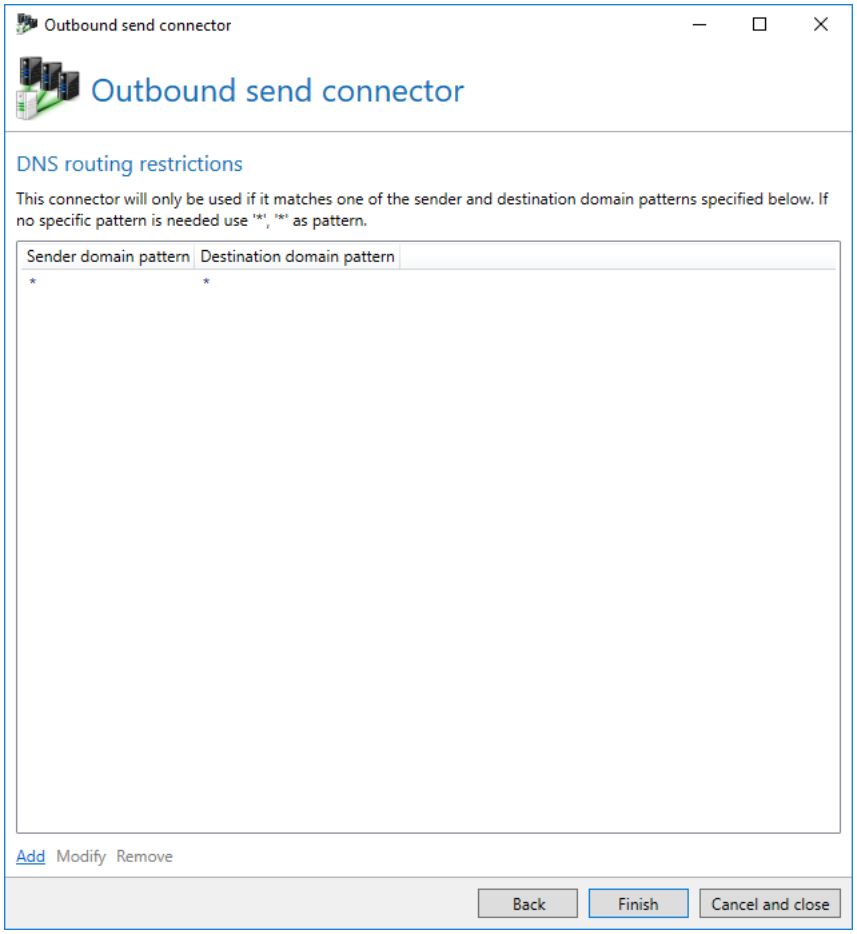


Picture 69: Determining the required client identity

DNS routing restrictions through connector namespaces

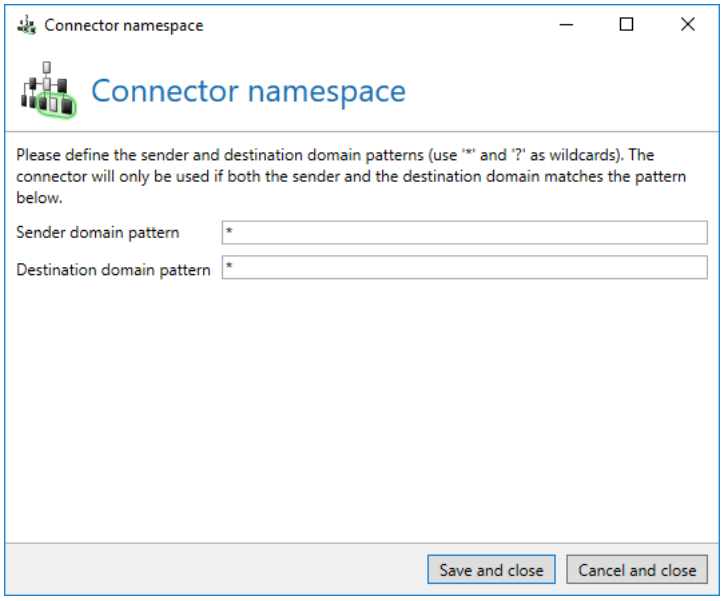
A send connector can also be configured in such a way that it delivers emails for a partial area of the available DNS namespaces only. Should several connectors be applicable to one email, the connector with the lowest costs is used.

By default, a namespace of "*" as sender domain and "*" as recipient domain is automatically created in a new connector. Thus, a new connector has no restrictions in the DNS namespace since the placeholder "*" corresponds to any possible name. If the connector created should only manage selected domains, you need to delete the default namespace and replace it by a different one.



Picture 70: Connector namespaces determine which sender or recipient domains are managed by a connector

A connector namespace (Picture 71) consists of a pattern for the "send domain" as well as the "target domain". This pattern may also contain placeholders ('*' and '?').



Picture 71: Definition of a DNS namespace

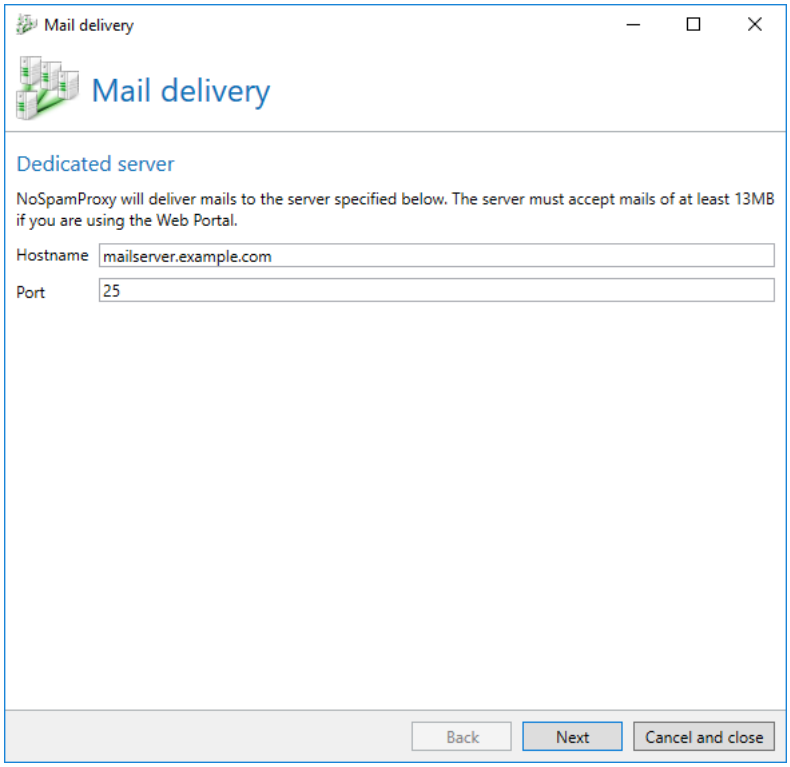
Example: To build a send connector for external addresses which only sends emails from the domain "example.com" to the domain "netatwork.de", you must apply the following settings.

Sender domain pattern	Target domain pattern
example.com	netatwork.de

Smarthost: Email delivery via dedicated server

A Smarthost is a dedicated server for email delivery. Smarthosts are, for example, located at your internet provider or in the owned company network in case emails can only sent from this server.

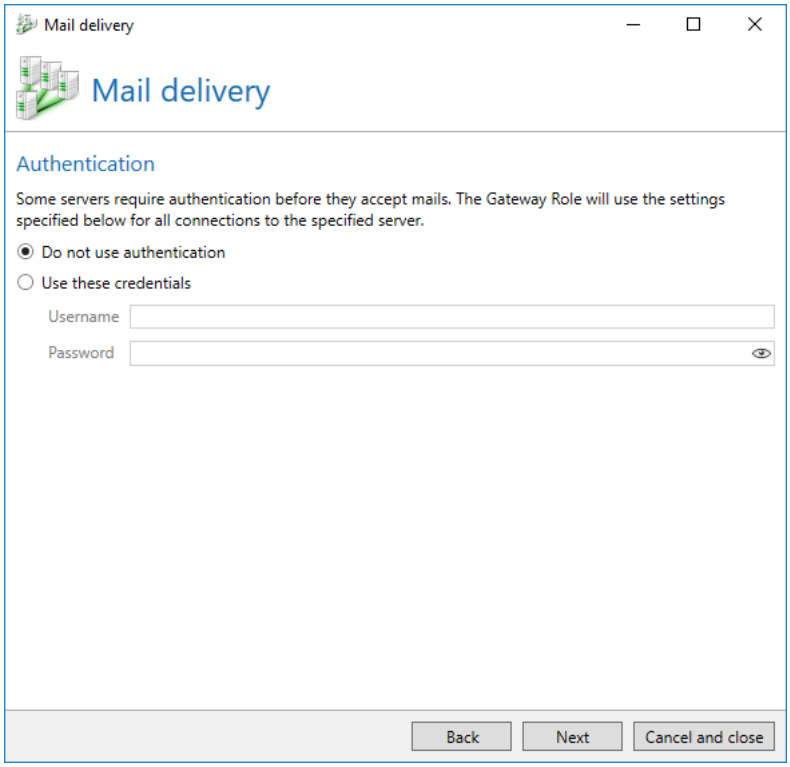
On the page **Dedicated server**, enter the IP address or the server name and the port of the dedicated server (Picture 72). As a rule, this is the IP address or server name of the next email system.



Picture 72: Connection settings for the dedicated server

We recommend to enter addresses not as IP addresses but by using server names.

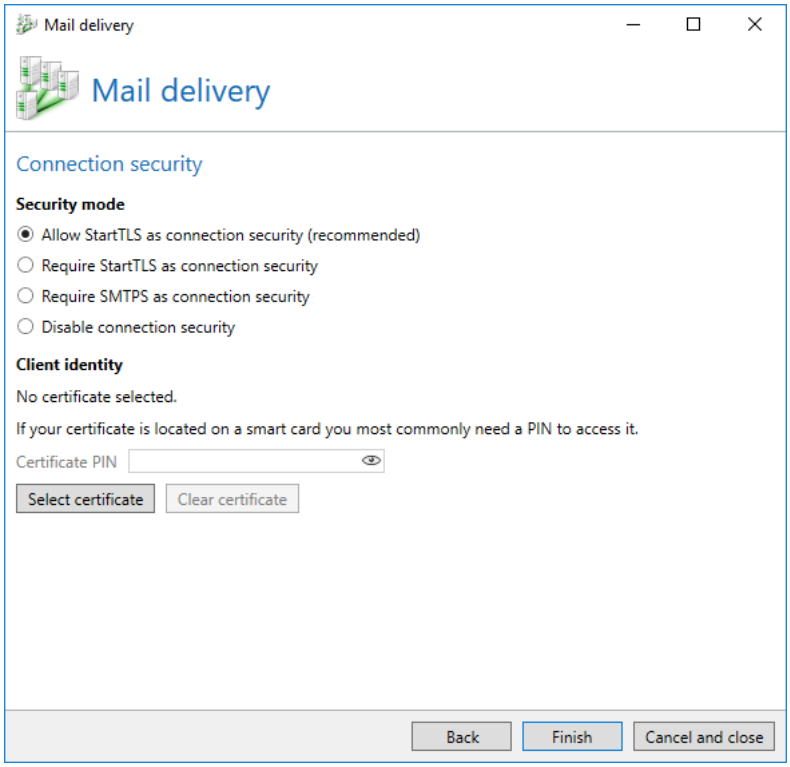
For external Smarthosts such as that of your provider, user name and password are often required for authentication. You can provide them on the tab **Authentication** (Picture 73).



Picture 73: If required, you can deposit login information for the dedicated server here

NoSpamProxy supports "Basic" as authentication procedure. When using this method, user name and password are transmitted without encryption. If supported by your provider, you should activate the connection security for the connections.

The options for the connection security to Smarthosts must be configured as described in chapter Connection security (Picture 74). SMTP send connectors for emails to external addresses use the certificate-based identity as Client identity.



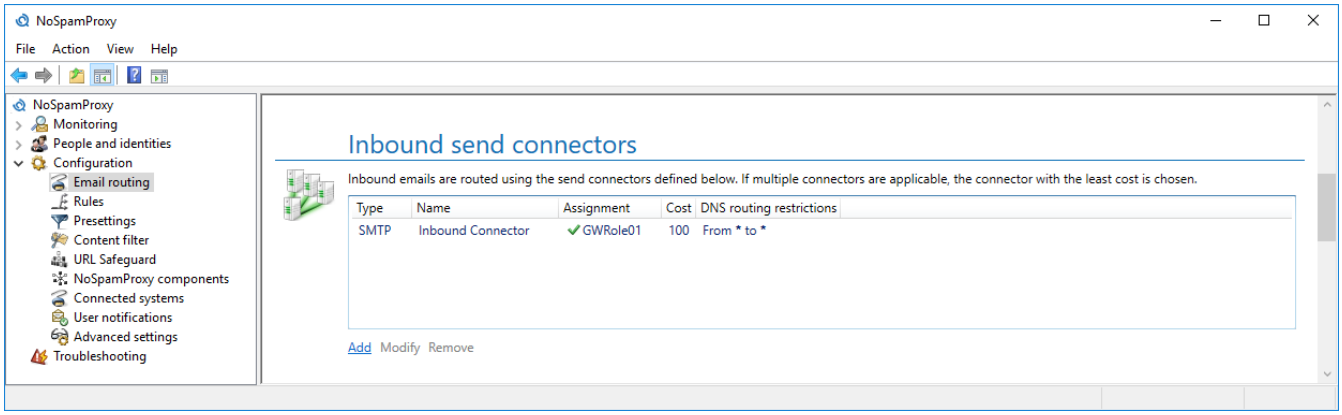
Picture 74: Connection security of an SMTP Smarthost

If you send emails to external addresses via another Smarthost and enforce the encryption in the domain trusts of a domain, the dispatch to this domain will fail, if the Smarthost for the emails does not support encryption. Thus, you must ensure that the Smarthost always supports StartTLS for the emails.

Inbound send connectors

Under **Inbound send connectors**, you determine which servers emails to local addresses are forwarded to.

The delivery of inbound emails is executed exclusively via the **Queue system**.



Picture 75: Overview of inbound send connectors

Delivery via queues

NoSpamProxy will add the email to a queue after receipt and subsequently forward it to the configured Smarthosts. It is irrelevant for the successful receipt of the email whether the next Smarthost is available or not.

The email will be scanned for viruses and spam contents by NoSpamProxy Protection during transfer and rejected if required.

If you have added Office 365 to the local servers, a "Office 365" connector is displayed here. This connector is responsible for the delivery of local emails to Office 365. Except for the binding to certain Gateway Roles, you cannot modify or delete this connector.

General settings

Enter a Name and select the Gateway Roles. Subsequently, determine the Costs of the connector.

SMTP connections

You can configure several Smarthosts under the SMTP connections. NoSpamProxy will attempt to deliver the email to one of the configured Smarthosts. The order cannot be configured or determined by the user. As soon as a Smarthost receives the email, it is regarded as "sent".

Configuration of a Smarthost

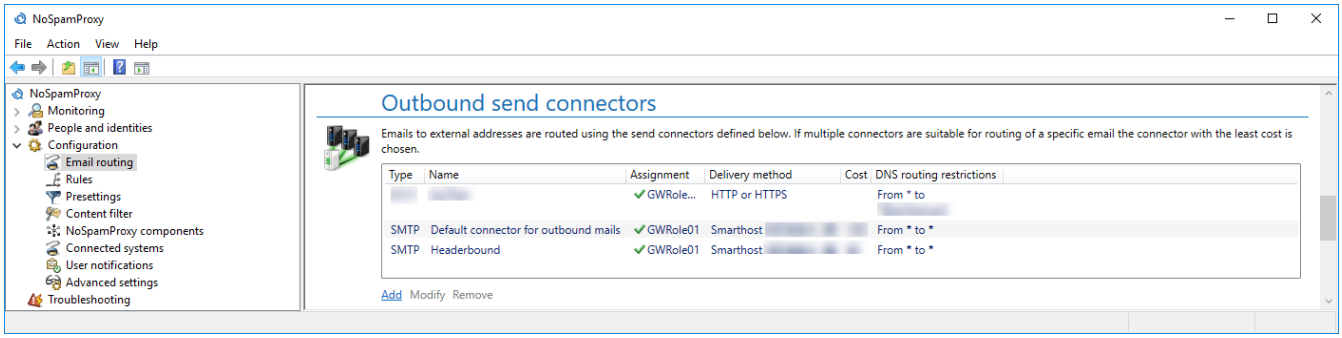
The configuration of a Smarthost for the inbound email delivery proceeds as described in chapter Smarthost: Email delivery via dedicated server. In the Connection security, the send connector for local addresses uses a Client identity.

DNS routing restrictions

You define the restrictions for the namespace managed by the connector under **DNS routing restrictions**. The configuration of the restrictions for the local delivery functions as described in chapter DNS routing restrictions through connector name spaces.

Outbound send connectors

Under the section **Outbound send connectors**, you determine how emails are sent to an external server.



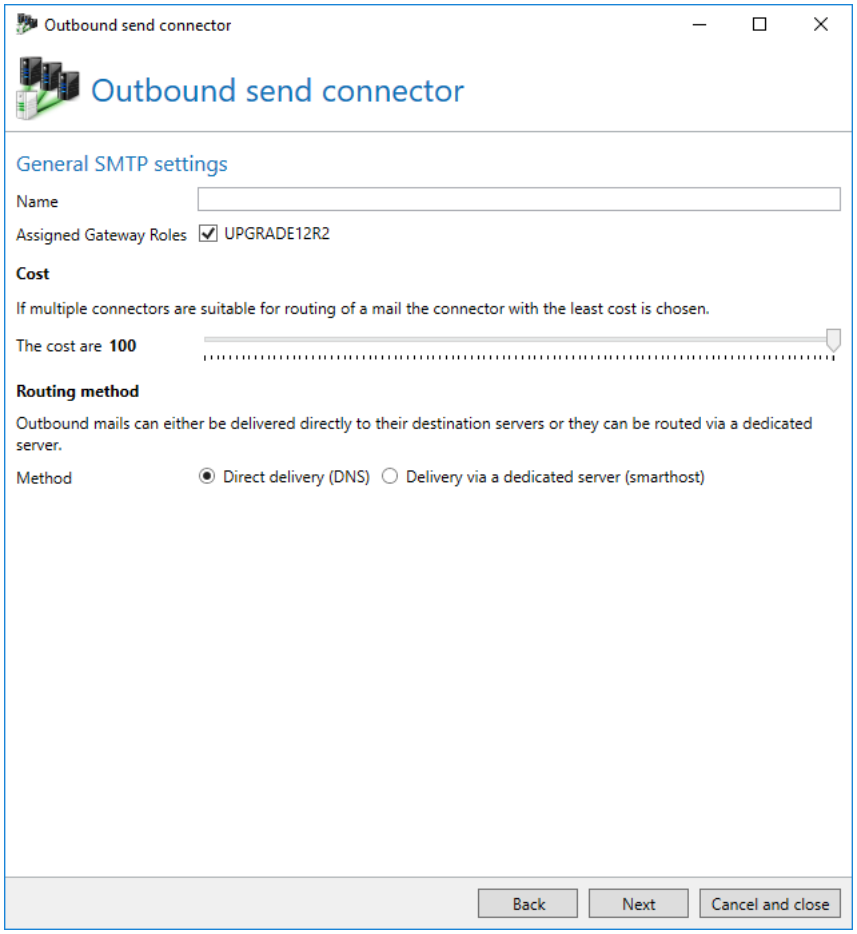
Picture 76: Overview of outbound send connectors

SMTP

The SMTP connectors are deployed for the delivery to external SMTP servers. Via these, you can either configure a direct delivery to the target SMTP server or a delivery via a dedicated server (Smarthost) which accepts all emails of the connector to forward them for delivery.

General settings

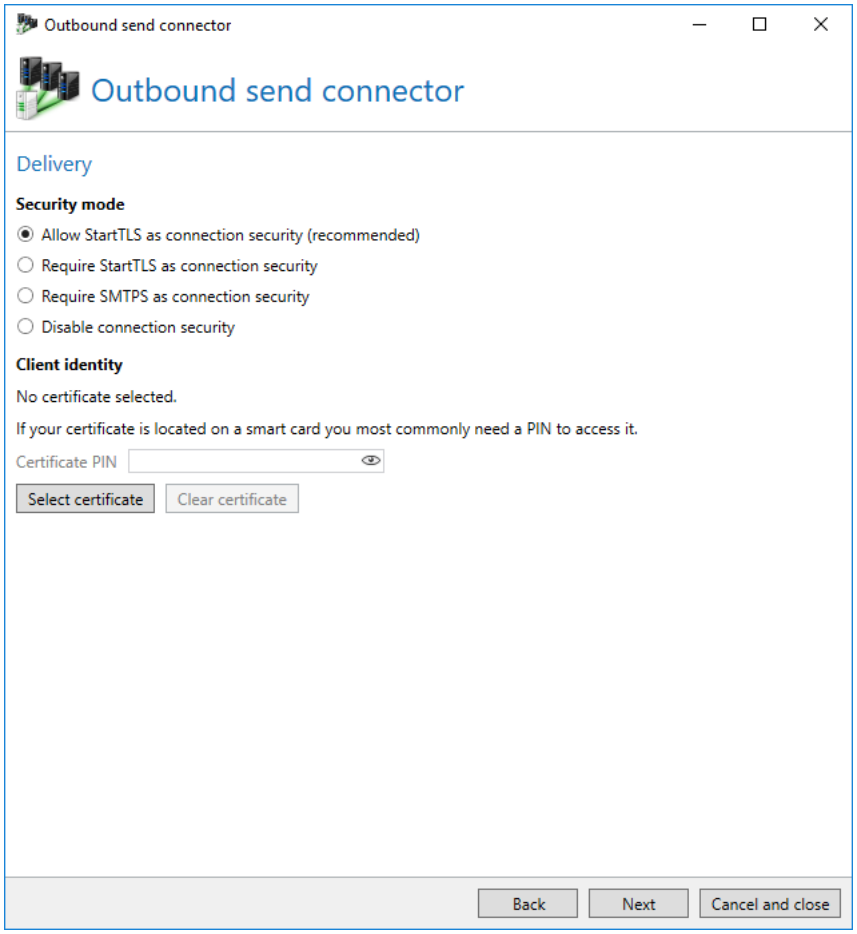
Enter a Name and select the Gateway Roles. Subsequently, determine the Costs of the connector. Subsequently, as for the **Routing method**, either choose the Direct delivery (DNS) or the Delivery via a dedicated server (Smarthosts) (Picture 77).



Picture 77: Names, costs and delivery method of an SMTP send connector

Delivery - Direct delivery (DNS)

The direct delivery via DNS servers attempts to deliver the emails directly to their target servers. The required Connection security must be configured for this connector. Additionally, you can deposit a specific Client identity in order for NoSpamProxy to be able to authenticate to other servers (Picture 78).



Picture 78: Connection security of the SMTP send connector

Delivery - Dedicated servers (Smarthosts)

The configuration of a Smarthost for the local delivery functions as described in chapter Smarthost: Email delivery via a dedicated server. The connection security for the connection to the respective Smarthost offers the same options and restrictions as described in chapter Delivery - Direct delivery (DNS).

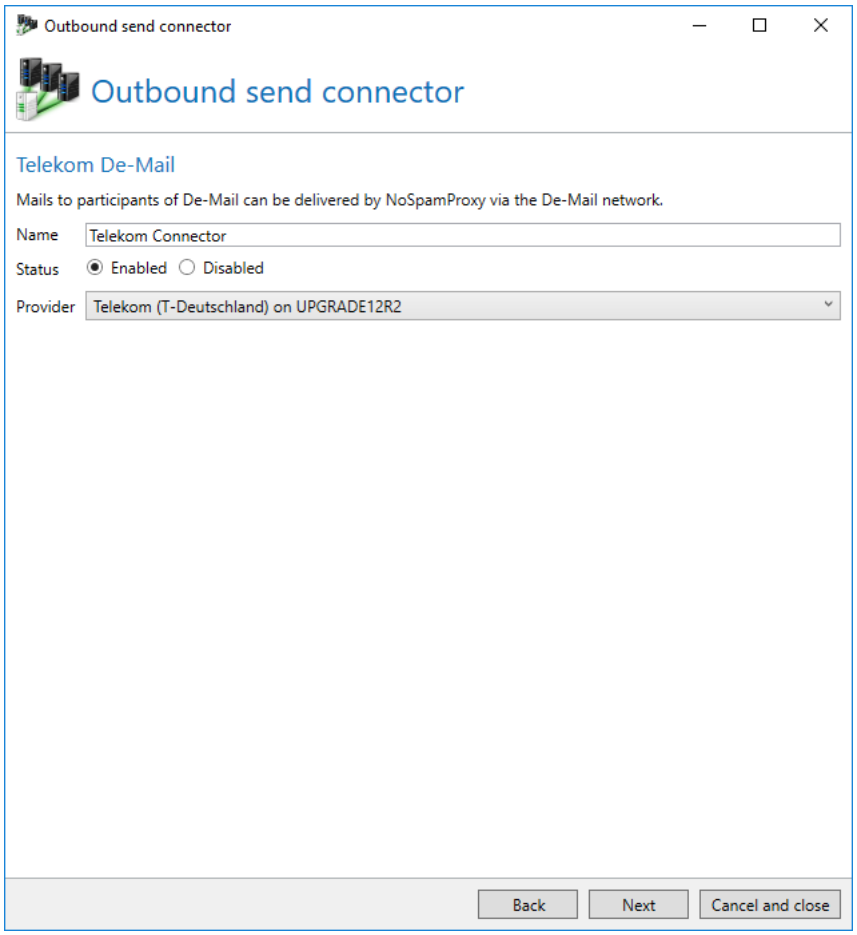
DNS routing restrictions

You configure the restrictions for the namespace managed by the connector under **DNS routing restrictions**. The configuration of the restrictions for the local delivery functions as described in chapter DNS routing restrictions through connector namespaces.

De-Mail via Telekom

For the connection to Telekom De-Mail, a De-Mail provider for a **Telekom De-Mail connection** must be set up under Connected systems.

Use this connector if you wish to send De-Mails via Telekom. First, provide the Name and the status of the connector. Second, select the configured provider from the list. The providers are described in the list along with their names, target system (T-Deutschland / T-Systems) and Gateway Role where they are located (Picture 79). Next, configure the Mapping of owned domains.

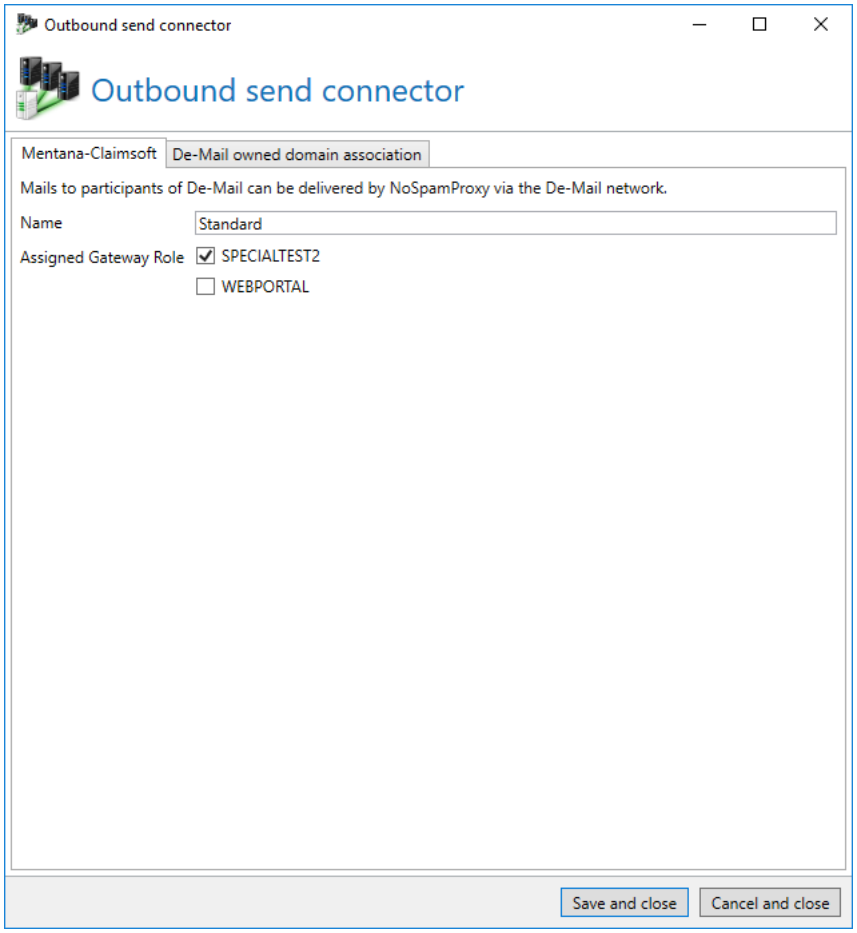


Picture 79: Telekom De-Mail connector settings

De-Mail via Mentana-Claimsoft GmbH

Connecting to Mentana-Claimsoft De-Mail requires a suitableDe-Mail provider which can be set up under Connected systems.

Select a unique Name for this connector and determine to which Gateway Roles it should be mapped (Picture 80). Now select the owned domains allowed to send emails through this De-Mail connector.

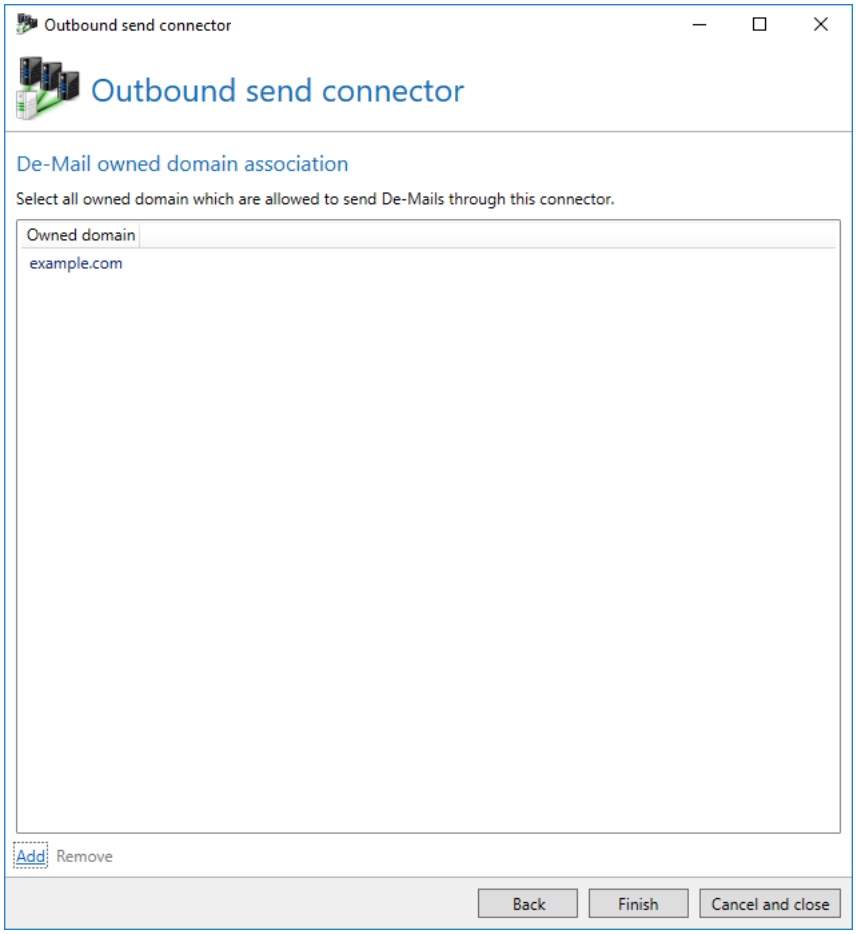


Picture 80: Mentana-Claimsoft De-Mail connector

Mapping of owned domains

Mapping owned domains to certain De-Mail connectors allows establishing separate De-Mail connectors for each of the different owned domains. If you configure only a single De-Mail send connector, make sure to map all owned domains to it. For multiple De-Mail send connectors you must map your owned

domains to the respective connector. This way, NoSpamProxy can decide via which De-Mail connector emails are sent.



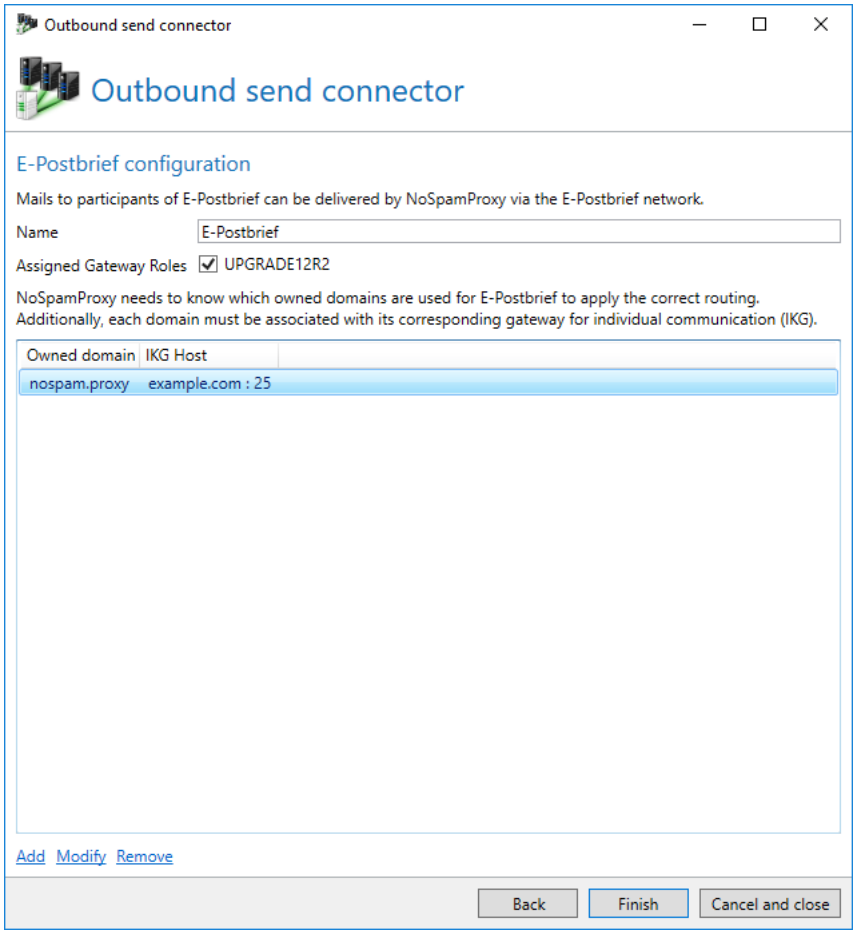
Picture 81: Mapping owned domains to De-Mail send connector

E-Postbrief connector

With E-Postbrief, Deutsche Post offers binding, confidential and reliable communication. For more details see http://www.epostbrief.de. Companies are offered the possibility of communicating directly to the Deutsche Post infrastructure via the so-called Individual Communication Gateway (IKG). The IKG is installed as part of your company's infrastructure and functions as an SMTP endpoint for email routing to the Deutsche Post network .

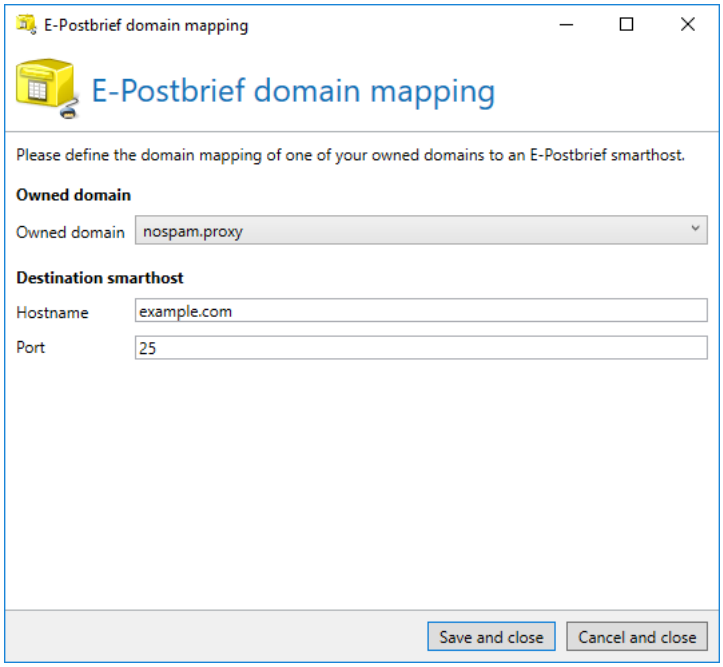
The E-Postbrief connector handles the automatic routing of emails to an IKG. Moreover, it ensures that an E-Postbrief is only accepted from the IKG. This prevents regular emails received from the Internet to be passed off as an E-Postbrief.

After selecting the E-Postbrief connector, on the following page you can determine for different internal domains to which IKG E-Postbriefe from this domain are sent . (Picture 82).



Picture 82: Configuring the delivery of E-Postbrief

Assignment of the owned domains to the IKGs is realised via a separate dialog (Picture 83).



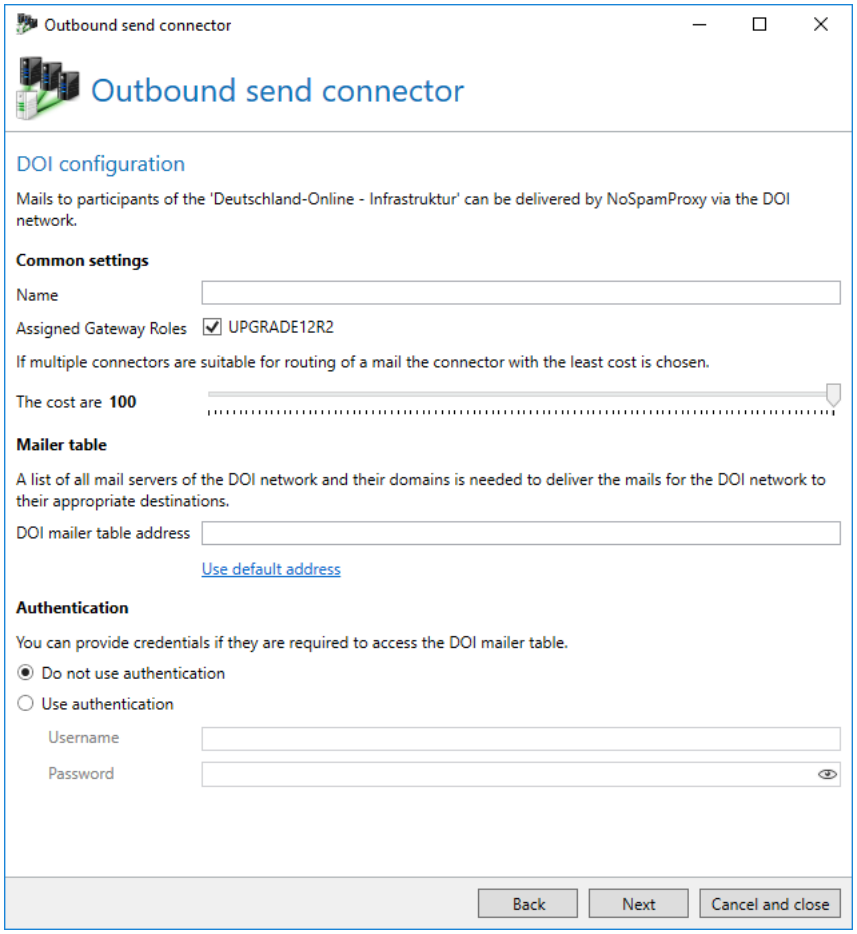
Picture 83: Mapping an owned domain to an IKG

Deutschland-Online - Infrastruktur connector

The Deutschland-Online - Infrastruktur (DOI) project is used, among others, by municipalities to ensure secure transfer of messages. If you are no member of the DOI project, you have no use for this connector and can skip this chapter.

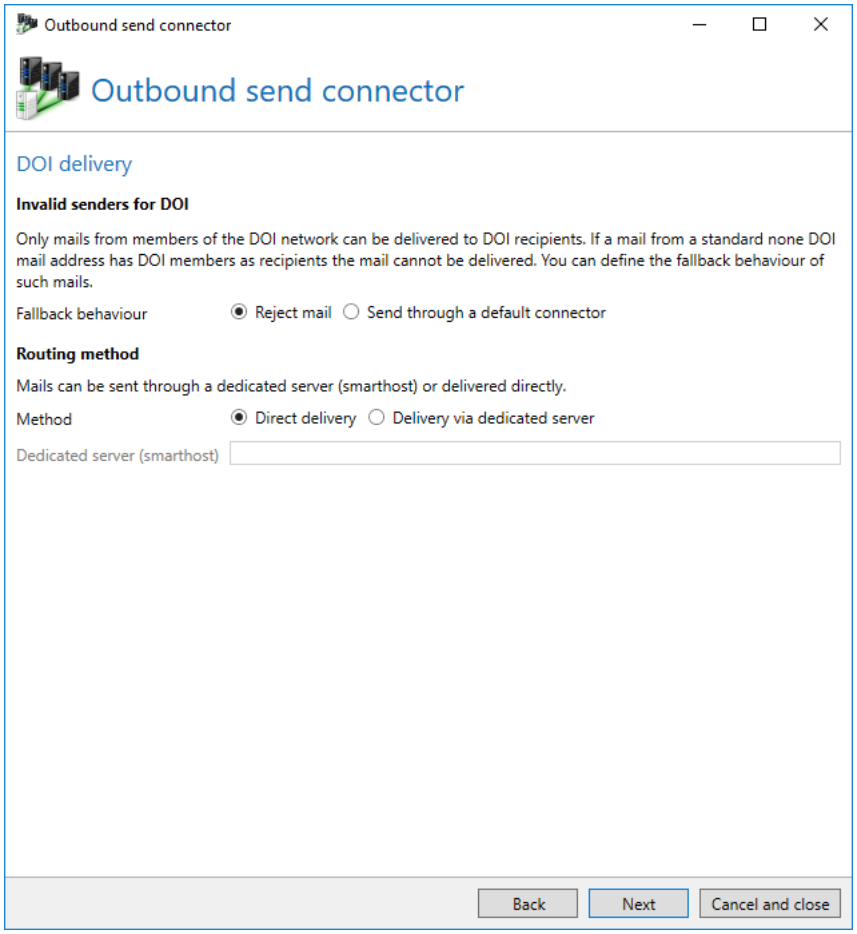
The DOI connector automatically downloads the current routing table of all participants and routes emails to other participants via the secure DOI network.

To activate the delivery to the DOI network, create a new connector under **Email routing** in section **Outbound send connectors**. In the following dialog, select **Deutschland-Online - Infrastruktur (DOI)** as type and click **Next**. In the next step, enter the FTP- or web address from where you obtain the mailer table. Enter your user name and password under **Authentication**. Then, you select a value for the costs which is smaller than the one provided for the default connector for emails to external addresses. By doing this, you ensure that the default routing connector does effect the routing for these emails. When finished, click **Next** (Picture 84).



Picture 84: Configuring the delivery to the network of Deutschland-Online - Infrastruktur

On the page **DOI delivery**, you can configure the properties for invalid senders (Picture 85). Senders are considered invalid if the sender domain is not part of the DOI network. These emails must not be delivered via the DOI network. You can now select whether these emails should be returned to the sender or sent via a different, more expensive connector. Furthermore, you can determine how emails should be delivered. Emails can either be delivered directly or via a Smarthost (recommended). Such a Smarthost is provided by the DOI network.

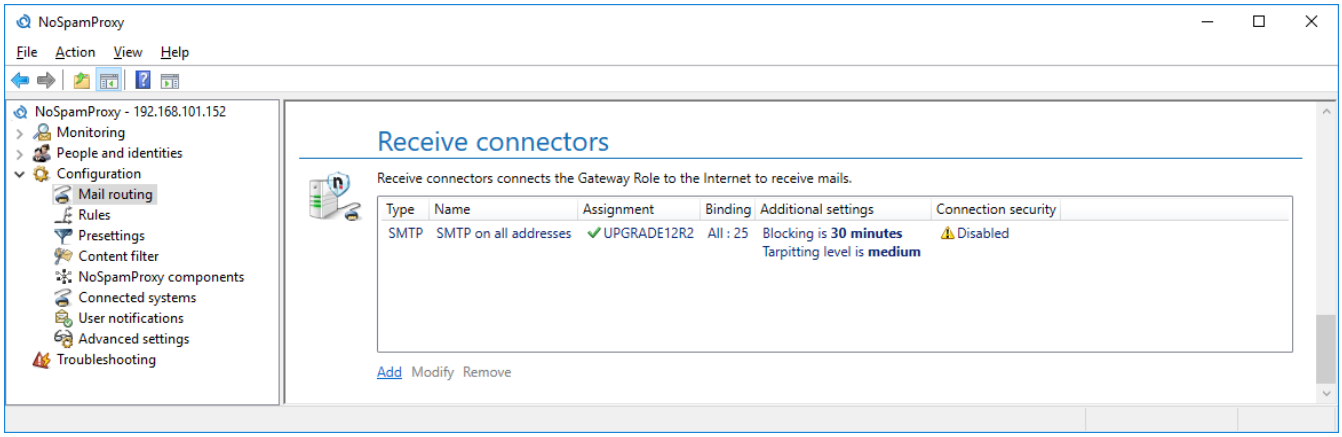


Picture 85: Extended delivery options for the DOI network

When delivering emails via the DOI network, the delivered email is categorized as "not encrypted" in message tracking. In this case, the email is encrypted via the DOI network and is thus bug-proof. This type of validation is not listed under transport security.

Receive connectors

In order to receive emails on different network interface cards but also to meet different security requirements for email traffic, multiple receive connectors can be configured.



Picture 86: Overview of receive connectors

SMTP connectors

The SMTP receive connector defines which IP address and port are used by NoSpamProxy to receive emails. It also determines how invalid requests from external email servers are dealt with and what type of connection security should be applied during the transport of the email.

SMTP settings

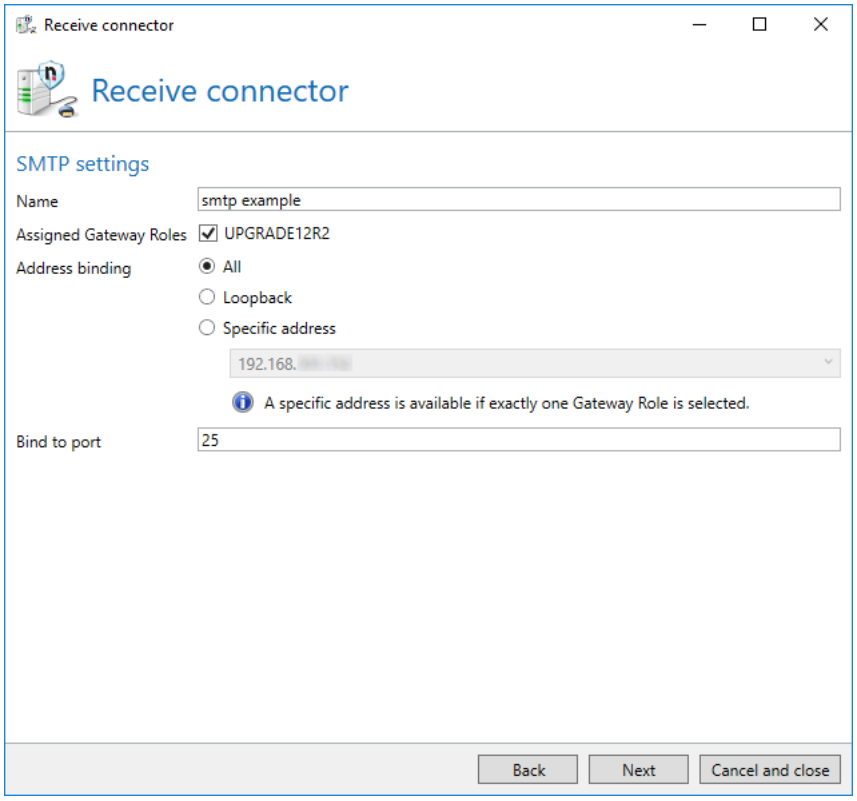
Determine the Gateway Roles of the receive connector, the IP address as well as the port of the connector (Picture 87).

Values entered into **Binding on IP address** define the address used to accept connections.

All selects all existing IP addresses. You can also select specific addresses out of all available mapped IP addresses. For doing so, click on the arrow symbol and select the desired IP address from the drop down list.

If you have selected multiple Gateway Roles, you cannot implement a constant link to individual IP addresses. In this case, select **All** or **Loopback**.

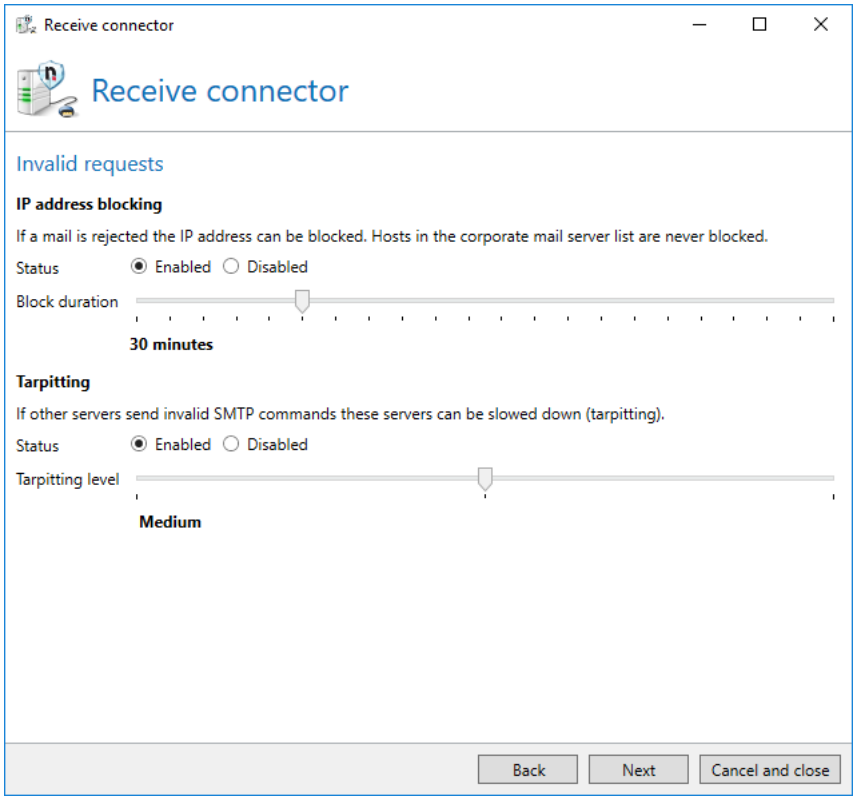
Via **Port**, you can configure the port used by NoSpamProxy to receive emails.



Picture 87: Connection security of an SMTP receive connector

Invalid requests

Some internet users attempt to utilize other email servers by sending invalid requests (so-called 'Denial of Service' attacks) or exploit security gaps to break into that server. To minimise these attacks, you can fend off such requests (e.g. through so-called "tarpitting"). The tab **Invalid requests** (Picture 88) shows the configuration settings for these invalid requests.



Picture 88: Determine the properties on the receipt of invalid SMTP commands

Blocking of IP addresses aims at deliberately outmanoeuvring servers already identified as spam senders. If a server sends an email to NoSpamProxy and classifies it as spam, subsequent emails from the same send server are blocked for the given time period. A regular email sender will retry to deliver the email after this time period, while a spam sender will probably cancel the delivery and concentrate on unprotected email recipients.

Via **Blocking for suspicious IP addresses**, you activate or deactivate the blocking option. Settings made using the slider for the **Blocking period** determines the duration of the blocking starting from 5 minutes up to one day (1440 minutes).

"Tarpitting" is a method which aims to outmanoeuver email relays which do not correspond to the RFC with regard to the SMTP command rules and/or their correct order. As soon as an SMTP command is transferred incorrectly or at the wrong location, NoSpamProxy waits for 5 seconds before responding to all subsequent commands. The transfer of the commands is thus artificially aggravated as if taking the route through a tar pit; hence the name tarpitting.

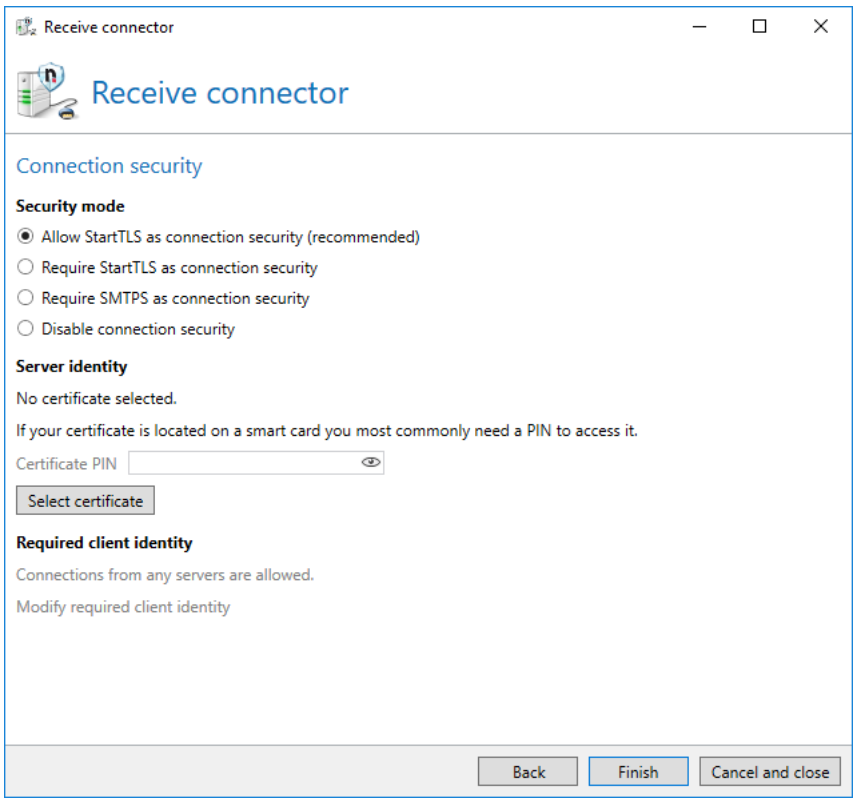
You can activate or deactivate **Allow retarding of bad connections (Tarpitting)** via **Activated** and **Deactivated**. By using the slider for the **Tarpitting level**, you can set the response delay in seconds. If set to 'low', the gateway delays the response by 2 seconds, when set to 'medium', the delay is 5 seconds and when set to 'high', 10 seconds.

Connection security

In the Connection security, the SMTP receive connector uses a Server identity.

If you demand StartTLS or SMTPS as connection security, you can additionally validate the identity of the inbound server (Picture 89). The following settings are possible:

- **Allow connections from each server**
  The identity of the inbound server is not restricted. Emails from all servers are accepted.
- **Require a certificate**
  The certificate to be selected here can either be an end certificate or an intermediate or root certificate. If you select an end certificate, the inbound server must prove its identity with it. If you select an intermediate or root certificate, it must prove its identity with a certificate which has the given certificate in its certificate chain as intermediate or root certificate.
- **Require a trusted certificate**
  The inbound server must prove its identity with a certificate which is deposited as trustworthy in the certificate store of the local computer.



Picture 89: The connection security of an SMTP receive connector

Rules

To process emails, NoSpamProxy applies rules which you can configure individually.

After the installation of NoSpamProxy, you can create a set of default rules after the installation of the licence. They help you get the gateway up and running as quickly as possible and with minimum administration effort. Nevertheless, you should check these rules and, if necessary, adjust them to your needs.

The rules of NoSpamProxy are set up modularly. You can create your own rules and change already existing ones. This is done by selecting the desired filters for each single rule. Within each rule, you can prioritize it with a multiplier and, if needed, configure it.

The filters perform the actual work during the check of the email: They assess to what extent the email meets a specific filter criterion and assign points accordingly. How this point distribution is precisely implemented is explained below. Thus, you can set up your own set of rules with different filter combinations and restrict the rules to certain senders and recipients. This offers several advantages, one being that you can react to spam attacks very individually and flexibly. Not each suspicious email is spam; classification of emails as spam depends on the organization and situation at hand.

If you, for instance, apply a word filter, the term "Viagra" certainly is on your "black" list; you wish to block emails with "Viagra" advertisements. For a pharmaceutical company, however, this term only is a spam criterion to a limited extent. With NoSpamProxy Protection, you can decide yourself whether you add "Viagra" to the word filter; or whether you deploy a word filter at all and if so, to what extent you weigh it with the multiplier.

If, apart from that, an email appears to be legitimate or was sent from a known email sender, the suspicious word might be acceptable under certain circumstances. You can also determine that the rule regarding the word filter only applies 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.

The order of the rules is important. If a rule is responsible for an email to be checked, it is used. If several rules apply to one email, the rule at the very top of the list is applied.

Pos.	Rule name	From	To	Action
1	"General"	*	john.smith@example.com	
2	"Japan"	*.jp	john.smith@example.com	

Rule 1, which is called "General" here, is defined for all emails addressed to john.smith@example.com. Rule 2 named "Japan" on position 2 is also defined for the recipient john.smith@example.com but only considers senders from Japan.

To an email from Japan to "john.smith", both rules apply. However, only the rule "General" is used for assessment since it is at the top of the list. Even if the Japan rule would actually be "more precise" here, the order is the decisive criterion.

To use the rule for "Japan" you have to reorder the rules as shown below. In that case the more special rule is applied first.

Pos.	Rule name	From	To	Action
1	"Japan"	*.jp	john.smith@example.com	
2	"General"	*	john.smith@example.com	

Filters

The individual filters of the corresponding rule are applied to each email. The filters assess the email to be checked and assign minus and bonus points. These points are weighted with the multiplier of the filters and added to a total value. If this value exceeds the set threshold value (SCL) of the rule, the email is rejected. You can set the threshold value for each rule individually.

Information on which filters are available and how they exactly function can be found in chapter Filters in NoSpamProxy.

Actions

Actions for spam check

After the email has been processed and is rejected or passed through based on the filters, the configured actions are invoked. Actions can, among other things, change emails in order to add a footer or delete undesired attachments. However, actions can also reject emails although they would have actually been passed the assessment by the filters. A virus scanner can, for example, reject an email although it had not been identified as spam.

This means that actions are superordinate settings which will overrule filter settings.

All actions are described in detail in chapter Actions in NoSpamProxy .

How NoSpamProxy Protection classifies an email as spam

In the rules you can configure different filters and actions. The filters contained in a rule are the checkpoints which assess the spam character of an email according to certain criteria. The higher the probability for spam, the higher the point result for this e-ail will be. However, if an email is assessed as potentially trustworthy, the result can also become negative. The range of values is -10 to +10 points. You can individually weigh the filters within the rules by using the multiplier. The assessment of the filter is applied against the multiplier. In doing so, you can increase the influence (=point share) of an important filter within a rule.

Based on the calculated total score, a "Spam Confidence Level" (SCL) is determined. An SCL of 0 means that the email was classified as neutral. The higher the value, the more the email was classified as spam. If the value is below 0, the email was classified as trustworthy. If this total weight reaches the threshold value of the rule, the email is treated as spam and rejected.

The following example illustrates the procedure:

You created a rule with an active filter; the word filter. Moreover, the Level of Trust system for this rule is activated. The word filter checks an email for undesired terms.

Assuming that an email contains a large number of undesired terms, the word filter will thus raise the alarm and assign a high minus value for this email, for example, **6**. If the word filter was the only filter in this rule, the email would now be assigned a total value of **6**. If you had set the threshold value to **4** , this email would now be blocked and rejected. The sender would receive a non delivery report.

Moreover, the Level of Trust system is activated in this rule. The email comes from a very reliable email partner with whom you already exchanged many emails. The Level of Trust system assesses this email with **-4** SCL points. The Level of Trust system always contains a multiplier which equals the sum of all multipliers of all activated filters in the rule plus **1**. This amounts to a factor of **2** in our example. The SCL value thus arises from **6+2*-4**. Thus, an SCL of **-2** emerges. The email would pass NoSpamProxy Protection.

This example already hints at the possibilities offered by the modular setup of the rules and the importance of the filter weighing. SCL calculations are described in detail in chapter Calculating the Spam Confidence Level.

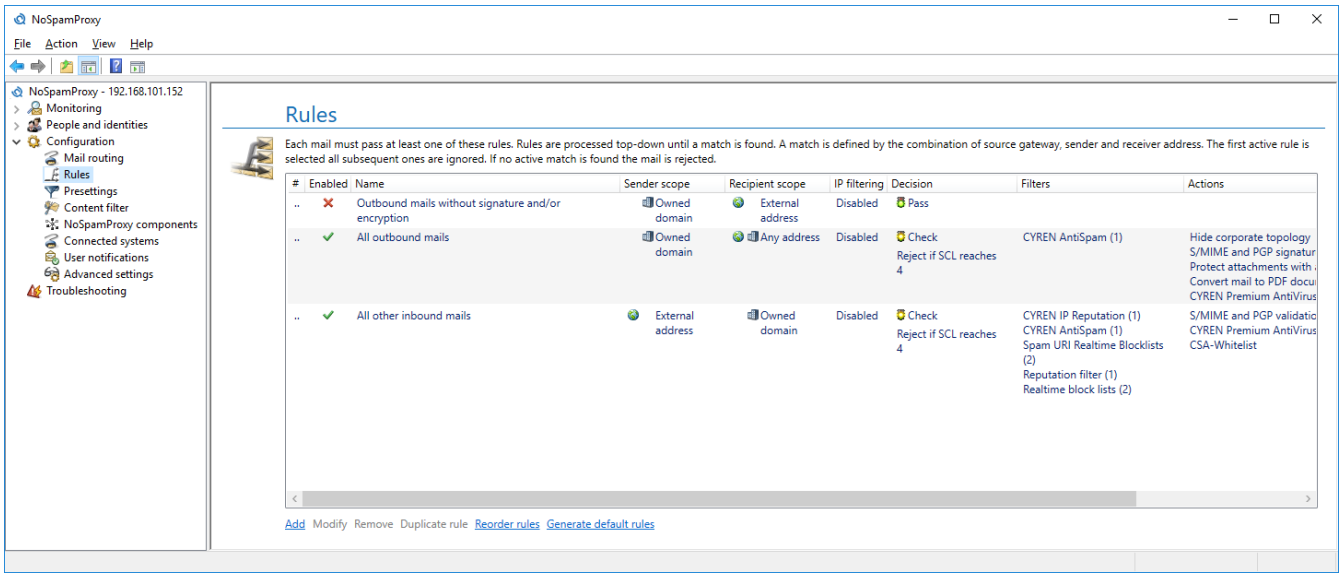
Another example is the following case:

An email is sent from a system listed on a blocking list (RBL). Most filter products would categorically reject such a connection without detailed analysis. With NoSpamProxy Protection, however, you can relativise this decision. If the email is, for example, a reply , the Level of Trust filter can overrule the assessment. This results in the email from this provider not being blocked but delivered.

However, emails from a different unknown sender which misuses this unsafe server cannot pass.

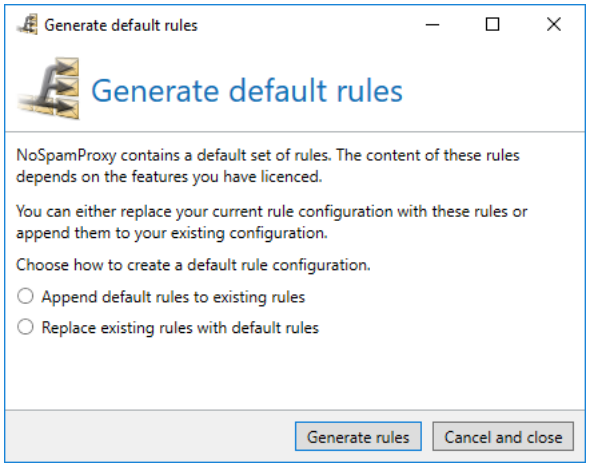
Configuration of rules

The rules that determine how emails are processed are managed under **Rules** (Picture 90).



Picture 90: Overview of all rules which determine the processing of e-mails

After a NoSpamProxy clean install the rules list is empty. In this case default rules can be created by clicking **Generate default rules** (Picture 91). The function for generating default rules is also available at a later point in time, e.g. in case you wish to supplement or replace your own rules with/by the default ones. When supplementing, the default rules are located behind the existing ones and their order can be changed afterwards, see Reorder rules.

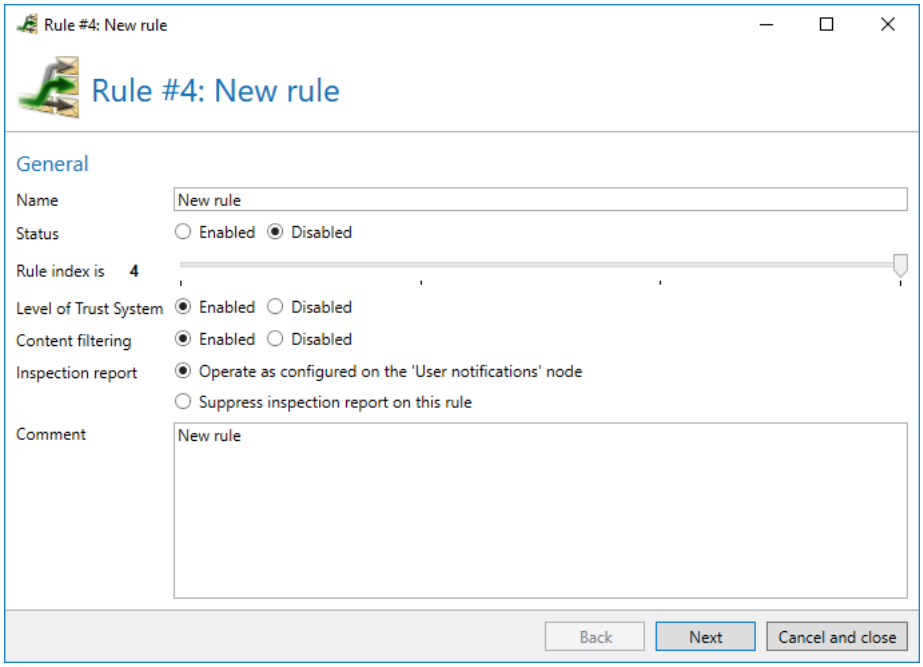


Picture 91: Generate default rules

Create new rule

A rule contains the following settings: **General**, **Email flow**, **IP filtering**, **Filters**, **Actions** and **Reject behaviour**. Which rule is applied to an email is determined by the settings made on the tabs **Email flow** and **IP filtering**. The other tabs determine how the emails are processed.

The first tab (Picture 92) contains important parameters used to determine basic settings.



Picture 92: General settings of the rule

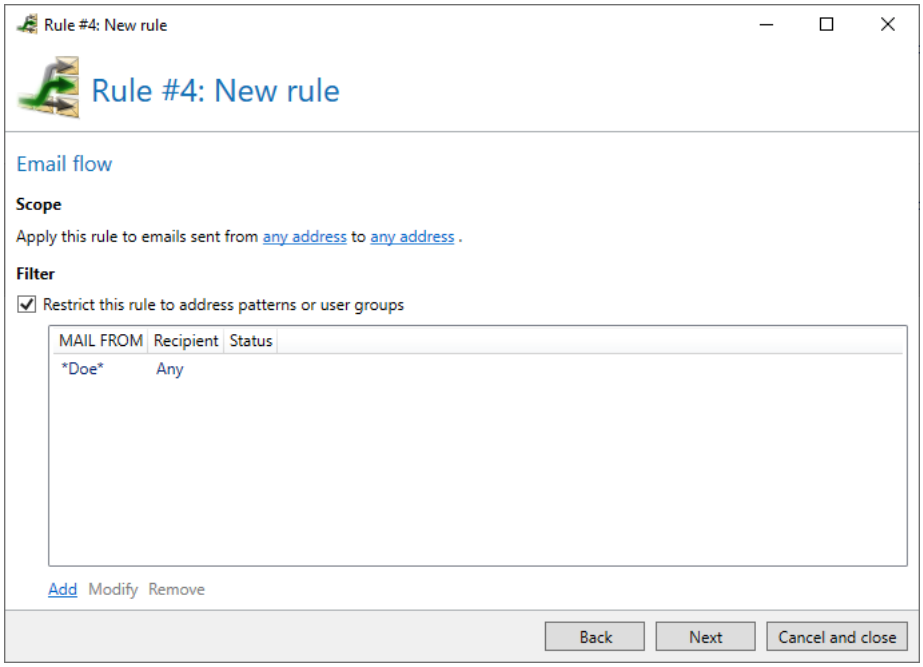
First, enter a unique for the rule in; the name should be able to help you keep track of the rule in the rule summary. Under **Status**, state whether the rule is activated or deactivated. The **Index** determines the hierarchy of the respective rule.

The option **Level of Trust system** activates or deactivates the Level of Trust system for this rule.

The option **Content filter** enables or disables the Content filter for this rule.

Under **Comments** you can add a comment. The comments have no impact on the definition or function of a rule; they only serve documentation purposes.

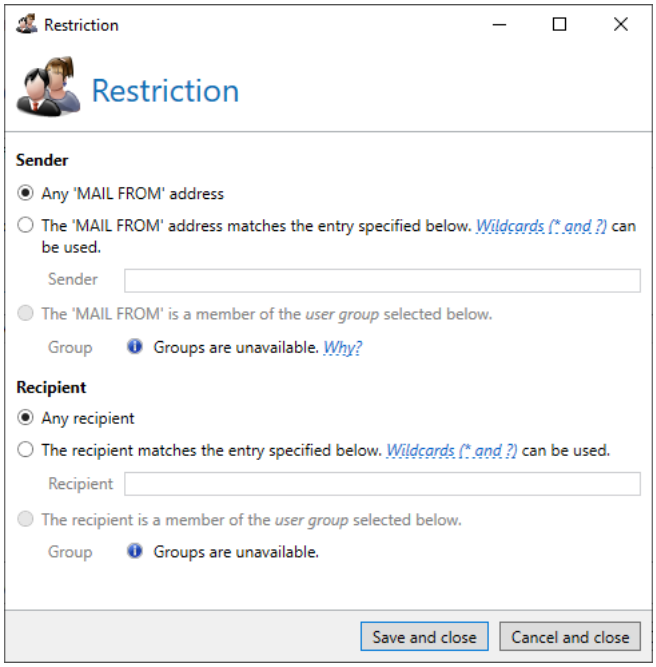
On the tab **Email flow**, you restrict the rule to specific senders and receivers (Picture 93).



Picture 93: Define the addresses to apply this rule to.

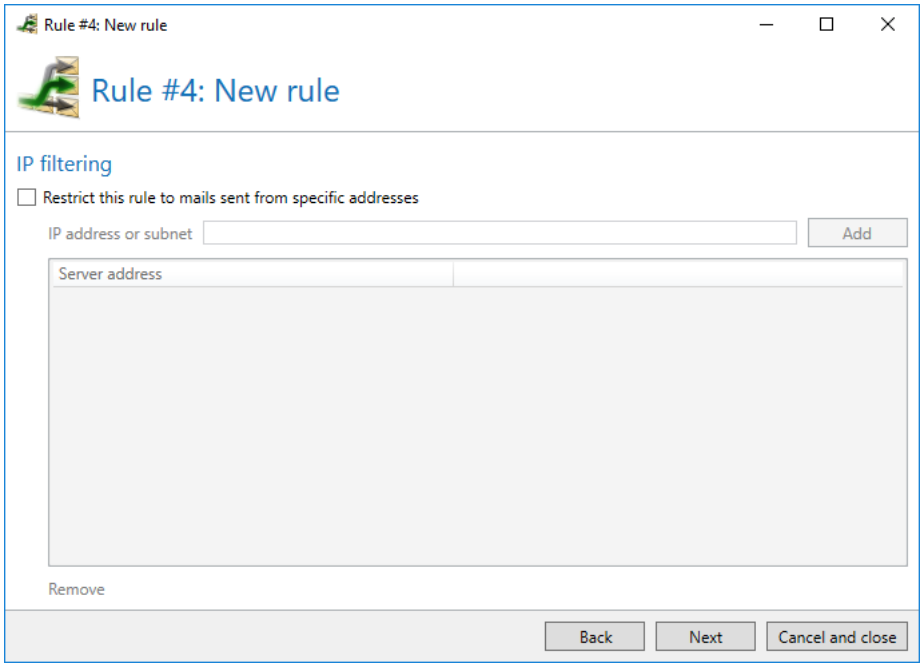
Under **Scope**, you select the senders and receivers this rule should be applied to. Moreover, you can restrict the rules by adding one or more **Filter entries**. Here, you can use address patterns or user groups(Picture 94).

To receive groups from a user directory, you must configure an automatic user import from LDAP or Active Directory users under 'Domains and users'. Groups are available after the initial synchronisation.



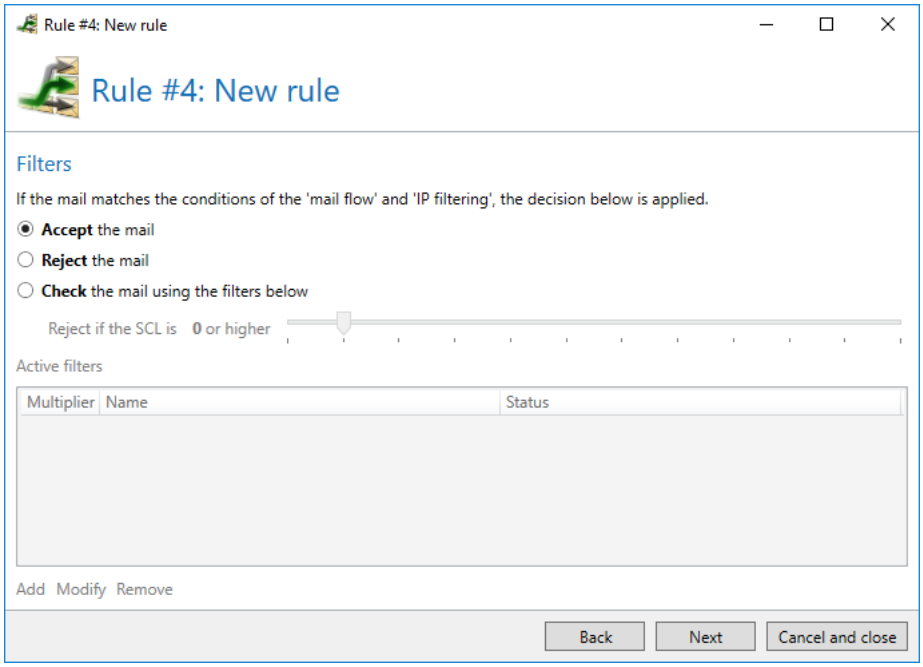
Picture 94: Configuring a filter entry within a rule

You can restrict the rule to certain inbound servers in the tab **IP filtering** (Picture 95).



Picture 95: Defining the validity of the rule with regard to the inbound server

On the tab **Filters**, you activate the desired filters for a rule (Picture 96). The filters, however, can be weighed differently with multipliers and thus increase or decrease their effect.



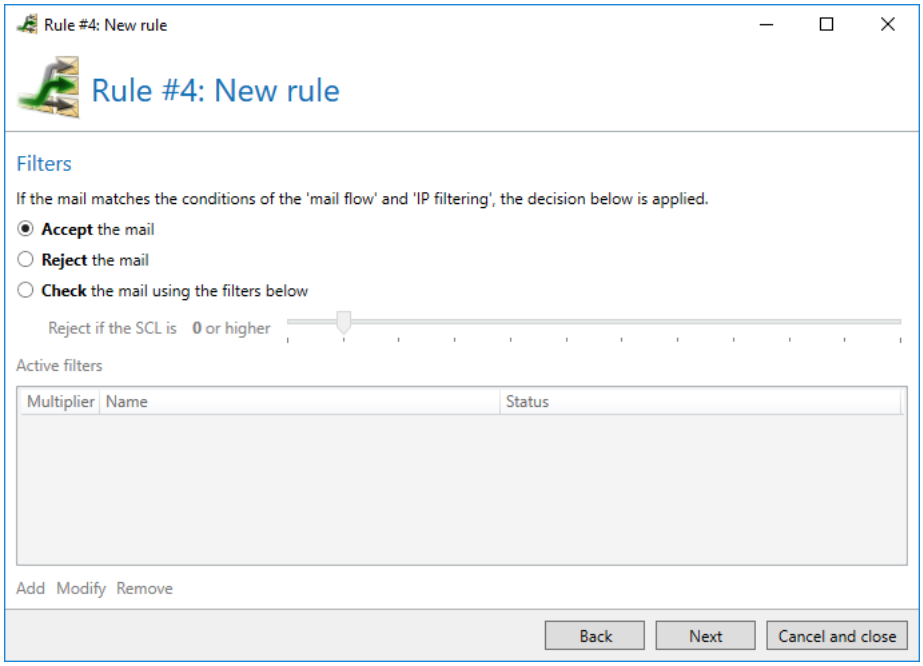
Picture 96: Determining the filter settings of the rule

Set the **Filter setting** to **Reject**, if all emails which are processed by this rule should be rejected without being checked. Select **Accept**, if all emails of this rule should be delivered without being checked. With **Check**, the Spam Confidence Level (SCL) of each email is checked and rejected as spam when reaching the set value. An SCL value of "1" means that emails are rejected as soon as any indication of the email being spam appears. An SCL value of "10" only rejects emails with a high spam indication level.

Only if you have selected the filter method **Check**, you can select the filters to be applied. This can be done under **Active filters**. To activate one or more filters for a rule, click on **Add filter**. A dialog opens in which you can select the desired filter (Picture 97). Depending on the filter, another specific configuration dialog opens in which you can configure the filter. Next to the filter name, you will find sliders via which you can set the multipliers. The value "5" means that the filter is weighed five times as much as a filter with the value "1".

Some filters are not functional for the sender selected in the rule. At this point, the text **Cannot be applied to rules for local (or external) senders** appears in the column **Status**. These filters cannot be added; rules with invalid filters cannot be saved either.

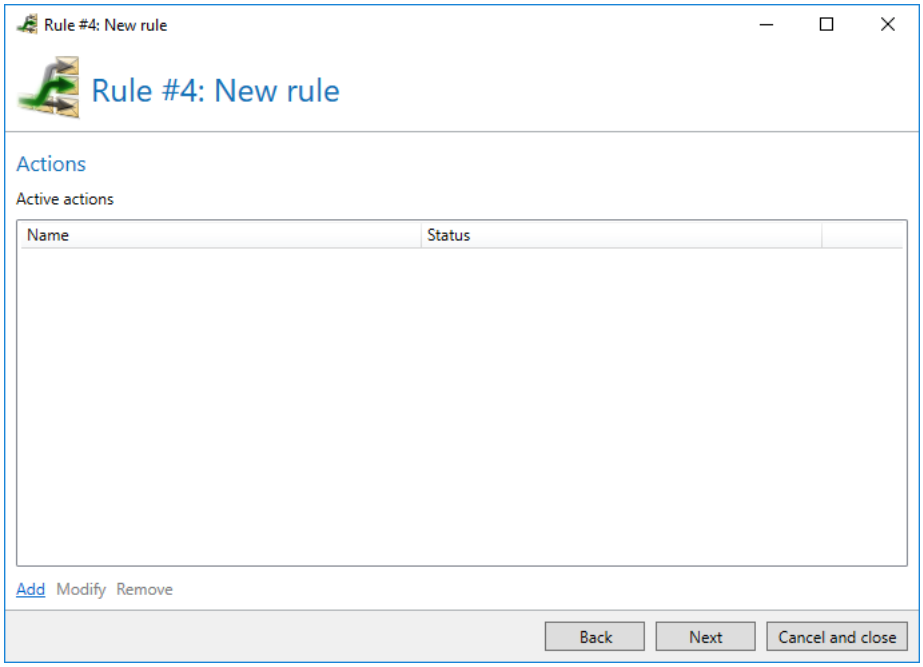
The addition of a filter to a rule caused by the direction is only prevented if it does not show any function for this direction. This restriction does not always constitute the recommended deployment. This means that filters which are intended for a certain direction but also function in the opposite direction are thus configurable for both directions. The recommended direction, however, is sometimes indicated in the name of the filter.



Picture 97: Add an available filter to your rule

Actions are executed on each delivered email whether checked or not. You can decide on this tab which actions should be executed in the rule and how these actions are configured in the rule. Actions are always executed even if the emails are not checked by filters.

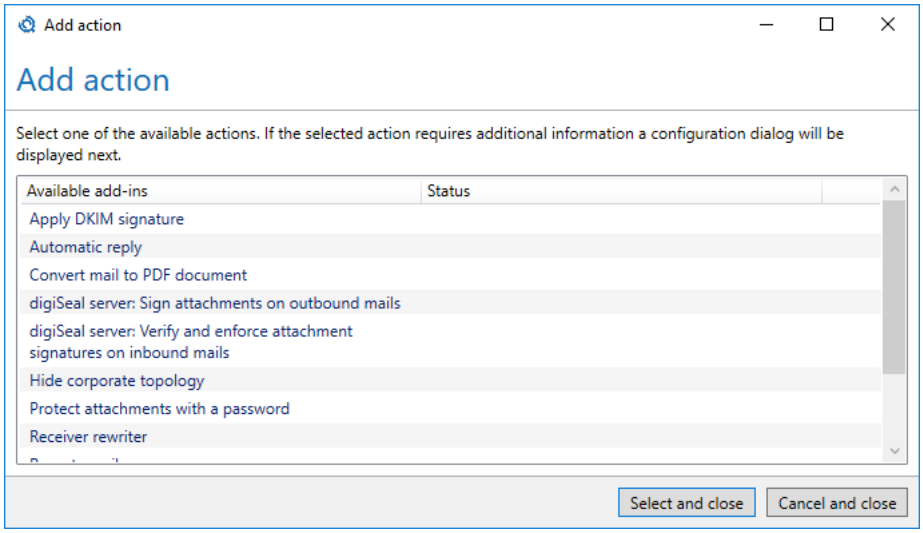
The active actions in the rule are shown in the list **Active actions** (Picture 98).



Picture 98: The actions of an email

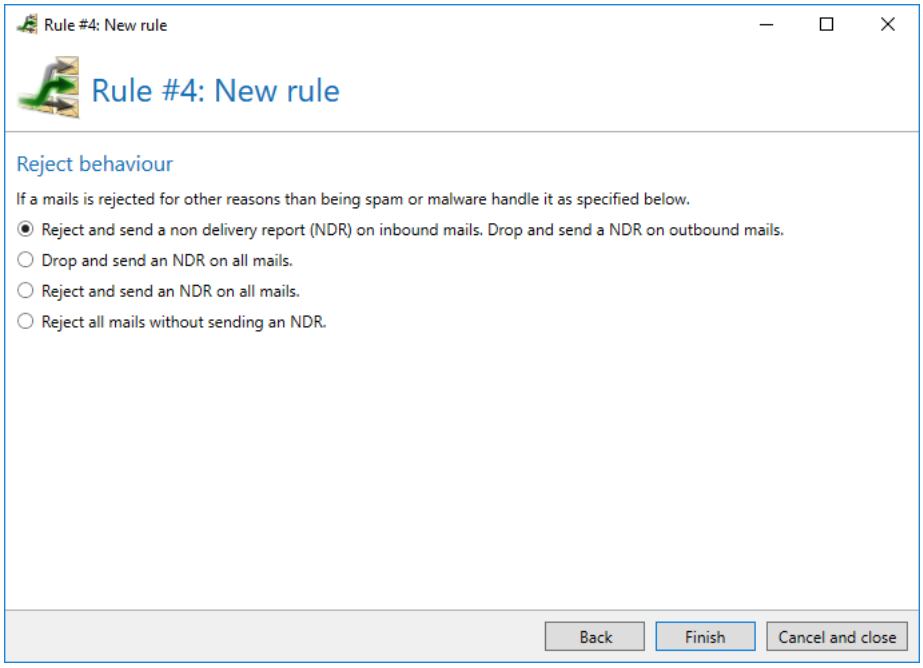
Via **Add**, you can add actions to the rule. Depending on the selected action, you must configure it before it is added to the list of actions. (Picture 99). Some actions are not functional for the sender selected in the rule. If so, the column **Status** contains the text **Local (or external) senders supported only**. These actions cannot be added; rules containing invalid actions cannot be saved either.

The addition of an action to a rule based on the sender is only prevented if it does not show any function for this direction. This restriction does not always constitute the recommended application. This means that actions which are intended for a certain direction but also function in the opposite direction are configurable for both directions. The recommended direction, however, is in some cases indicated in the name of the action.



Picture 99: Actions from this list can be added to a rule

On the next tab you can configure settings for the **Reject behaviour**. If an email does not meet the rules set by you for dispatch or receipt, the properties configured here are applied. Rule violations emerge, for instance, if email encryption failed or invalid attachments to emails were found.



Picture 100: Properties for Reject behaviour

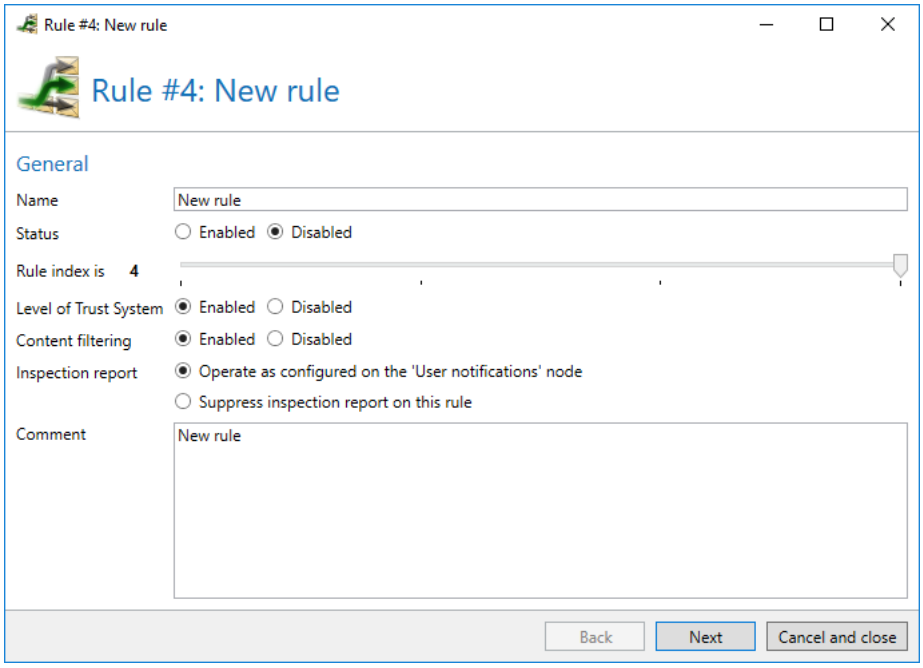
The following options are available to you: To **Reject** an email means that the server rejects acceptance (SMTP prompt 5xx). Thus, the inbound server needs to generate a non-delivery report (NDR). To

Drop means a positive acknowledgement by the receiving server to the inbound server (SMTP prompt 200) without any further processing of the received email. Since the email is directly deleted after the acceptance, NoSpamProxy will generate a non-delivery report and send it to the sender of the email.

Reorder rules

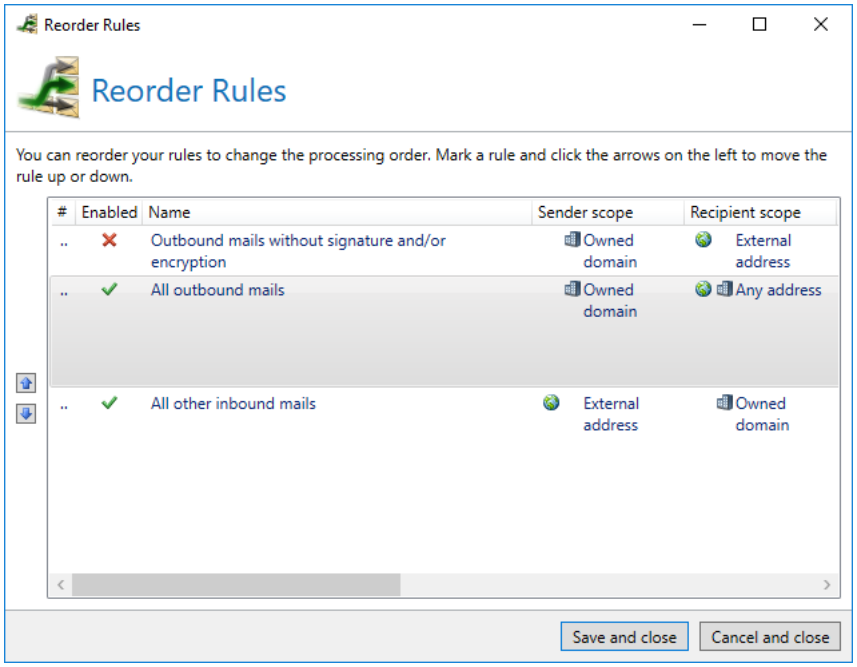
After completing the rule editor, the new rule appears in the rules list. The position in the list corresponds to the index you determined on the tab **General** of the rule editor.

To change the position of a rule, open the configuration for the rule and set the new position via the setting **Rule index**.



Picture 101: Via the slider for the "Rule index", you can change the position of the rule

Alternatively, you can click **Reorder rules** below the list with the rules (Picture 102).



Picture 102: Here, the order of all rules can be changed simultaneously

Unsupported scenarios

Enforcing automatic encryption results in emails not being delivered to the recipient if all the factors listed below are present:

- An S/MIME certificate for the recipient is available.
- The email is sent as a PDF Mail from the Outlook Add-In.
- For PDF Mail, the option **Convert email to PDF and protect it wih a password** is selected **or** the email is converted into PDF by using the subject flag **[PDF]**.

Filters in NoSpamProxy

Filters assess emails and thus influence the Spam Confidence Level (SCL) of emails. Consequently, the decision can be made whether an email is rejected in case the examination result exceeds a certain SCL value.

Cyren IP Reputation

Valid for the following senders: **External**.

Default SCL value for a multiplier of one is **3** for a "bad" reputation and **1** for an "unknown Sender".

This filter checks the reputation of the sending IP address by using the service of Cyren to boost the spam detection rate of NoSpamProxy further. If the reputation is "bad" or the sender is unknown, the

respective SCL points are assigned (see above). The filter has no settings of its own but you can adjust the filter result by using the multipliers.

Cyren AntiSpam

Valid for the following senders **External** and **Local**.

Default SCL value with single multiplier is **4**.

The "Cyren AntiSpam" filter creates a fingerprint of the email to be checked based on defined criteria and compares it to fingerprints known to the Cyren Detection Center. If it is recognised (or 'known'), this means that Cyren classifies the email as a spam email. The "Cyren AntiSpam" filter will consequently assign 4 SCL points. The filter itself does not contain any further settings options. The administrator can only exert further influence on the filter result via the weighing using multipliers.

The Cyren service supports malware scans with a file size up to 50MB. Archives, for example ZIP archives, are decompressed if possible and all of the files are scanned individually. The limit of 50MB for archives refers to the size of each decompressed file.

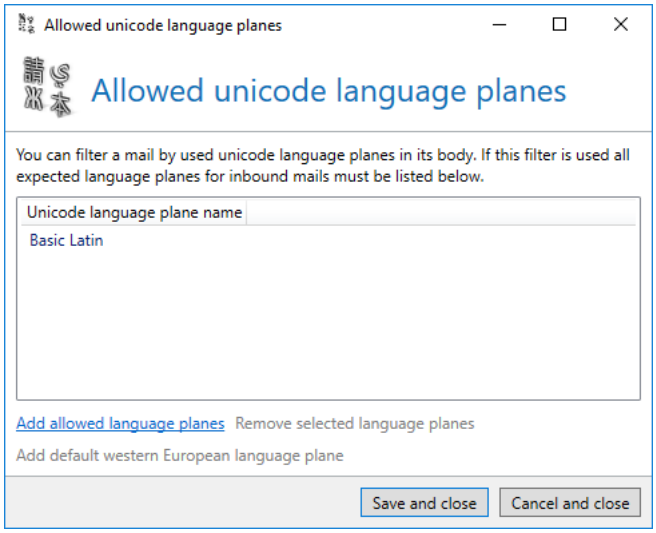
Allowed Unicode language planes

Valid for the following senders: **External** and **Local**.

Default SCL value with single multiplier is **4**.

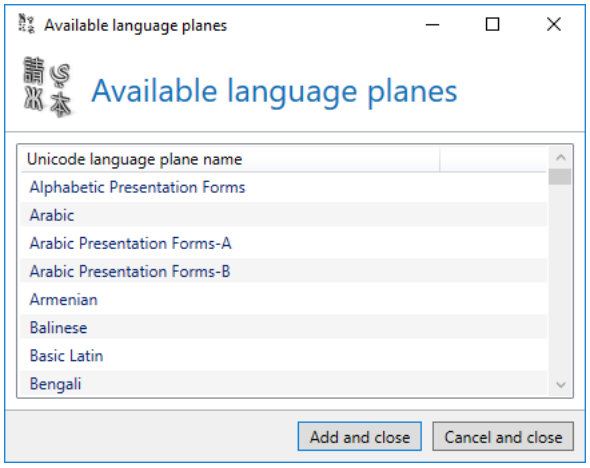
Emails containing spam sometimes come from language areas with which communications occurs only rarely. For example, incoming spam might contain Chinese characters. This filter can block emails by analysing all character sets contained and only letting pass the email if all character sets contained have been explicitly allowed by you.

Add the filter **Allowed Unicode language planes** to your rule. The dialog for the configuration opens (Picture 103).



Picture 103: The list of the allowed Unicode language planes

Now, add all language planes which can be used in incoming emails to the allowed language planes. To do so, select **Add allowed language planes**. A dialog with all language planes which have not yet been allowed appears (Picture 104).



Picture 104: The list of the available Unicode language planes

If you only communicate with Western Europe or America, the language plane for western European languages usually suffices. You can add it, if it is not yet contained in the list of the allowed languages, via **Add default western European language plane** to the list.

Realtime block lists

Valid for the following senders: **External**.

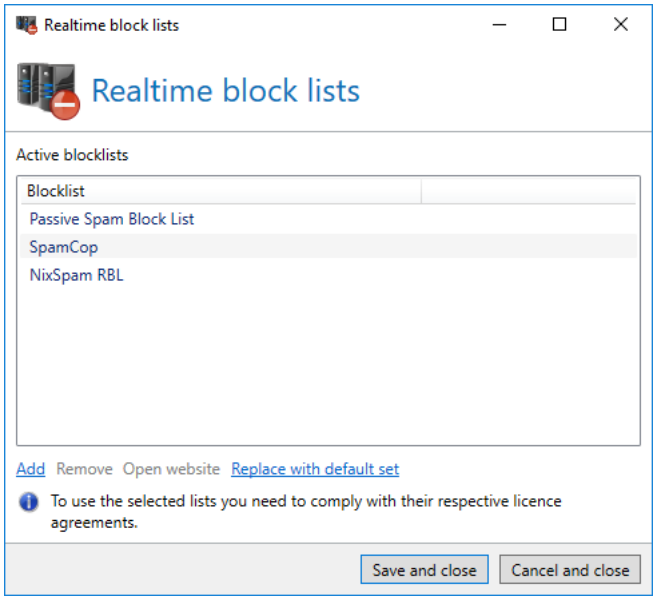
Default SCL value with single multiplier depends on the lists selected in the filter. The SCL points set in the list are assigned per hit.

The filter "Realtime block lists" checks whether an address entry is available in realtime block lists. You can select several different block lists. Since even the best lists might contain false positives, you should always use several lists. As each hit is evaluated as a minus point, the risk for an email to be immediately blocked through a "false positive" based on a single blocklist is minimised.

Add the filter **Realtime block lists** to your rule. The dialog for the configuration opens (Picture 105).

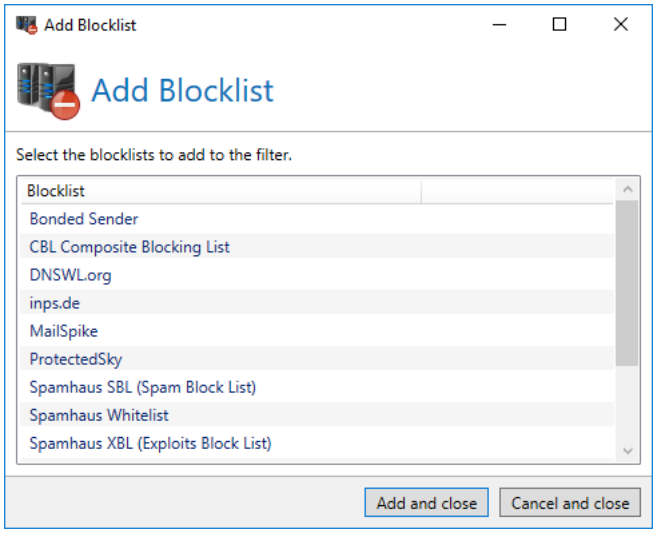
For the filter **Realtime block lists**, you can determine which block lists are used. Similar to the filter **Word matching**, the individual lists are globally preconfigured in the menu **Presettings** and must only be selected in the filter.

Via **Replace with default set**, you can replace the currently selected lists by lists recommended by Net at Work.



Picture 105: Add all blocklists which should check the IP addresses of incoming emails

Click **Add** to select the blocklists to be scanned by NoSpamProxy Protection during filtering. The dialog **Realtime block lists** opens. (Picture 106). Select the desired blocklist/s and click **Add**. The previously selected lists appear in the overview of the realtime block lists.



Picture 106: You can select from all defined blocklists

To remove one or more lists, select the entries to be deleted and click on **Remove**.

Keep in mind that the removed lists are only removed from the rule just edited. The lists still appear in the Presettings.

In order for the DNS requests to function correctly you must properly configure the DNS settings of the operating system. The server must be able to resolve external domains. It may be useful to install an own DNS server as forwarder.

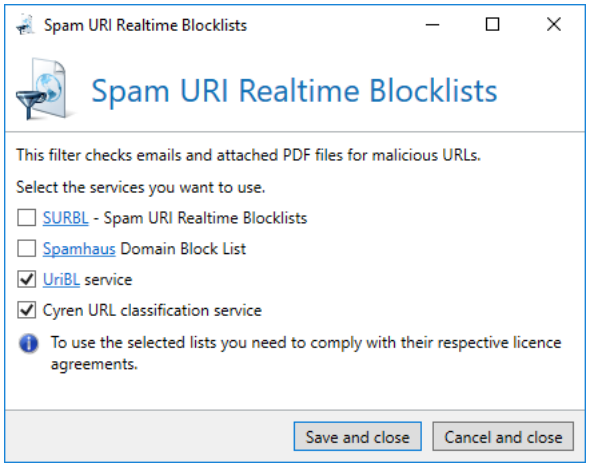
Spam URI Realtime blocklists

Valid for the following senders: **External** and **Local**.

Default SCL values with single multiplier depends on the lists selected in the filter. **2** SCL points are assigned per hit of a list.

Spam URI Realtime blocklists manage lists with suspicious spam URLs. It is possible to check via the internet whether a URL is possibly contained in this list or not.

The "Spam URI Realtime blocklists filter" analyses links contained in emails and PDF documents and checks whether a corresponding entry is available in these lists. Moreover, it searches for addresses which start with "www." and do not appear as links in emails or PDF documents.



Picture 107: Configure the spam URI Realtime blocklists filter

You can select several different blocklists (Picture 107).

Similar to the realtime blocklist filter, DNS requests must function correctly. The server must be able to resolve the given service. It may be useful to install an own DNS server as forwarder.

The Cyren URL Classification Service analyses URLs and categorises them. Malicious links are assigned to one of the following categories:

- Malware
- PhishingAndFraud
- Compromised
- CriminalActivity
- Botnets
- IllegalSoftware
- ChildAbuseImages
- SpamSites
- ParkedDomains

SpamAssassin connector

Valid for the following senders: **External** and **Local**.

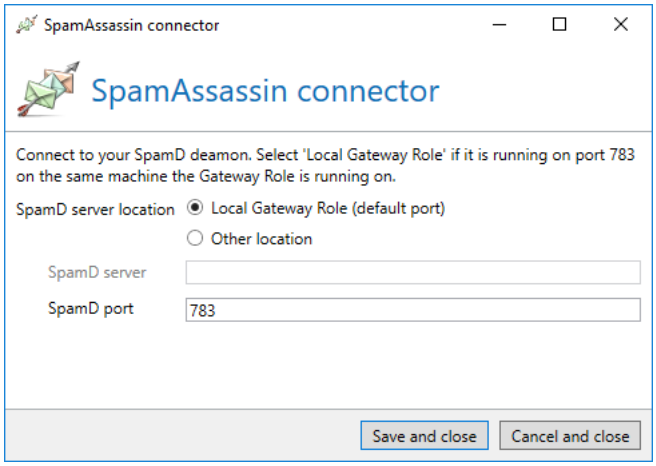
Default SCL value with single multiplier depends on the **Return value** of the SpamAssassin Daemon.

SpamAssassin is a free spam filter which contains different pre-defined tests to classify messages. Many of these tests, such as RBL, are executed by NoSpamProxy Protection itself at an earlier point in time already and more effectively. However, it might be interesting to integrate the remaining rules of the filter.

SpamAssassin assesses a message and adds the result to the header of the message. It consists of server (SpamD) and client (SpamC). The filter of NoSpamProxy Protection acts as SpamAssassin client (SpamC) and functions only in connection 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. The operation on the same server as NoSpamProxy is also possible.

Add the filter **SpamAssassin connector** to your rule. The dialog for the configuration opens (Picture 108).



Picture 108: Defining the connection to the SpamD server

As for the SpamAssassin connector, you can set the IP address or the Full Qualified Domain Name (FQDN) of the SpamD server. The default port of the SpamD server is "783" and can be changed if your SpamD accepts on connections on another port.

With the setting **SpamD server name**, you can initially determine whether the SpamD server is located on the same client or on a remote client.

Under **SpamD server**, you can give the IP address or the DNS name of the SpamD server. Under **SpamD port**, you can give the port number of the SpamD server. By default, the SpamD server accepts the connections on the port number "783".

Please ensure that NoSpamProxy can actually connect to the requested system. Often, port filters, IP routing and firewalls need to be configured in order that NoSpamProxy Protection can actually reach the SpamD server.

Reputation filter

Valid for the following senders: **External**.

This filter executes different tests on the email envelope, the content of the email and the headers . Through some of the tests, DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) are analysed as well. For each test, individual SCL points can be assigned in order for you to be able to adapt the assessments to the requirements of your company. The following tests are available:

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.

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 DNS. If this assignment is not possible, this indicates an attempt at misuse.

Suspected dynamic address

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. This often occurs with infected computers acting as spambots.

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.

SPF failed

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.

DKIM failed

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. This test only awards points if no DMARC policy (see below) is active.

DMARC result 'quarantine'

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 DKIM and SPF. The amount of points awarded depends on the DMARC result applied.

DMARC result 'reject'

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. The amount of points awarded depends on the DMARC result applied.

Address is not aligned

Checks whether the 'MAIL FROM' domain and 'Header-From' domain are identical ('alignment'). This test only awards points if no DMARC policy is active.

Invalid angle brackets (Header-From)

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 specified in the header form contains a corporate domain. If this is the case, it indicates identity theft, since this filter can only be used for inbound emails, which is why this email must be an external email. 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 Corporate email server.

Corporate domain in display name

Checks if the display name contains 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.

Subdomain of a corporate domain in email address

Checks whether a subdomain of a corporate domain used. If this subdomain is legitimate, the filter 'Corporate domain in email address' is applied.

Subdomain of a corporate domain in display name

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.

Obfuscated corporate domain in email address

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 (homographic attack).

Obfuscated corporate domain in display name

See filter '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 (homographic attack). Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name.

Subdomain of an obfuscated corporate domain in email address

See filter 'Subdomain of a 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 (homographic attack).

Subdomain of an obfuscated corporate domain in display name

See filter '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 (homographic attack). Domains in the display name are used by spammers because many mobile devices and email applications initially display only this name.

Multiple email addresses

Checks whether the 'Header-From' contains more than one email address, which is not RFC compliant. Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.

Domain in display name different from email address

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.

Invalid '@'

Checks if the 'Header-To' contains an '@' character that is not part of an email address, which is not compliant with RFC 5322. Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.

Invalid angle brackets (Header-To)

Checks if the 'Header-To' contains angle brackets with an invalid email address, which is not compliant with RFC 5322. Lack of RFC compliance indicates spam, as spammers may be less concerned with ensuring such compliance.

Missing 'Header-To'

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.

Missing corporate email address

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.

Word matching

Valid for the following senders: **External** and **Local**.

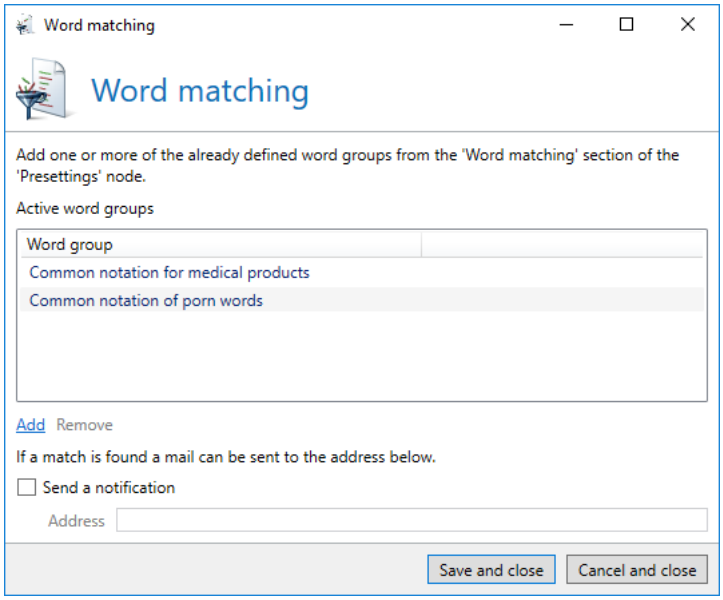
The default SCL value with single multiplier depends on the word groups selected in the filter. The SCL points set in the word group are assigned per hit.

With this filter, you can identify pre-defined words and terms in the subject line as well as in the email body and evaluate them with positive or negative SCL points. Each occurrence or, depending on the setting, each lack of such a term in an email is evaluated only once with the points set in the filter.

If one or more word/s is found in the configured word groups, an optional email with a notification can be sent to a local mailbox. This email contains the sender of the email, the recipient, subject and the words found.

The word groups available in this filter are previously defined under Presettings.

Add the filter **Word matching** to your rule. The dialog for the configuration opens (Picture 109).



Picture 109: Add your defined word groups to the filter of the word matches

Now you can add add previously created word groups via **Add word group**. Several word groups are already preconfigured. Select the desired word group/s and click **Add**. In the overview of the dialog for the word matches, the selected word groups appear.

Actions in NoSpamProxy

Actions can change emails

An action contains information on the filter result and can subsequently execute further tasks. In contrast to the filters, actions can change the emails; for example, sort out attachments due to a detected virus. Moreover, actions can overrule filter results. Examples for this are virus scanners and a greylisting action.

To activate an action, you must select the tab **Actions** in the rule that should contain this action. Click on **Add**. The dialog **Add** appears in which you select the action to be added and click on **Select and close**. Now, the action is added or, if it has to be configured, the configuration of the action opens and the action is added to your rule afterwards.

Receiver rewriter

Valid for the following senders: **External** and **Local**.

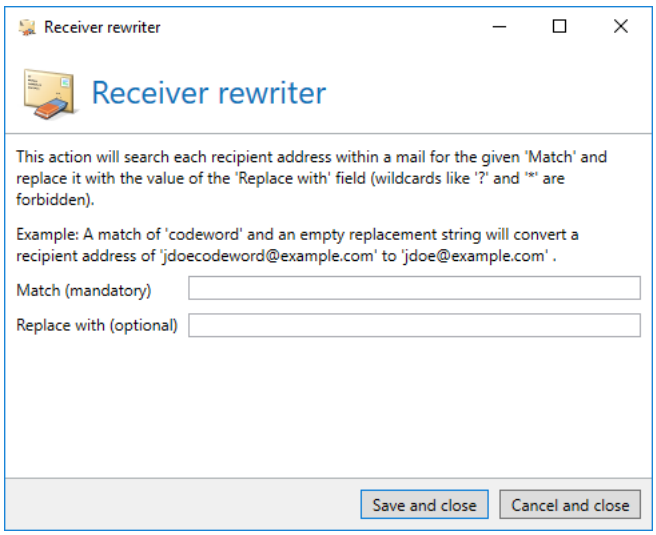
This action enables you to change the target address during the receipt of an email. In doing so, you can, for example, after a change of name of the company, rewrite all emails addressed to the former address to the new one.

A second application scenario is the definition of a "secret address". You can determine that all emails with an entry *secret* in the address field are classified as desired and thus delivered without performing a check. A rule could be as follows:

Pos.	From	To	Decision	Action
1	*@*	*secret@example.com	Pass	Receiver rewriter

The receiver rewriter removes the "code" word and forwards the email to your correct email address. The "code" word in the address can of course be set by you and can be changed again if required.

Add the action **Receiver rewriter** to your rule. The dialog for the configuration opens (Picture 110).



Picture 110: Configure the replacements on the recipients' addresses of the emails

You can set which part of a **"Code" word address** should be replaced by a part of the correct address.

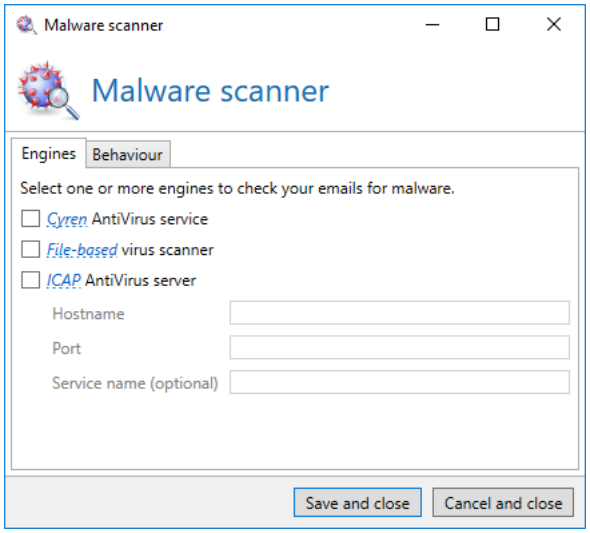
In the settings of the **Receiver rewriter**, you enter the string from the "secret" address which is to be replaced and for which the address manipulation should become active under **Match**.

Under **Replace with**, you enter by which text the text from the field **Match** should be replaced.

As an example, it may make sense to replace the string "topsecret" in the "secret" address "user1topsecret@example.com" by an empty string for the correct address "user1@example.com" .

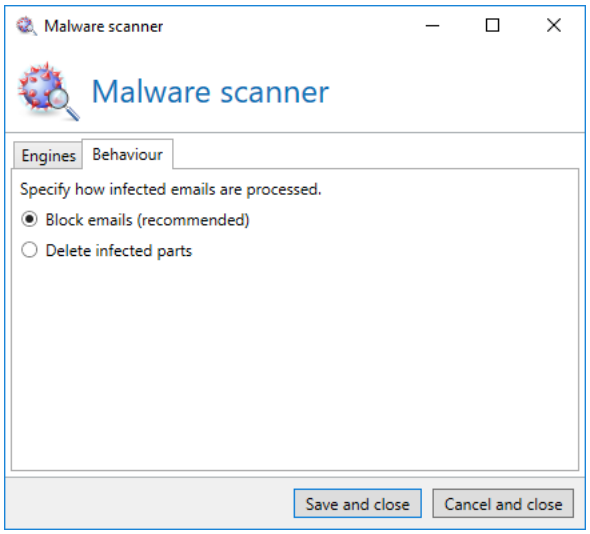
Malware Scanner

The action **Malware Scanner** comprises three engines which can be used individually or in combination with each other. See below for details on the individual engines.



Picture 111: Engine selection

On the tab **Behaviour** you determine how emails are processed in case on or more engines has detected malware.



Picture 112: Determining the behaviour

Cyren AntiVirus

Valid for the following senders: **External** and **Local**.

Regardless of the filter results, the "Cyren AntiVirus" action creates a fingerprint of the email to be checked based on determined criteria and compares it to the fingerprints of the Cyren Detection Center

in the Internet. Should the fingerprint be known, this means that Cyren classifies the email as virus email. Additionally, the entire email is checked with locally available pattern files on all known viruses.

The Cyren service supports malware scans with a file size up to 50MB. Archives, for example ZIP archives, are decompressed if possible and all of the files are scanned individually. The limit of 50MB for archives refers to the size of each decompressed file.

File-based virus scanner

Valid for the following senders: **External** and **Local**.

Viruses are, along with spam, a huge threat and should also be sorted out as soon as possible. While searching for viruses filters may mistakenly remove emails. Most products delete these kinds of emails without notifying the recipient or sender. The difficulty is comparable to a quarantine directory of a conventional solution. NoSpamProxy Protection, in contrast, works differently.

The action "File based virus scanner" stores email attachments coming through to a specific directory. If you have installed any on-access virus scanner, this scanner will deny read access to possibly infested attachments. NoSpamProxy Protection checks whether access is possible or not immediately after the storage of the attachments to the directory. Attachments which can be accessed are considered virus-free. NoSpamProxy Protection can cooperate with any other virus scanner which monitors file accesses in real-time. This scan method is preinstalled on many servers, reliable and performs very well.

Attachments from emails in RTF format can also be processed by virus scanners. The attachments, which are named winmail.dat by default, are checked and, if necessary, individually blocked. Keep in mind that this type of processing constitutes a modification of the email.

The directory to temporarily save the files is in current installations `%ProgramData%\"Net at Work Email Gateway\Temporary Files \Netatwork.NospamProxy.Addins.Core.Actions.FileVirusScanAction"`. Older installations may save the file the file to the installation directory of NoSpamProxy in the folder `"\AntiSpam Role\Temporary Files \Netatwork.NospamProxy.Addins.Core.Actions.FileVirusScanAction"`.

Simultaneously operating on-access virus scanners and the integrated Cyren Antivirus may result in errors or issues. These are caused by the fact that virus scanners may assess files produced by and required for the operation of Cyren Antivirus as harmful. Accordingly, these files are deleted or blocked. To avoid this, make sure to exclude the directories `C:\ProgramData\Net at Work Mail Gateway\Cyren` and `C:\ProgramData\Net at Work Mail Gateway\Temporary Files\MailQueues` as well as `C:\ProgramData\Net at Work Mail Gateway\Temporary Files \MailsOnHold` from all scanning actions. This applies to all systems which have a Gateway Role or a Web Portal installed. Keep in mind that the directories mentioned may be hidden directories.

You can determine whether attachments are only deleted or if the corresponding email should automatically be blocked.

If an email is rejected, the sender is notified by the inbound server. In case an attachment is deleted, neither the sender nor the recipient are informed.

As for all virus scanners, password-protected ZIP files are not checked.

ICAP Antivirus Server

The Internet Content Adaptation Protocol (ICAP) is a protocol used for forwarding of content for HTTP-, HTTPS- and FTP-based services. An ICAP-Server receives files which can then be processed, for example by a server-based virus scanner.

If you select the action **ICAP Antivirus Server** NoSpamProxy acts as an ICAP client. NoSpamProxy sends the data to your ICAP server which will check the data. The result is sent back to NoSpamProxy. Depending on the configuration of NoSpamProxy, specific actions are taken.

Access to an **ICAP Antivirus Server** is required for this action.

CSA-Whitelist

Valid for the following senders: **External**.

Often, newsletters are welcome as their contents are delivered with the recipient's consent. The problem with newsletters is that their receipt cannot be ensured since no Level of Trust entry has so far been created automatically and entering all trustworthy newsletter senders as trusted Partners would result in excessive effort.

The CSA Whitelist is a positive list created by a control committee monitors the legitimacy of the newsletters sent. As a result, newsletters from senders not listed on the CSA Whitelist can be delivered safely.

If the sender of an email is on the CSA-Whitelist, the CSA Whitelist action marks the email as trustworthy. Thus, all filters of the applied rules are skipped.

Add the action **CSA-Whitelist** to your rule. It appears in the action overview of the rule.

The configuration of the action is can be edited under Connected systems.

Greylisting

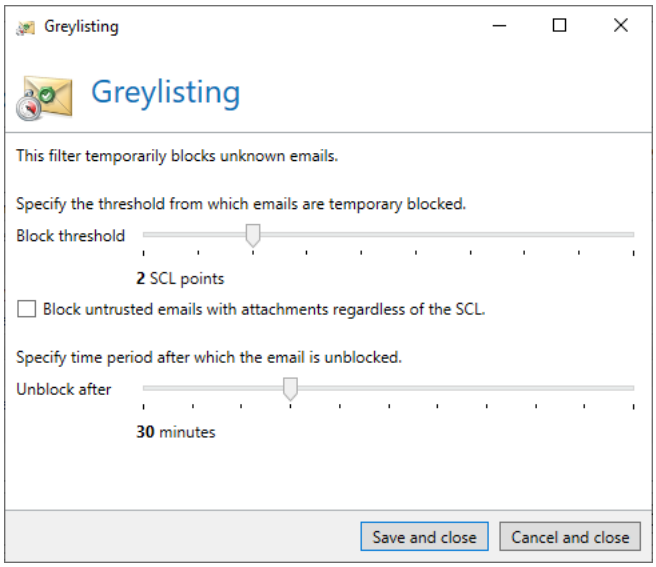
Valid for the following senders: **External**.

Greylisting is a precautionary measure against suspicious emails. If an email stays below the spam threshold value, this email would be rated as sufficiently positive without greylisting. The greylisting action will not let the email pass immediately but rather reject it temporarily. The inbound server receives an error message which instructs the server to send the email again after a specified time. In the second attempt, the email is delivered. It can be set accordingly when the inbound server can start a second attempt.

This action is based on the following principle: Usually, a spammer avoids the effort to send a second email. A usual sender, however, will retry delivery after some time. In the second attempt, this connection is now rated more positive so that the email can pass.

You can set the maximum threshold for minus points which classifies a passing email as suspicious.

Add the action **Greylisting** to your rule. The dialog for the configuration opens (Picture 113).



Picture 113: Configure the greylisting options

You can define the threshold value which initiates greylisting and set the delay period after which the email is unblocked.

With the slider **Block threshold**, you define the threshold value (SCL) after which emails are temporarily blocked. This threshold value must be lower than the spam threshold value; otherwise greylisting will not take effect.

To define the time period after which emails are unblocked, use the **Unblock after** control.

Optionally, you can specify that untrusted emails with attachments are blocked regardless of the SCL value. To do this, tick the checkbox.

Hide corporate topology

Valid for the following senders: **Local**.

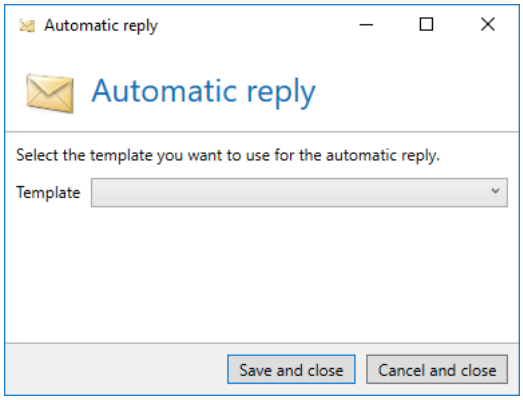
The action **Hide corporate topology** removes the "Received" email header of emails from a local sender. Otherwise, conclusions on the local topology can be made through these Received entries.

Automatic reply

Valid for the following senders: **External** and **Local**.

The action **Automatic reply** sends an automatic reply to the sender of an email (Picture 114). The text of the email is created via a template from the **Templates** folder of the Intranet Role. The setup copies an sample template (**SampleAutoReply.cshtml**) into the folder. You can use this template to create copies and adjust them to your needs.

Changes to templates are replicated within a few minutes from the Intranet Role to all Gateway Roles. The roles do not need not be restarted to do so.

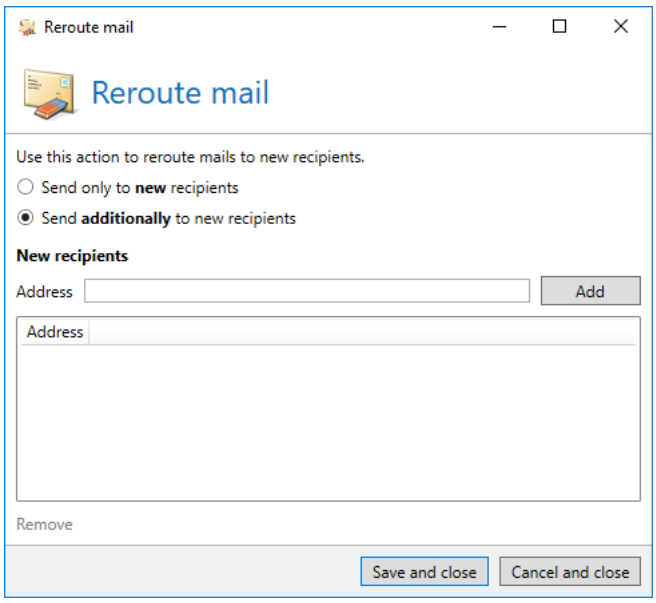


Picture 114: Create automatic reply

Reroute email

Valid for the following senders: **External** and **Local**.

This action offers the possibility to add or completely replace the recipients of an email. Depending on the settings, emails are either delivered additionally or to the recipients deposited in the action only. (Picture 115).



Picture 115: Configuration for rerouting emails

At least one recipient's address must be deposited in the list to enable the use of the action.

Project Heimdall (Preview)

This action allows metadata for emails, email attachments and URLs to be collected and uploaded to the NoSpamProxy Cloud. No file contents are collected or accessed.

The goal of Project Heimdall is to build an even more powerful anti-malware intelligence that can detect and defend against spam and malware attacks faster and more accurately.

Only the following metadata is collected by NoSpamProxy and uploaded to the NoSpamProxy Cloud:

Attachments

- File name
- File size
- SHA-256 hash
- MIME Type (as detected by NoSpamProxy)
- Information about whether malware has been detected in the attachment

URLs

- The complete URL
- The URL classification (spam, phishing, malware)

Other

- Transaction ID

- Information about whether the email was inbound (trusted/untrusted) or outbound

Heimdall as filter

The unique feature of Heimdall is that it can act both as an action and a filter. In principle, Heimdall is added to a rule as an action. In certain cases, however, Heimdall can also award appropriate bonus or negative points when calculating the spam confidence level. This is the case, for example, if there is no hundred percent certainty that the email in question is spam or malware. If Heimdall acts as a filter, it is listed in the message tracking under **Filters**.

Heimdall's assessment of emails is generally based on the evaluation of a number of indicators. This assessment results in a final evaluation 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.

Apply DKIM signature

To use Disclaimer you have to licence it separately.

Valid for the following senders: **Local**.

This action adds a DKIM signature (DomainKeys Identified Mail) to outgoing emails. In doing so, the recipient can ensure that the email was actually sent by your company. To create the signature, a DKIM key is required. How such a key is created and published can be obtained from chapter DomainKeys Identified Mail.

CxO Fraud Detection

The **CxO Fraud Detection** action is used to detect phishing attacks. The action compares the sender name of inbound emails to the names of corporate users. Fake emails sent to you in the name of superiors or employees are intercepted.

During the check, different variants of the sender name are included in the comparison. Here are some examples:

- Erika Mustermann
- Mustermann Erika
- ErikaMustermann
- MustermannErika

All corporate users that you want to use for CxO Fraud Detection must first be enabled in the respective corporate users.

Apply disclaimers

Valid for the following sender: **Local**.

This action adds a disclaimer to outgoing messages. For doing so, the disclaimer rules and templates are evaluated and attached to the respective positions in the email. In chapter Disclaimer, you learn how you can configure the disclaimers.

11. Calculating the Spam Confidence Level

NoSpamProxy Protection rejects all emails whose Spam Confidence Level (SCL) exceeds a certain threshold. As the administrator, you can set this threshold in the individual rules. The following paragraph explains the procedure of NoSpamProxy Protection for the calculation of the SCL. In the following, a very simple example explains how the filters work without the Level of Trust system. The filter configuration is as follows:

- Emails will be checked and rejected as soon as the SCL is 4 or greater.
- The filter Realtime Blocklists is enabled and assigns two points for each hit.
- The Spam URI Realtime Blocklists filter is enabled and assigns two points for each hit.
- The Word matching filter is enabled and assigns two points for each hit.

Now, an email is processed which contains eight forbidden words and one forbidden link. The link is included in a blacklist. Moreover, the inbound IP address is available on two blacklists. The preliminary result of the filters is as follows:

Filter	**SCL evaluation of filter**
Realtime block lists	4 (Two hits X two minus points per hit)
Spam URI Realtime blocklists	2 (One hit X two minus points per hit)
Word matches	16 (Eight hits X two minus points per hit)

The calculated value is always reduced to 10 if it exceeds "10". Negative values smaller than "-10" are adjusted to the value -10. The net value of the filters in our example would then be as follows:

Filter	**SCL evaluation of filter**
Realtime block lists	4
Spam URI Realtime blocklists	2
Word matches	10 (limited since the first value was >10)

Finally, the multiplier of the individual filters is taken into account. The filters Realtime block lists and Spam URI Realtime blocklists have the multiplier "2", the word matches have the multiplier "1". The net value of the filters is now multiplied by the respective multipliers. This results in the following values:

Filter	**SCL evaluation of filter**	**Multiplier**	**SCL**
Realtime block lists	4	2	8

Spam URI Realtime block lists	2	2	4
Word matches	10 (limited since the first value was >10)	1	10
Total			**22**

Therefore, the email receives an SCL of 22 and is rejected.

In the second example, the filter configuration from the first example is only extended by the Level of Trust system. Moreover, this concerns the same email as in the previous example. However, now the email is a desired email and the address pair and domain bonus of the sender and recipient address exist in the database. Since the last email communication took place four days ago, the address pair bonus has been reduced to 65 bonus points. The domain, however, is located in the trust settings with 100 static bonus points. The bonus points of the Level of Trust system in the database are not identical to the SCL value but rather the so-called trust points. They are only used within the filters.

The Level of Trust system now assesses as follows:

First, the biggest value of the individual Level of Trust values (Address-, Domain, Subject, MessageId bonus as well as the points of the DSN verification) is used "100". For the calculation of the SCL, this sum is divided by the value "-10" and results in this example in an SCL of -10 points. Similar to all other filters, the calculated value is also reduced to 10 or -10. The table with the net values is now as follows:

Filter	**SCL evaluation of filter**
Realtime block lists	4
Spam URI Realtime blocklists	2
Word matches	10 (limited since the first value was >10)
Level of Trust system	-10

You can determine the multiplier of the individual filters in the respective rule. The Level of Trust system, however, chooses its multiplier independently. To do so, the multipliers of all other filters are added up and amount to the value "5" in our example. The definite calculation of the SCL with the influence of the Level of Trust system is as follows:

Filter	**SCL evaluation of filter**	**Multiplier**	**SCL**
Realtime block lists	4	2	8
Spam URI Realtime blocklists	2	2	4
Word matches	10 (limited since the first value was >10)	1	10

Level of Trust system	-10	5 (=2+2+1)	-50
Total			**-28**

In this example, the email would have been delivered since the SCL is less than 4.

To illustrate the example, the filter "Cyren AntiSpam" with the multiplier "3" is additionally configured. This filter always assigns 4 points per hit and this value is not configurable.

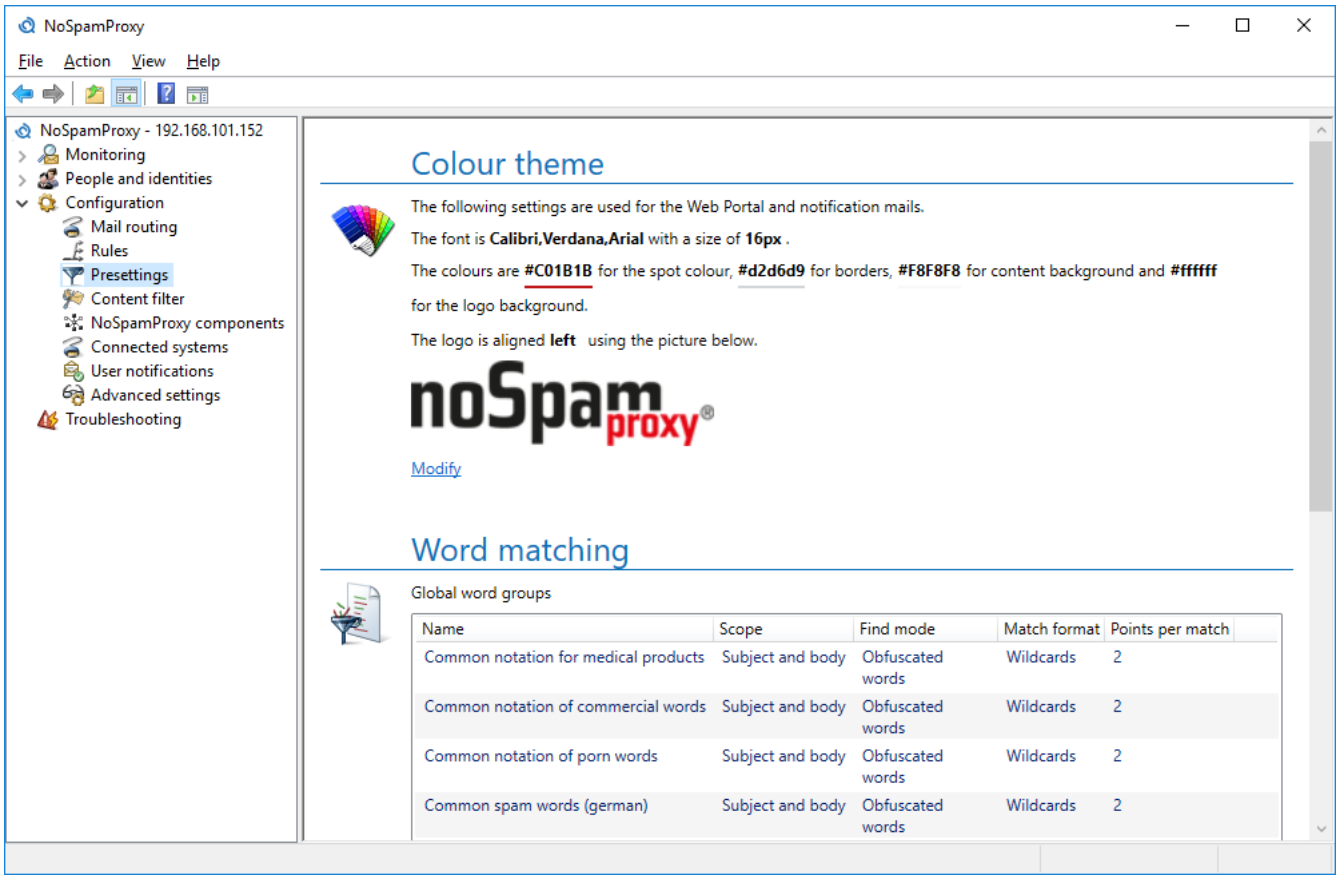
The "Cyren AntiSpam" filter also assesses the email negatively. The overall result of the SCL calculation is as follows:

Filter	**SCL evaluation of filter**	**Multiplier**	**SCL**
Realtime block lists	4	2	8
Spam URI Realtime blocklists	2	2	4
Word matches	10 (limited since the first value was >10)	1	10
Cyren AntiSpam	4	3	12
Level of Trust system	-10	8 (=2+2+1+3)	-80
Total			**-46**

The multiplier of the Level of Trust system has automatically adjusted itself due to the additional filter and can thus establish itself with even greater force. This ensures that desired communication always reaches the recipient regardless of the content of the email.

12. Presettings

This area contains global settings which can be used in other areas of the configuration such as rules, partners or corporate users (Picture 116).

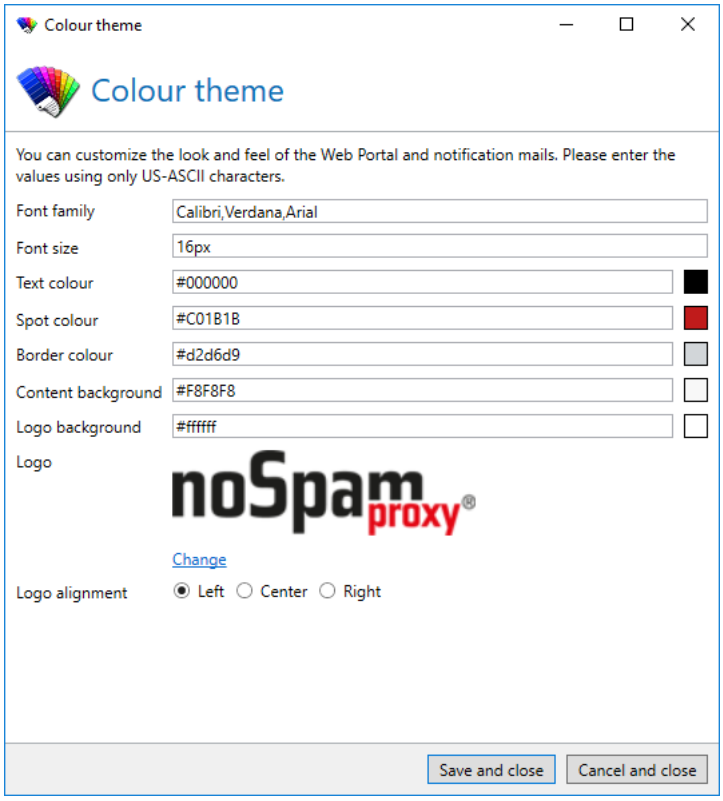


Picture 116: Presettings

Changing settings in this area also influences existing rules, partners or corporate users. The settings always apply to all configurations in which they are referenced.

Colour theme

You can adjust the layout of emails generated by NoSpamProxy as well as that of the Web Portal to your needs via the colour theme (Picture 117)



Picture 117: Dialog for changing the colour theme.

Usually, you will only adjust the highlight colour and the logo to your Corporate Identity.

The colour theme is applied to the following elements:

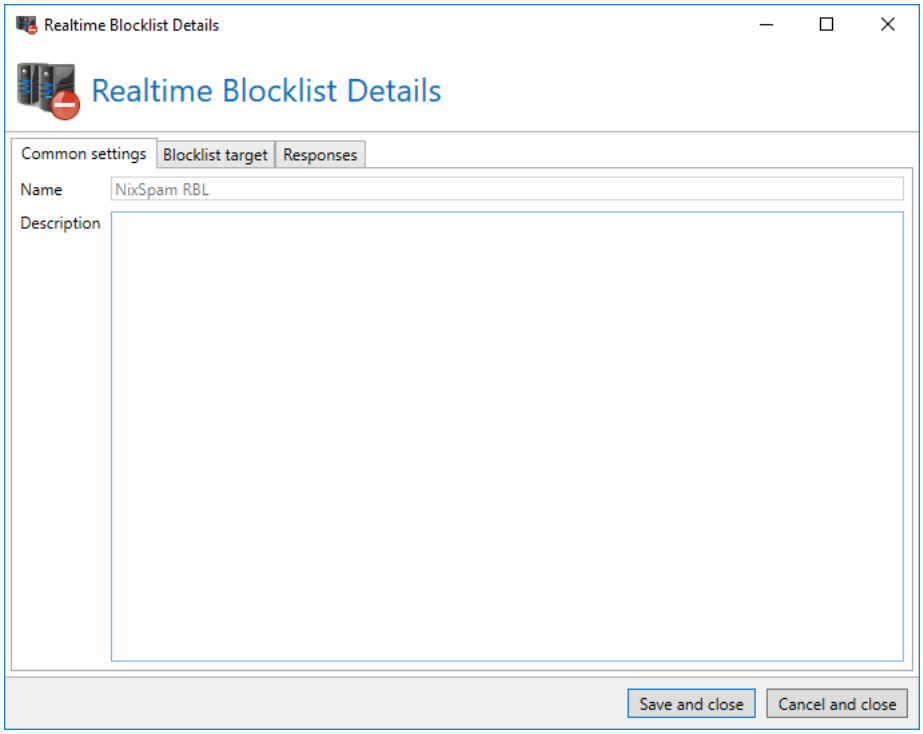
- The Web Portal
- All email notifications created by NoSpamProxy
- The substitute attachment for files which are sent via Large Files.

Realtime block lists

Realtime block lists (RBL) manage lists with suspicious spam IP addresses. Via the Internet, it is now possible to check whether an IP address might be included in the RBL list or not. These blocklists are maintained in the section **Realtime block lists** and can later be selected individually in the rules.

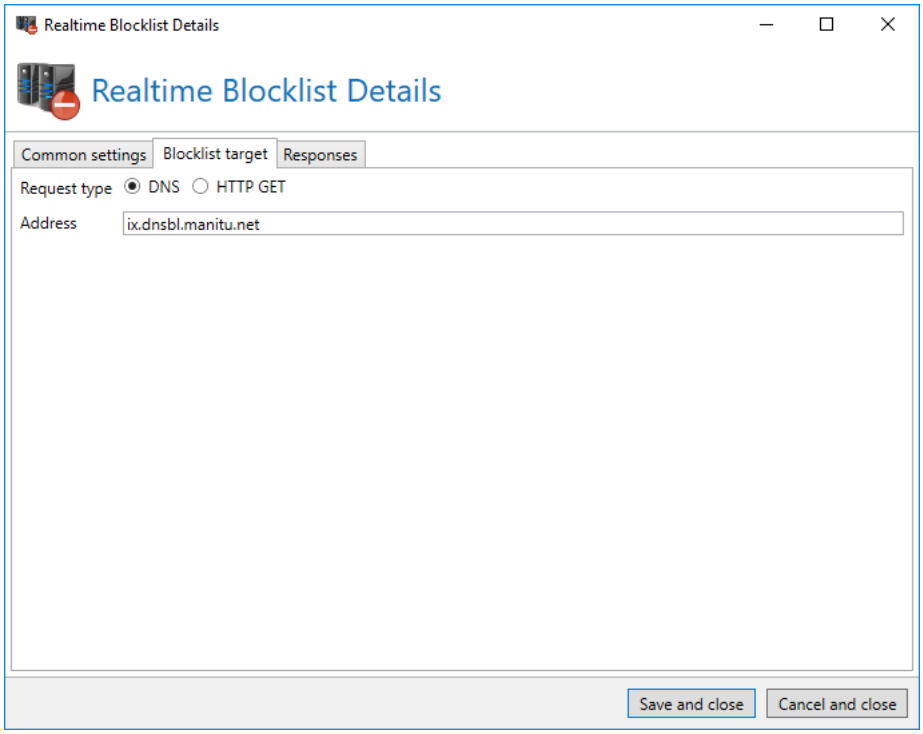
Add new blocklist

Under **Common settings** (Picture 118), you enter the name of the new RBL list in the field **Name**. In the field **Description**, you can add personal remarks that help you remember the purpose of this list at a later point in time. Both entries have no effect on the functionality of the list.



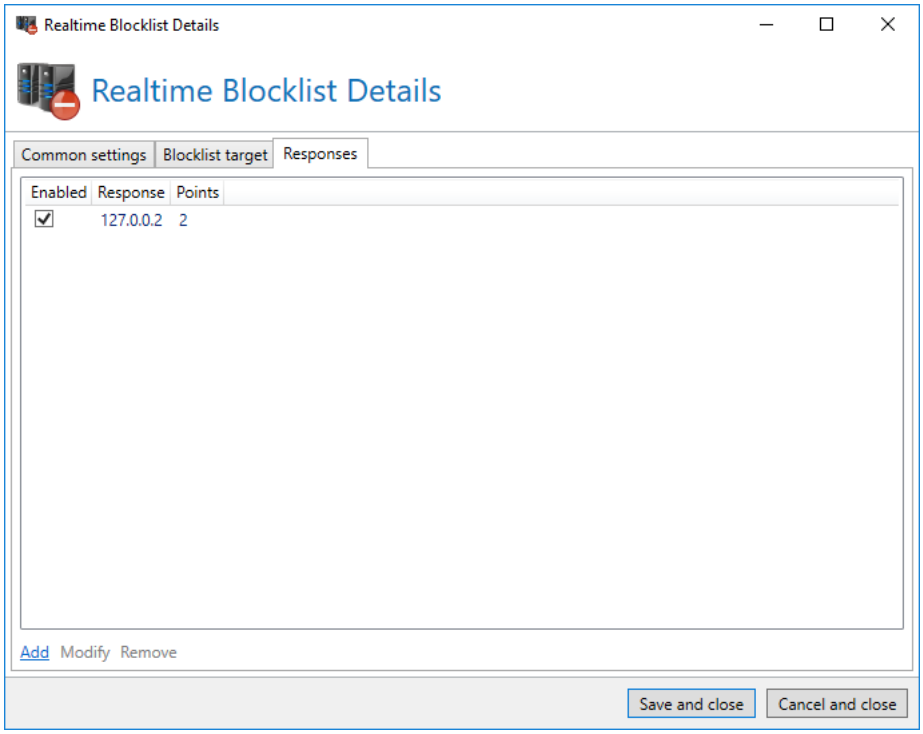
Picture 118: Enter the name and a description of the blocklist

In the tab **Blocklist target**, you indicate whether the RBL list is addressed via DNS or HTTP GET. In the field **Address**, you either enter the IP address or the server name of the server to be enquired.



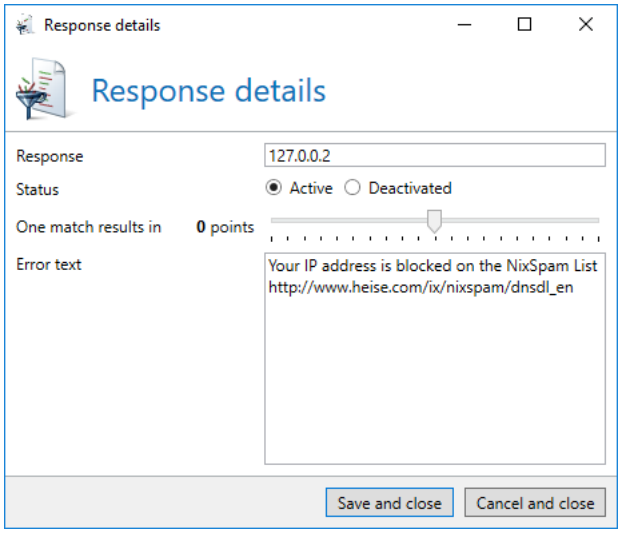
Picture 119: The dialog for the definition of a blocklist reply

Possible replies of the requested server and their meaning are defined on the tab **Responses** (Picture 120).



Picture 120: All replies of the blocklist to be expected and their assessment in SCL points

You can add new responses in the dialog **Response details** (Picture 121). Determine here how many SCL points this reply weights and a descriptive error text. A negative value equals bonus points, a positive value minus points. The text of the reply might appear in the non delivery report if the creating server supports this. In doing so, senders of rejected emails knows on which blacklist they are included and for what reason. The response can also be deactivated.



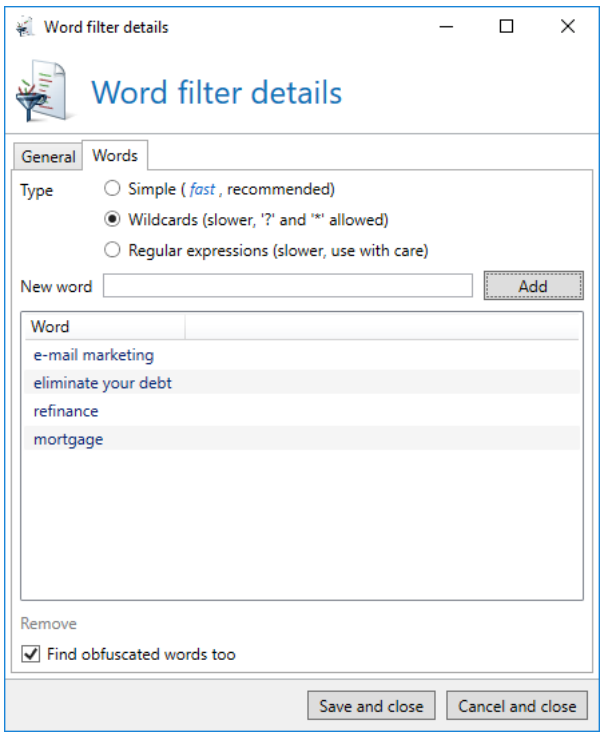
Picture 121: A response of the list

Word matching

In the paragraph **Word matching**, you can manage lists with terms to which you either assign bonus or minus points. The terms are summarised in separate word groups that you can use in the individual rules later. For each word group you determine whether bonus or minus points should be assigned to the terms. This provides you with the possibility to create groups with desired terms and undesired terms.

Add new word group

When adding a word group, the dialog **Word filter details** opens (Picture 122).



Picture 122: Definition of the word group

Choose an unique **Name**.

You can determine for each word group which part of the email should be scanned for the configured terms. You have three choices. Select the **Subject** if NoSpamProxy Protection should search for the terms of this group in the subject line of one email only. If you wish to have searched the body of the email for the terms, select **Body** here. Alternatively, you can scan both parts of the email for the terms. To do so, select **Subject and body**. This is the recommended setting.

Additionally, you can set whether to distribute points for each occurrence of a word or only if none of the words is found in either the content or the subject.

You can use two different types of terms in the word groups. With the setting **Type**, you determine whether it concerns so-called wildcards or regular expressions. If you simply wish to create a list with usual content such as Viagra, Cialis, etc., select the option **Wildcards**. Here, you also have the possibility to use wildcards ('*' and '?'). Wildcards allow you to enter Cialis* to search for all expressions starting with the term Cialis.

If you have already prepared regular expressions, you can continue to use them. To do so, select the option **Regular expressions** in the setting **Type**.

The setting **Find obfuscated words too** is only available to you if you have selected the option **Wildcards** in the setting **Type**. You can determine now whether NoSpamProxy Protection should only search for the exactly stated terms or also for similar words. If you select the option **Exact matches only** and enter the word Viagra for the matches, NoSpamProxy Protection will only search for the word Viagra. The search does not distinguish between capital and small letters so that you can disregard the

accurate use of capital and small letters. However, NoSpamProxy Protection would not find the variant V1agr@ with this setting. If you select the option **Find obfuscated words too**, however, NoSpamProxy Protection recognises similar spellings such as Vlagra, V1@gra or V-I-A-G-R-A as well.

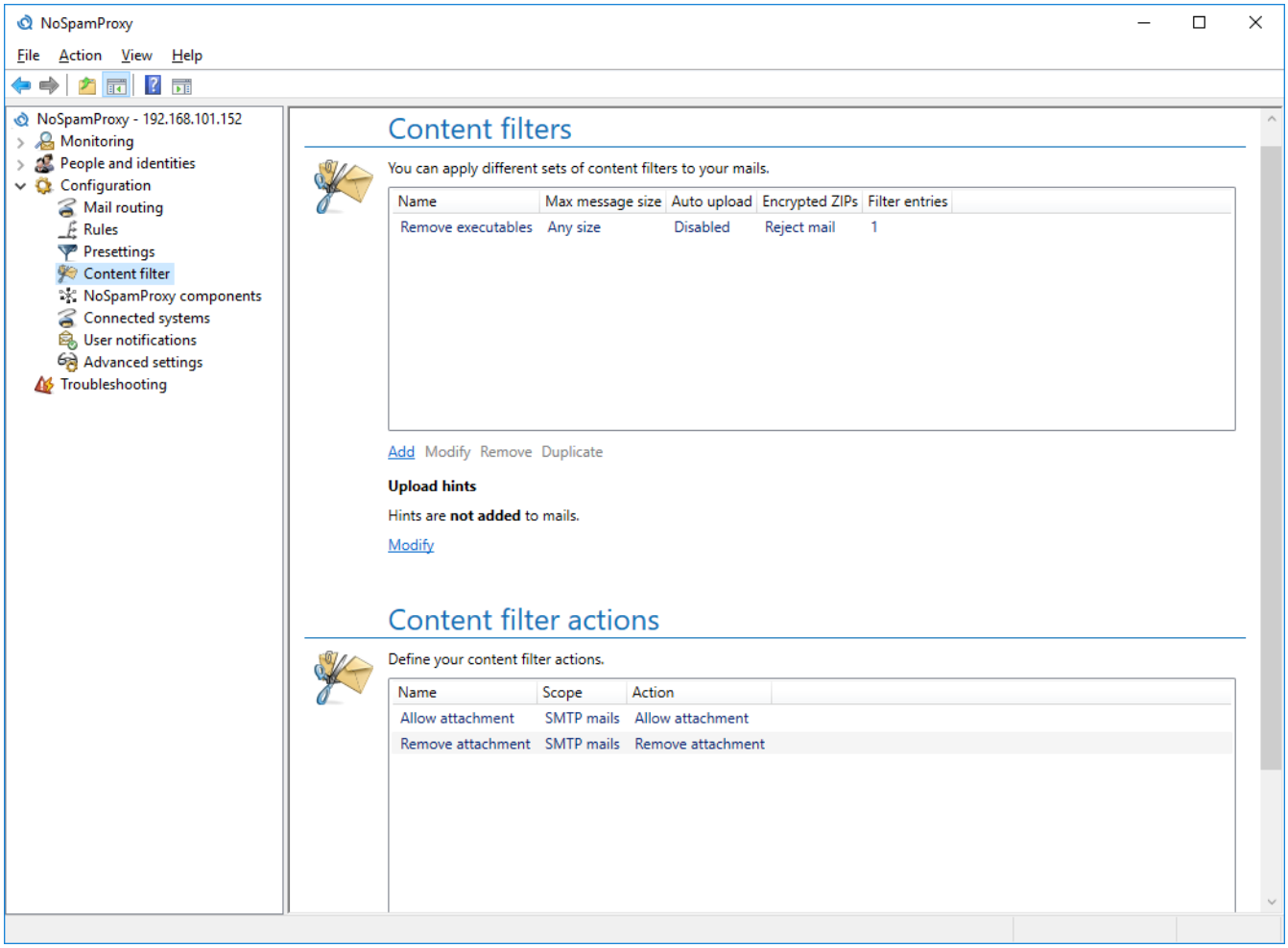
With the slider **Points**, you determine how many minus or bonus points should be assigned per hit. You can set values between -10 and 10. Here, the value -10 corresponds to bonus points. The setting 10 thus means 10 minus points.

If you implement changes to the word groups, they influence all rules which use the filter "Word matches" and have configured the respective word group.

13. Content filter

This section is available if you possess a valid licence for NoSpamProxy Large Files or NoSpamProxy Protection. The scope of available functions depend on your licence type.

The list of the content filters serves to allow, block or reroute attachments which correlate to one of the filters defined there (Picture 123). This list serves to centrally manage the content filters in order for it to be used in the Partners as well as in the corporate users. A content filter can be assigned in the partner node in the **Default partner settings**, in a **Domain entry** of a partner as well as to a partner address. The settings on a email address have priority over the settings on a domain and the settings on a domain have priority over the default partner settings.



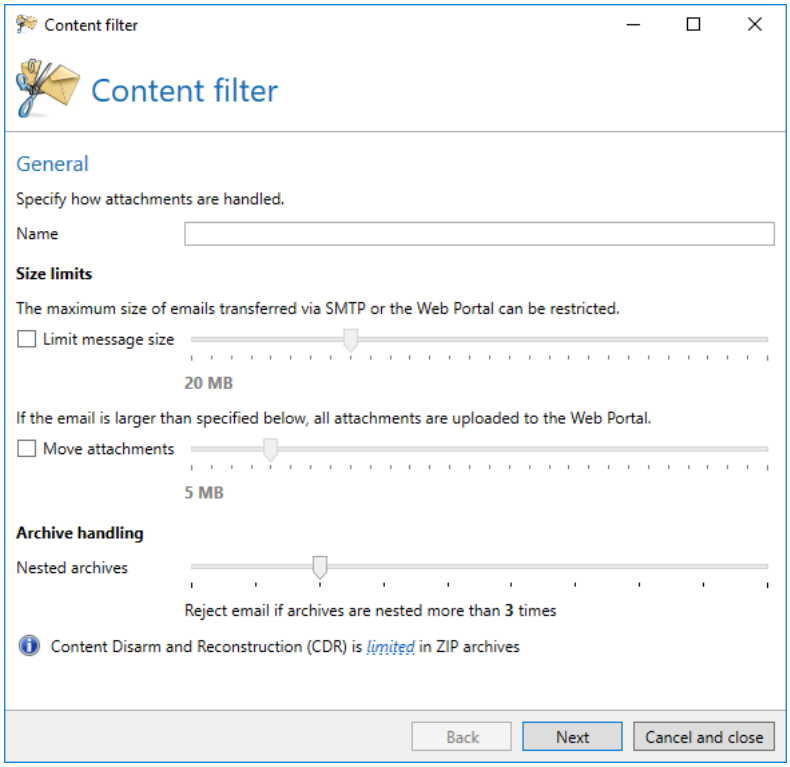
Picture 123: The list of all content filters

In addition to the settings of the content filters on **Corporate users** and **Partners** you can enable and disable the content filter on every rule in the section **General**.

Each filter in the list of content filters consists of one or more entries, with **conditions** like filename, type or size for the email attachments. Also, the action to be taken, e.g. block, allow or move to Web Portal, is defined. All actions are configured in a list of its own; thus they can be used in different content filter entries.

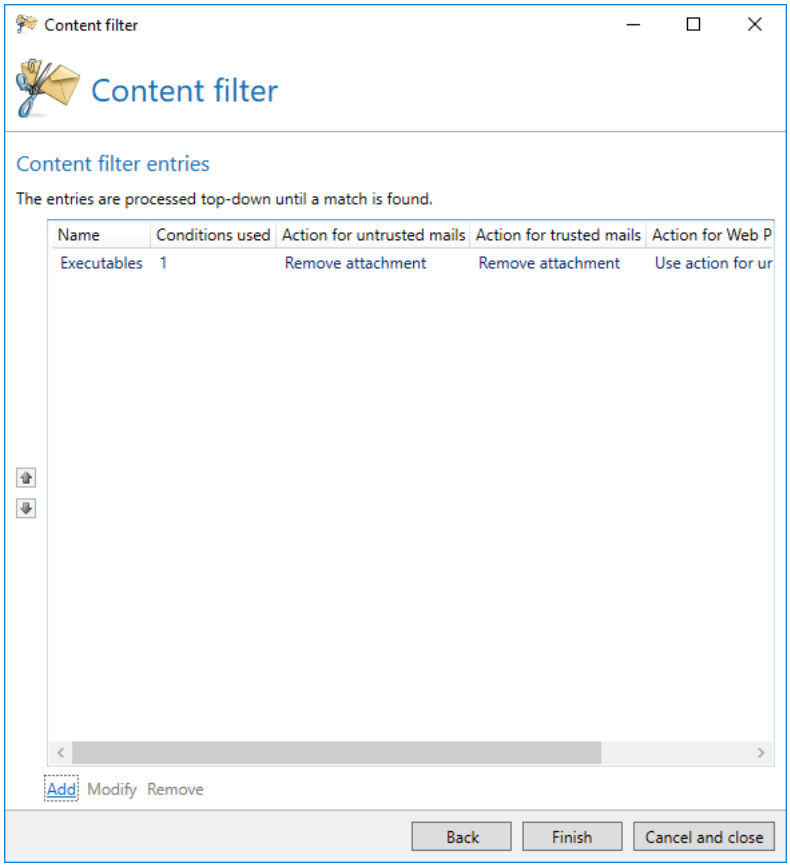
Content filter sets

Please enter a unique name. Additionally you can limit the maximum size of emails and attachments. Emails which exceed the maximum size are blocked. You can determine how many levels of nested archives are analysed. This restriction aims at separating out highly to unlimited nested archives (Picture 124).



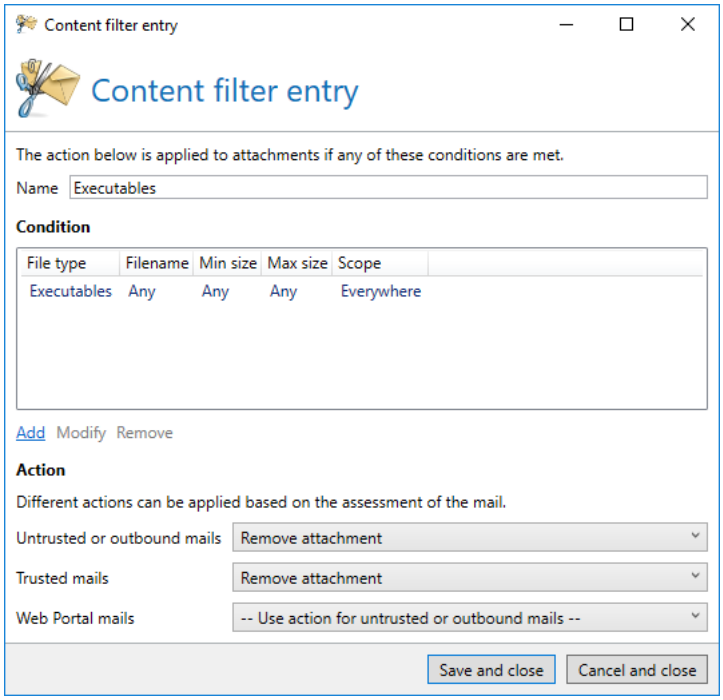
Picture 124: General settings for a content filter

Each content filter can contain one or more entries to configure all actions needed for different attachments. (Picture 125). All entries are processed top-down and can be reordered by the buttons with arrows on the left. If no filter entry of content filter matches the attachment, the attachment is delivered normally.



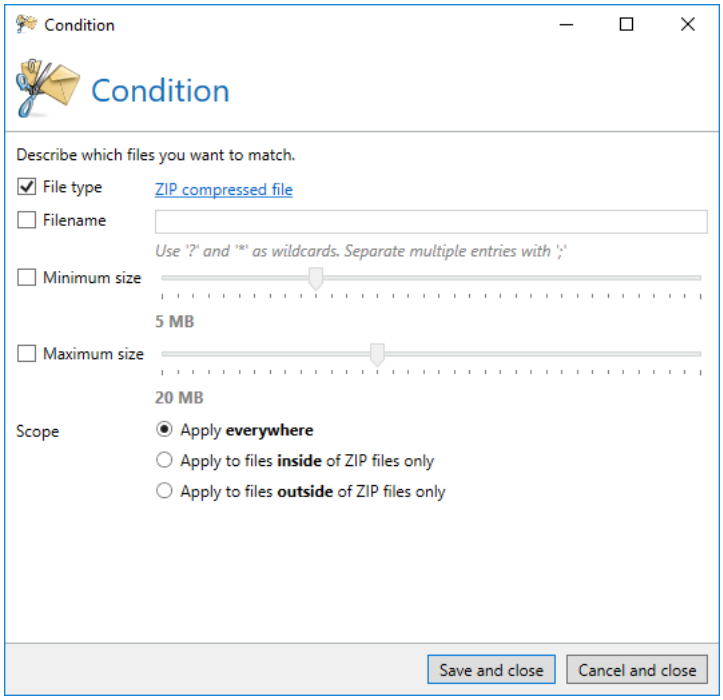
Picture 125: List of content filter entries

An entry of a content filter contains conditions to select attachments (Picture 126). Multiple, combinable criteria are available (Picture 127). If the entry has to match all attachments be sure to add a condition containing its default settings. Dependent on the assessment and the direction of the email different actions are available. For Web Portal emails the action selected for inbound and outbound SMTP emails can be selected; the attachments are then processed identical to the selected SMTP action without configuring an action for Web Portal emails of its own.



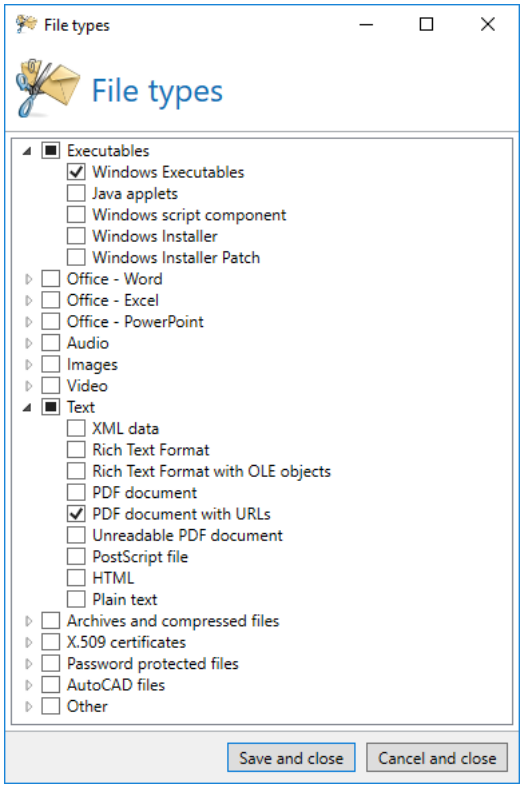
Picture 126: A content filter entry

A **condition** defines the files which are processed by the content filter. You can filter by various properties of the attachments. The section **Area** determines if files contained in archives are also analysed. By this your are able to use all analysis functions of the content filter for the contents of archives.



Picture 127: A condition for attachments

The **file type** in a condition is also capable to filter by the actual content of the file instead of its filename in order to detect and process attachments with renamed file extensions (Picture 128). You can select from a variety of file types, including executables, Office files and PDF files that contain URLs.

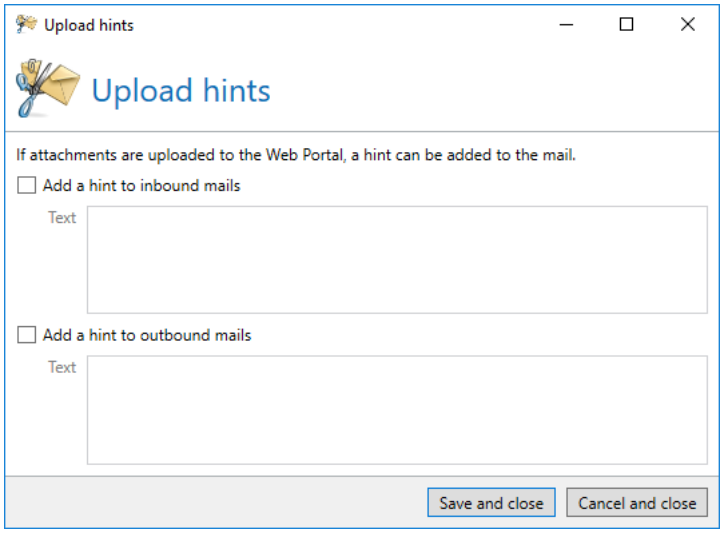


Picture 128: Dialog to select the file types

Detailed information on the RTF file filtering process can be found in the appendix under Processing of RTF files during content filtering.

Upload hints

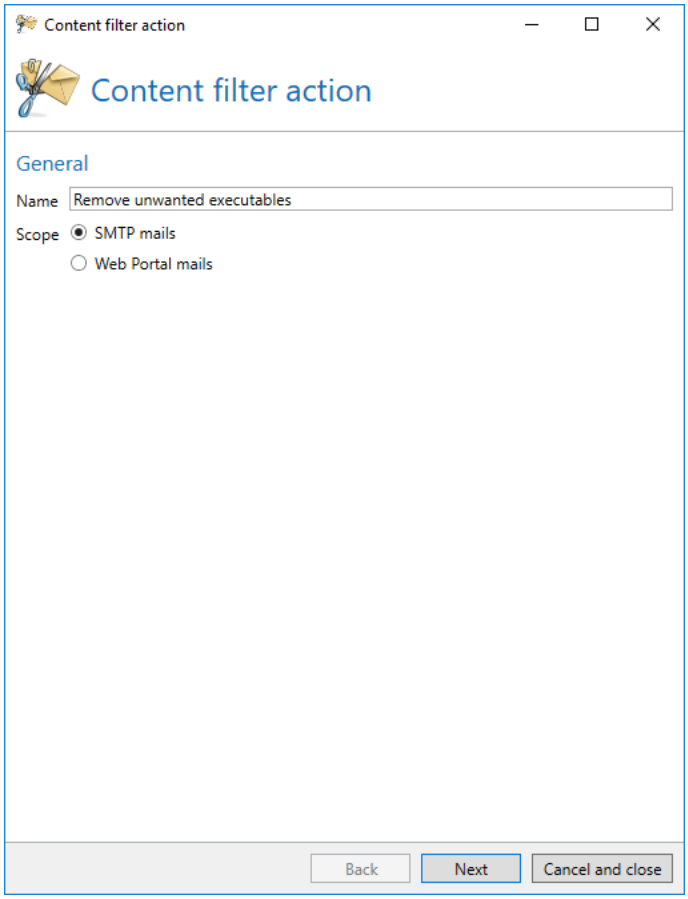
Some users may not recognise immediately if an attachment has been removed from an email and uploaded to the Web Portal. In case these users fail to download the file before it is removed from the Web Portal it may be irrecoverably lost. To avoid this, you can add a text to incoming and outgoing messages which notifies the recipient that attachments have been relocated to the Web Portal (Picture 129).



Picture 129: Upload hints

Content filter actions

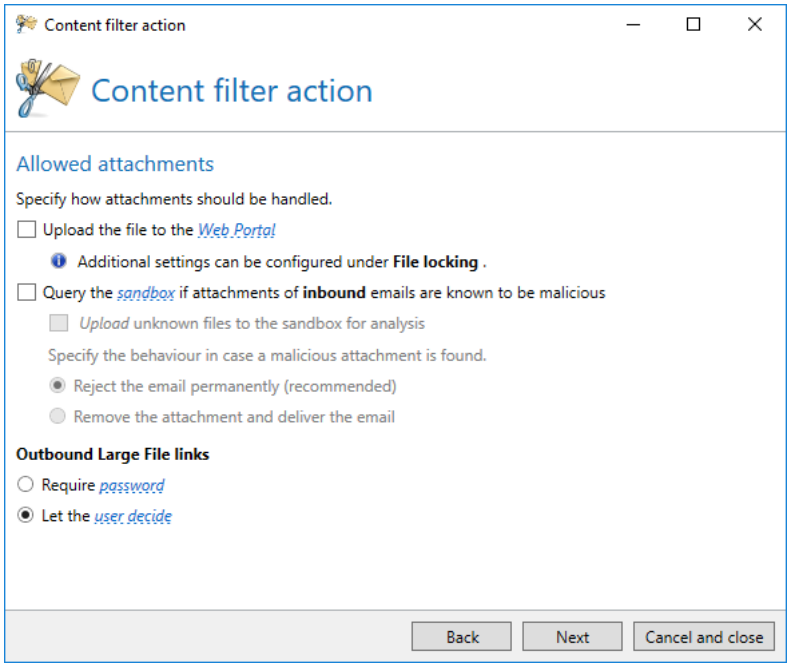
All content filter actions are configured centrally and provided with a unique name in order to reuse them without the need to create an action with the same content. In a new content filter action you have to choose a unique name and the type of filter first because the processing of SMTP and Web Portal emails differs from each other (Picture 130).



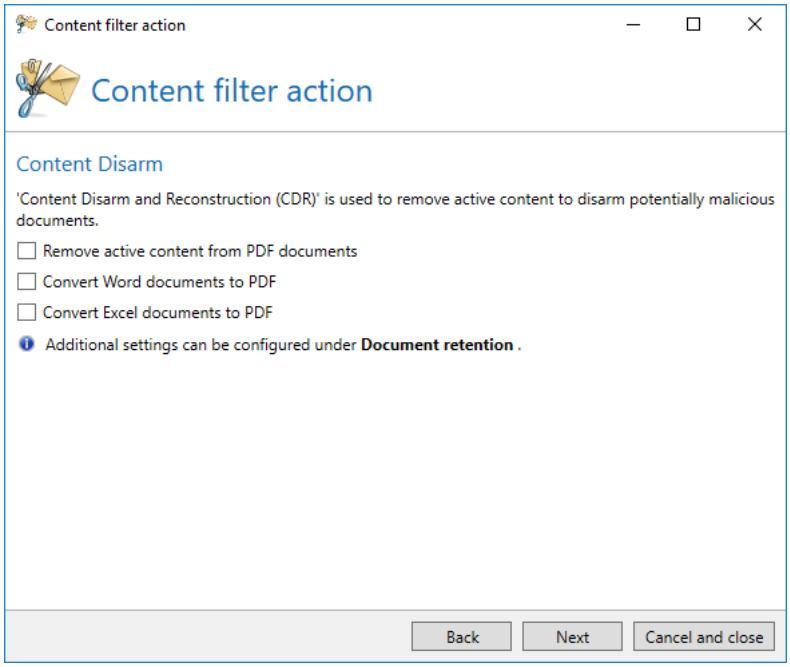
Picture 130: The type of action

On SMTP emails choose the basic behaviour first, like **Allow attachment**, **Remove attachment** and **Reject the entire email on SMTP delivery**. If you allow the attachment you will find options regarding attachment upload, Web Portal and Sandbox usage, conversion of documents to PDF as well as the treatment of original documents after their conversion to PDF. If your selection uses the Web Portal for Large Files, you can also configure treatment of the attachment in the section **Web Portal upload settings**.

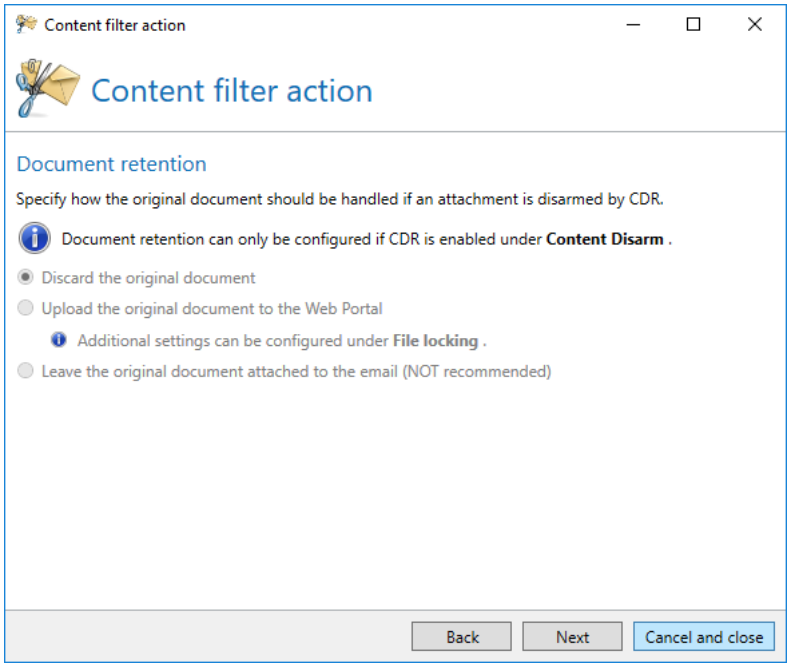
The Cyren Sandbox is a cloud-based security feature that analyses potentially dangerous content in an isolated environment. The file is loaded into the sandbox, where it is executed and analysed. Malicious files and URLs are blocked immediately.



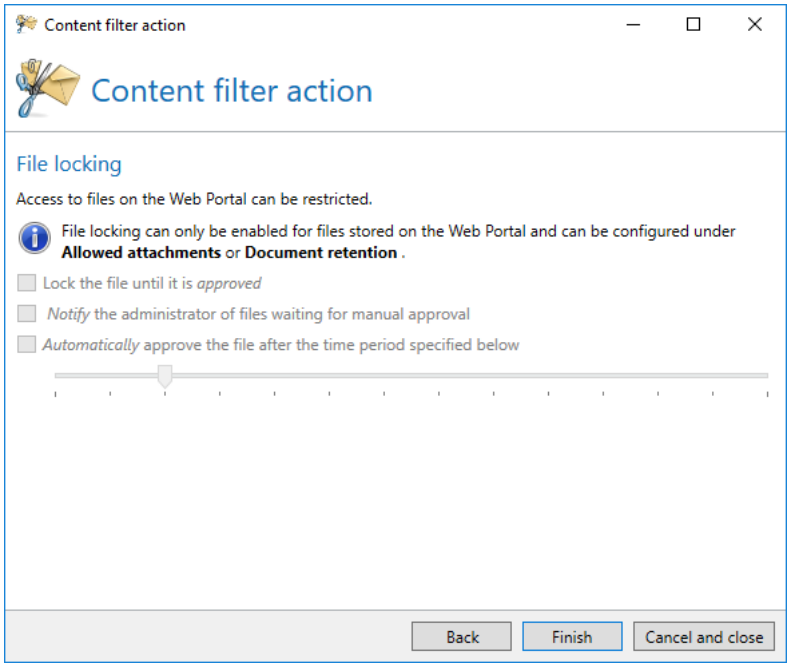
Picture 131: Web Portal, Sandbox and Large Files actions



Picture 132: Content Disarm actions

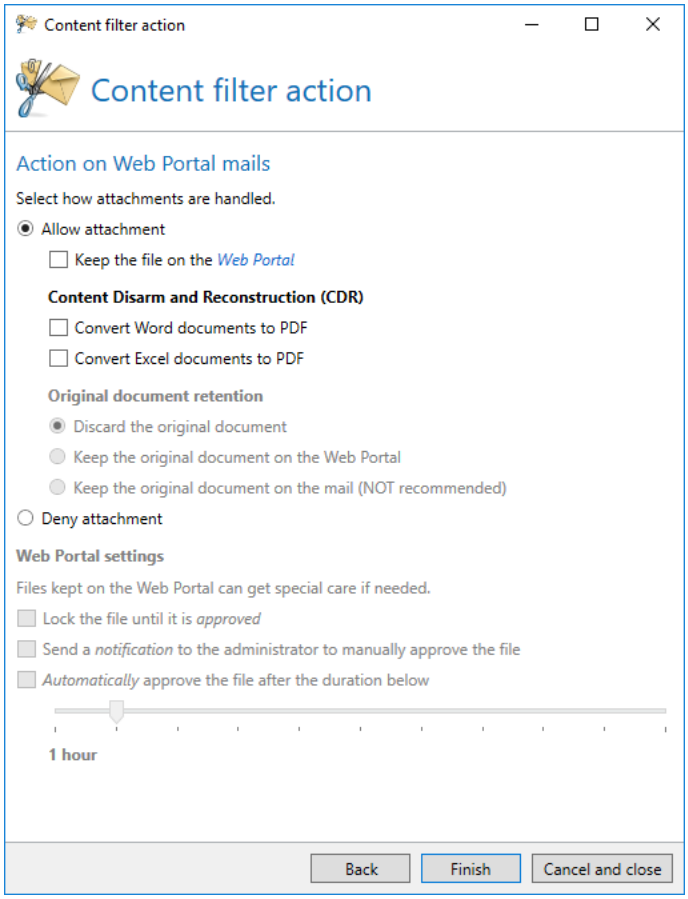


Picture 133: Actions regarding document retention



Picture 134: Actions regarding file locking

The **Action on Web Portal emails** is configured analogous to an **Action on SMTP emails**. (Picture 135)



Picture 135: Action on Web Portal emails

File locking for files stored on the Web Portal is not supported for outbound emails.

14. The URL Safeguard

The **URL Safeguard** prevents access to harmful content accessed via links. If configured accordingly, the URL Safeguard matches URLs contained in inbound emails against entries in the following lists:

- **NoSpamProxy Whitelist**, a list of known websites, curated by NoSpamProxy.
- The local whitelist created by the administrator.

Domains contained in one of these lists as well as as corporate domains are never rewritten.

Settings for the NoSpamProxy Whitelist and the local whitelist can be made under **Configuration/URL Safeguard**.

If the domain contained in the link is not found in any of the lists, NoSpamProxy replaces the original link with a link that points to the Web Portal. In these cases the email delivered to the recipient only contains the rewritten link.

On the Web Portal the links are then analysed with the help of our technology partner Cyren. If the link is classified as harmless, access to the original URL is permitted and executed.

If the link is classified as malicious, the access is blocked. A message about the incident is added to the message tracking. Depending on the configuration, the administrator also receives a notification.

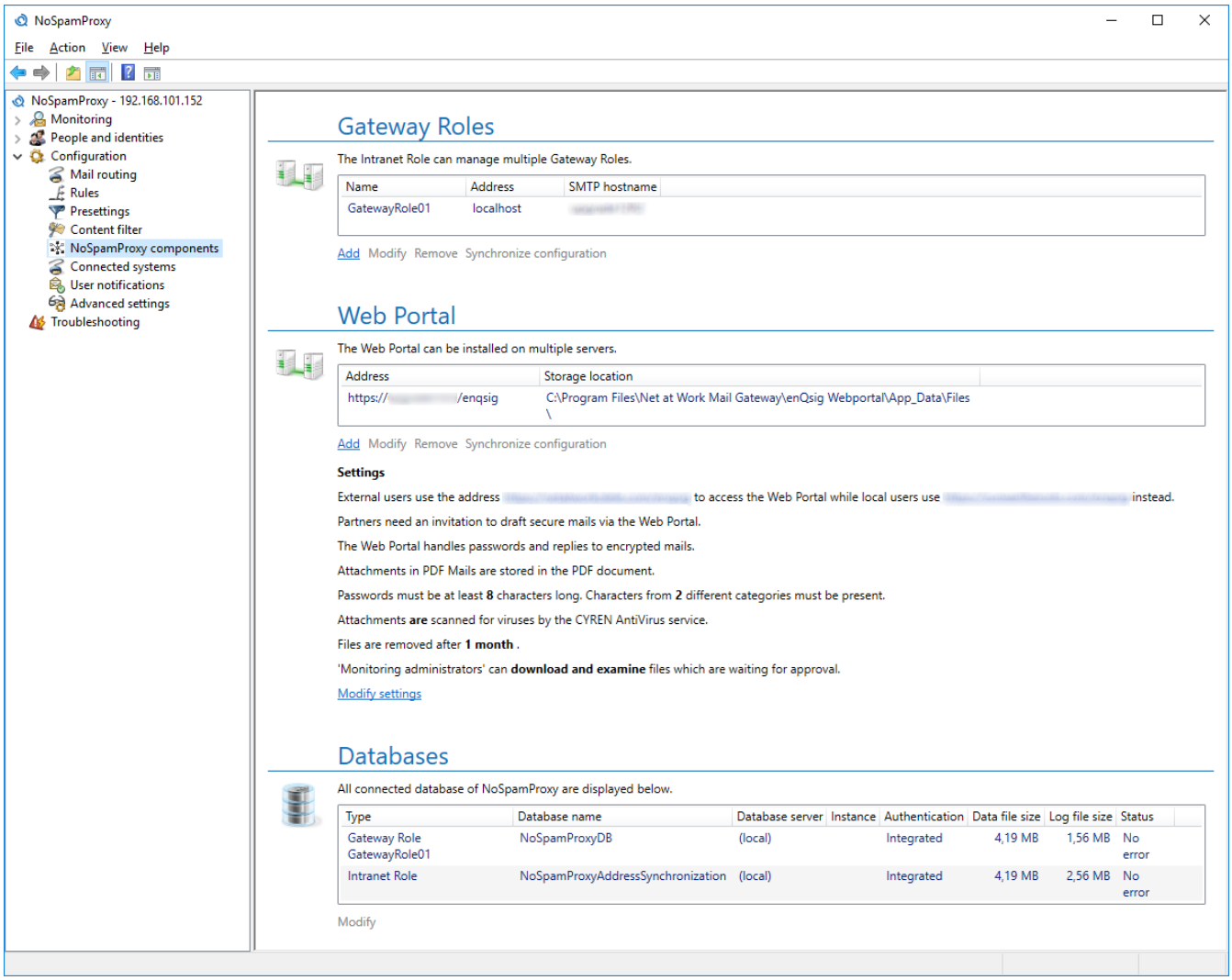
Blocked URLs can be unblocked by adding them to the local whitelist. The domain belonging to the blocked URL can be accessed on the Web Portal by the recipient of the email after clicking on the rewritten link. The administrator responsible can then perform the activation. A further delivery of the email by the communication partner is not necessary.

To activate the URL Safeguard you must add it as an action to a rule.

Further settings can be made in the Default partner settings or for individual Partner domains.

15. NoSpamProxy components

The connections between the individual components of NoSpamProxy are configured under **NoSpamProxy components** (Picture 136).



Picture 136: The connections to individual components of NoSpamProxy

Gateway Roles

The Gateway Role can either be installed on the same or on a different server as the Intranet Role. If you operate more than one Gateway Role, valid licences for all roles are required. The installation of the first Gateway Role is included in each licence. Contact us at sales@nospamproxy.de for detailed information on the subject of high availability with multiple Gateway Roles.

To ensure high availability, you can operate multiple roles in your company. An overview is provided in The roles of NoSpamProxy. Examples are explained in Functionality and infrastructure integration.

The configuration is transferred from the Intranet Role to all connected Gateway Roles. If you operate a DMZ in your company, we recommend you install the Gateway Roles as part of the DMZ and the Intranet Role as part of the internal network. You only need to activate the connection from the internal network to the DMZ for the TCP port 6060 and the HTTPS port 6061 in your firewall.

In some cases, the configuration of a Gateway Role can deviate from that of the Intranet Role. In this case, you can induce the Intranet Role via the button **Synchronise configuration** to synchronise the configuration with the marked roles.

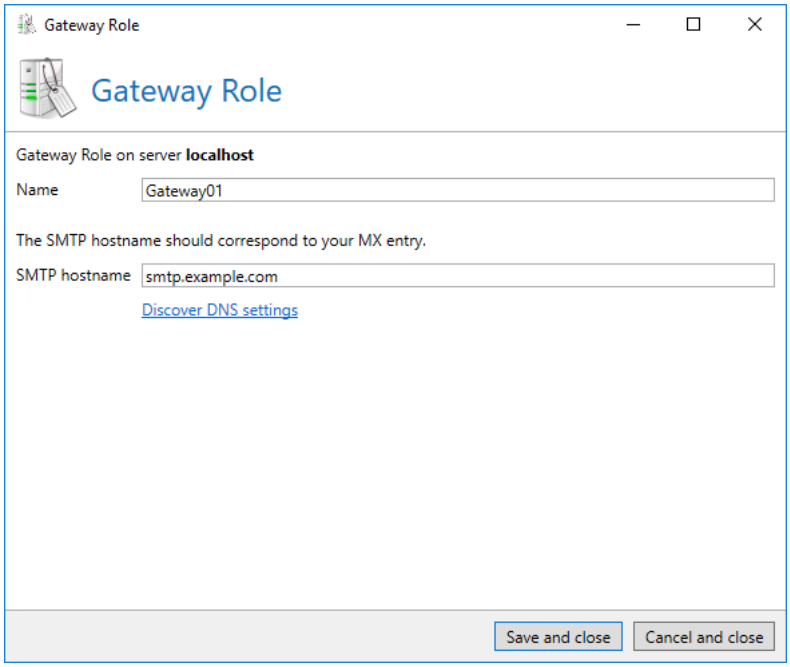
Server identity

When connecting to external servers, the client introduces itself to the receiving server with the HELO or EHLO command followed by the server name. One possible example:

```
EHLO mail.netatwork.de
```

Some servers check whether this name can be resolved via DNS. The resolvability of this name is required by an RFC. If the name is not resolvable, this is rated as a spam feature by some email servers. The FQDN which is resolvable in the Internet should be entered here. Usually, the MX of the owned email domain must be entered here.

To adjust the setting, click on **Change** in the section **Server hostname**. The dialog for changing the identity appears (Picture 137).



Picture 137: The server identity should correspond to the "MX" entry in your DNS

Provide the name to be used in the field **SMTP hostname**.

You can also automatically resolve the DNS name for your domain. To do so, the primary domain of your licence is used. For the automatic resolution, click on the button **Discover DNS settings**. A dialog appears which lists all available MX records for your domain sorted by priority.

Establish a connection to a Gateway Role

Select **The Intranet Role and the Gateway Role are both running on the same server.** in the dialog for the connection to a Gateway Role if you have installed the roles to be connected on the same server. If the Gateway Role is installed on a different server, first select the option **The Intranet Role and the Gateway Role are running on different servers...** Provide the name of the Gateway Role under **Hostname** and the **Port** where the current role can reach the Gateway Role. If the Management Role can connect to the Gateway Role using the same data, select the option **The Management console can connect to the Gateway Role with the server name and port provided above**. Otherwise, select **The Management console can connect to the Gateway Role with the server name and port provided below** and enter the data into the fields **Hostname** and **Port**. By default this is port 6060.

Web Portal

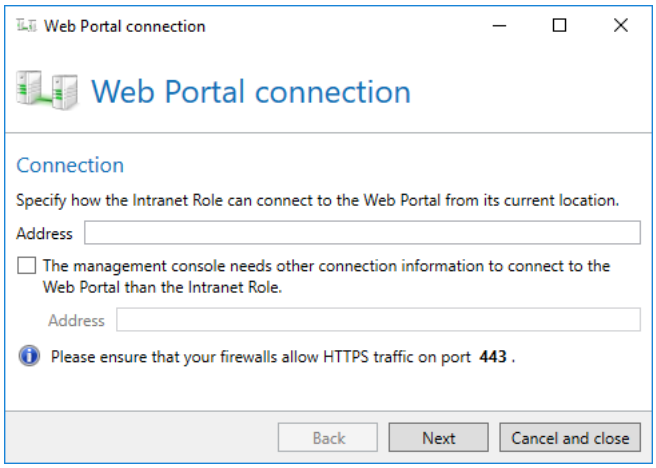
To be able to use the Web Portal, you must first establish a connection from the Intranet Role to the Web Portal. Subsequently, you can configure the individual features.

You can operate several Web Portals in your company for high availability. An overview is available in The roles of NoSpamProxy. Examples are explained in Functionality and infrastructure integration.

The Web Portal is available to you if possess a valid licence for NoSpamProxy Large Files or NoSpamProxy Encryption .

Web Portal connections

In the dialog for a connection to the Web Portal (Picture 138), enter the HTTPS address of the Web Portal under **Address**, e.g. `https://portal.example.com/` or `https://portal.example.com:1234/` for a connection via the port '1234' under which the Intranet Role can reach the Web Portal. If the Management Role is unable to connect to the Gateway Role using the same data, select **The Management console needs other connection information to connect to the Web Portal than the Intranet Role** and enter the HTTPS address into the field **Address** under which the Management console can reach the Web Portal. By default this is port 443.

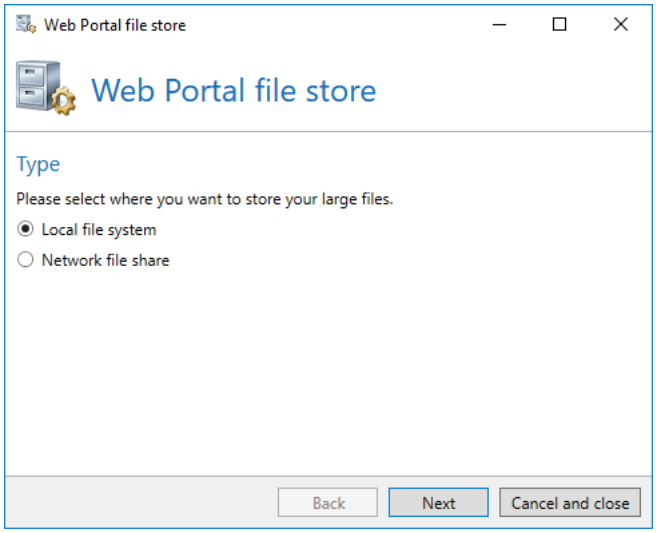


Picture 138: The settings for a connection to a Web Portal

In some cases, the configuration of a Web Portal can deviate from that of the Intranet Role. In this case, you can prompt the Intranet Role via the button **Synchronise configuration** to synchronise the configuration with the marked Web Portals.

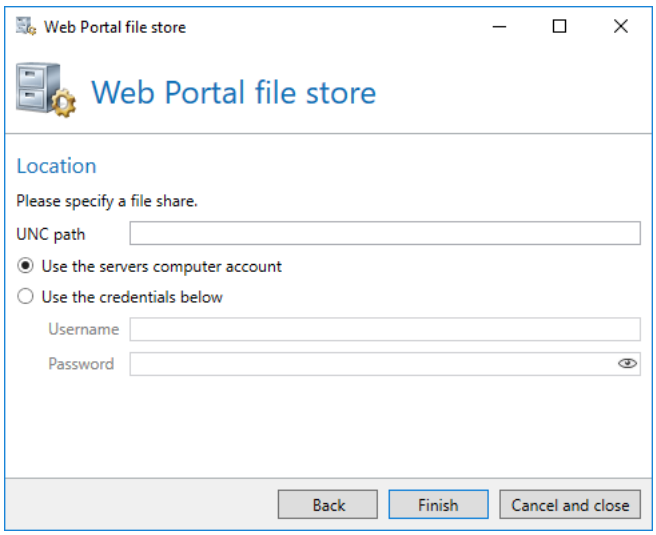
You can adjust the file storage location of 'Large Files' after the connection has been established. The following locations are available (Picture 140).

- **Local file system**
  Provide a path on a local storage to which the account given in the dialog have the respective rights.
- **Network file share**
  Enter the path for the network share. Select whether you access the share via the computer account of the server or whether a specific user account is used (Picture 139).
- **Microsoft Azure BLOB Storage**
  Providing an Azure account name and the corresponding account key will result in all files being stored in the associated Azure BLOB Storage.



Picture 139: Storage locations for 'Large Files'

Depending on the selected storage location, you need to enter storage location and/or user information (Picture 140).

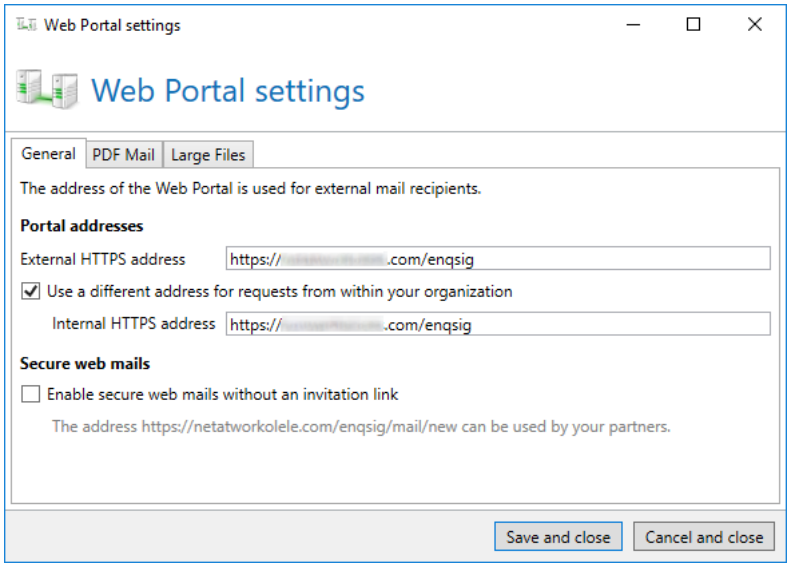


Picture 140: The connection to the file storage location of the Web Portal using the example of the network release

Web Portal - Settings

When using the Web Portal, a link to it might be included in emails. The link contains the address under which the Web Portal is available over the Internet (Picture 141). If you use a different address for the access from the company network, you can enter it into the field **Internal Https address**.

You can activate the section **Secure web emails** to enable the usage of the Web Portal without invitation link via the displayed address. If enabled, an external Partner can send an email to a recipient in your company of a corporate user via the Web Portal. To do this, he has to enter a sender address and a valid recipient address of a corporate user from NoSpamProxy. If NoSpamProxy has no corporate users, the domain of the recipient address will at least be validated against the list of owned domains.



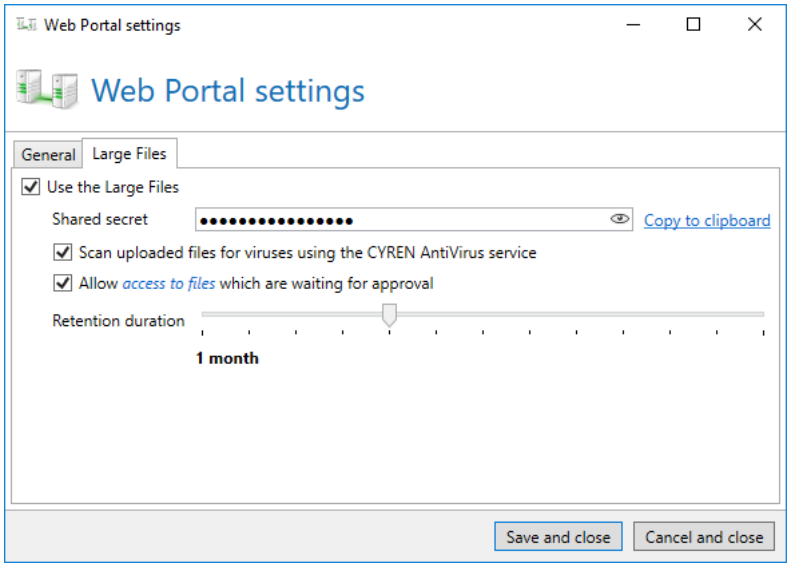
Picture 141: General settings

If you activate Large Files, you need to configure some further settings on the next page (Picture 142). To secure the communication between the Outlook Add-In and the Web Portal, a **Shared Secret** ("Shared Secret") is required. Enter a password which at least consists of 12 characters.

The 'Large Files' files stored by the Web Portal are encrypted completely. The decryption key is only available to the recipient so that the administrators of the server have no access to the files. If you wish to check the files which are waiting for approval, you must explicitly allow this via the option **Allow access to files which are waiting for approval**. After the file has been approved under 'Large Files', no further access by members of the 'Monitoring Administrators' group is possible.

With NoSpamProxy Protection, all files in the Large Files can be checked with the **Cyren AntiVirus service**.

The files of 'Large Files' are removed from the Web Portal after expiration of the **Retention duration** and are no longer available for download.

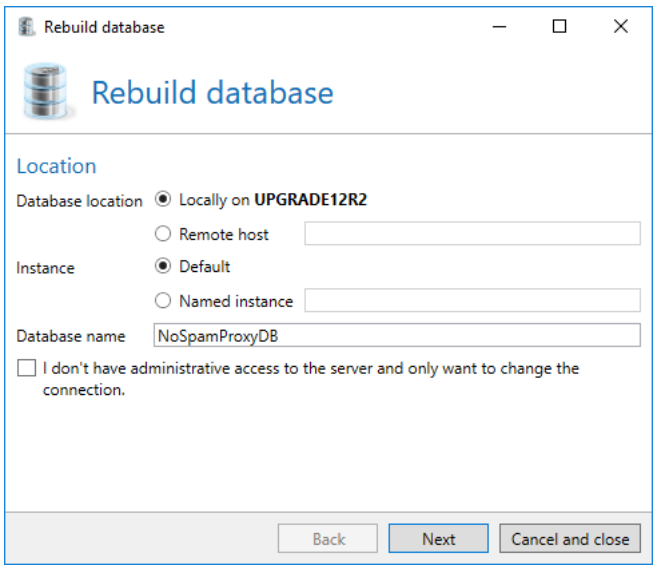


Picture 142: Settings for Large Files

Databases

Under **Database**, you can change the connection to the database of the respective role. The database is created during the setup. Changes need only be implemented in the case of a migration of the database to another SQL server. In this case, back up the existing database on the present SQL server and install this backup on the new database server. Change the connection to the new database server via **Modify**. (Picture 143).

Each role database is a self-contained installation and must not be shared between roles. If you use two Gateway Roles you also need two databases for these roles. They can located on the same database server or the same instance; in all other respects they are independent. Independent databases improve the stability of NoSpamProxy and they make administrative tasks like upgrades or a moving of the database much easier.



Picture 143: The connection to the database of the respective role

Under **Database location** you determine the server on which the database is located. If the database is located on the same server as the Gateway Role, select **On the local Gateway Role**. If the database is established on another server, first select the option **Remote host** and enter either the IP address or the fully qualified domain name (FQDN) of the server on which the database is located in the field **Remote host**.

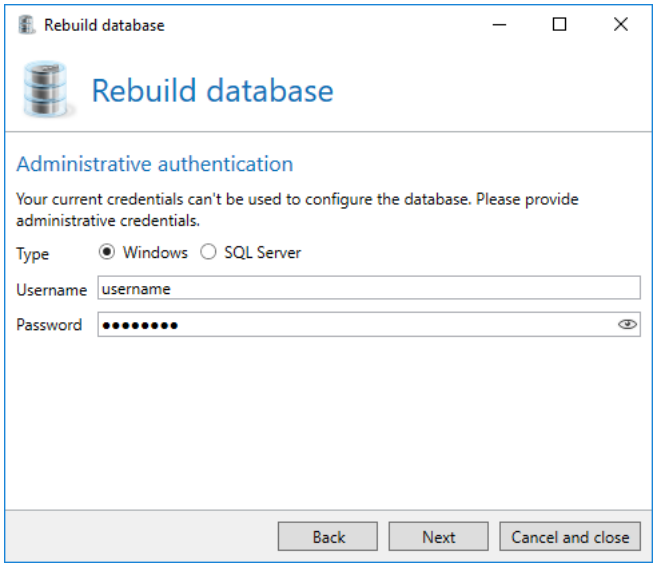
Under **Instance** you indicate whether the instance in which the database of the Gateway Role is located is the default instance of the SQL server or a named instance. If this concerns the default instance of the SQL server, you select the option **Default**. Otherwise, click on **Named instance** and enter the name of the respective instance into the field **Named instance**.

Enter the name of the respective database into the field, or, if several databases are required for the role, into the fields **Database name**. The following database names are used by default:

- **Gateway Role**
  `NoSpamProxyDb`
- **Intranet Role**
  `NoSpamProxyAddressSynchronization`

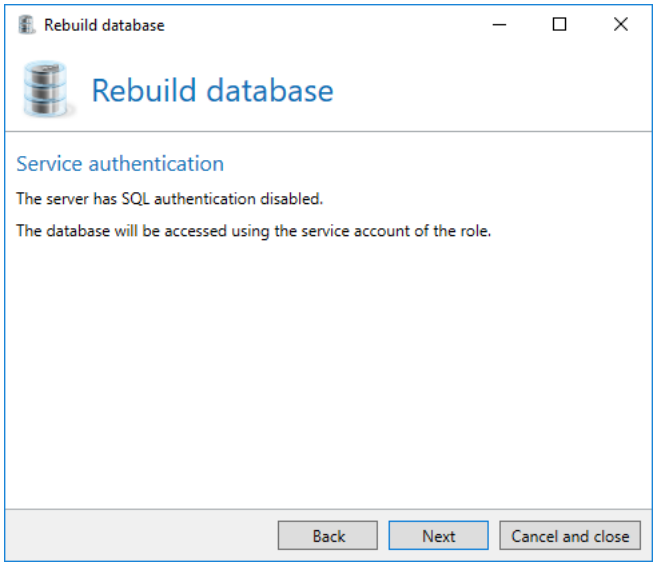
If you only wish to change the connection parameters, select the respective field in the bottom part of the dialog.

Under **Administrative Authentication** (Picture 144) you determine the user account used to add changes to the selected database. Select **Windows** if you wish to use a Windows user account. Otherwise, select **SQL server** and enter the login credentials into the fields **Username** and **Password**.



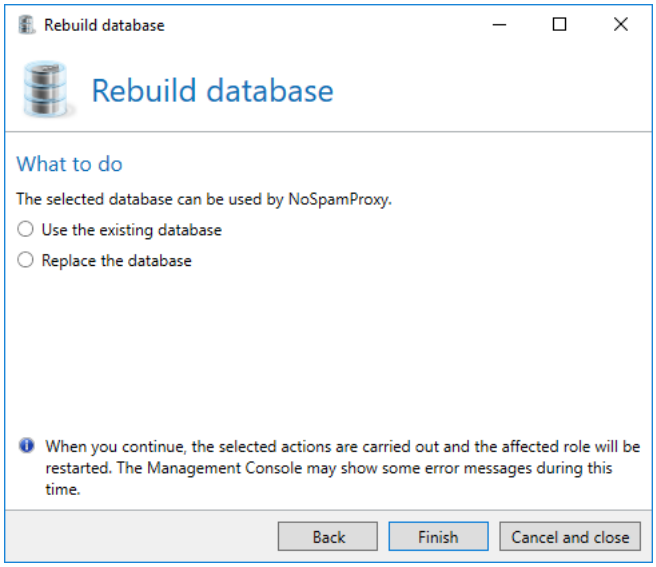
Picture 144: The connection to the database of the respective role

Under **Service authentication** you determine how the Gateway Role logs in to the SQL server. If the SQL authentication on the SQL server is deactivated, the integrated authentication must be used (Picture 145). Otherwise, you can either select integrated or SQL authentication here.



Picture 145: No SQL authentication available.

On the page **What to do**, you select the desired action. Depending on which database was found by NoSpamProxy, different possibilities are available here. Select the desired action and click on **Finish** (Picture 146).



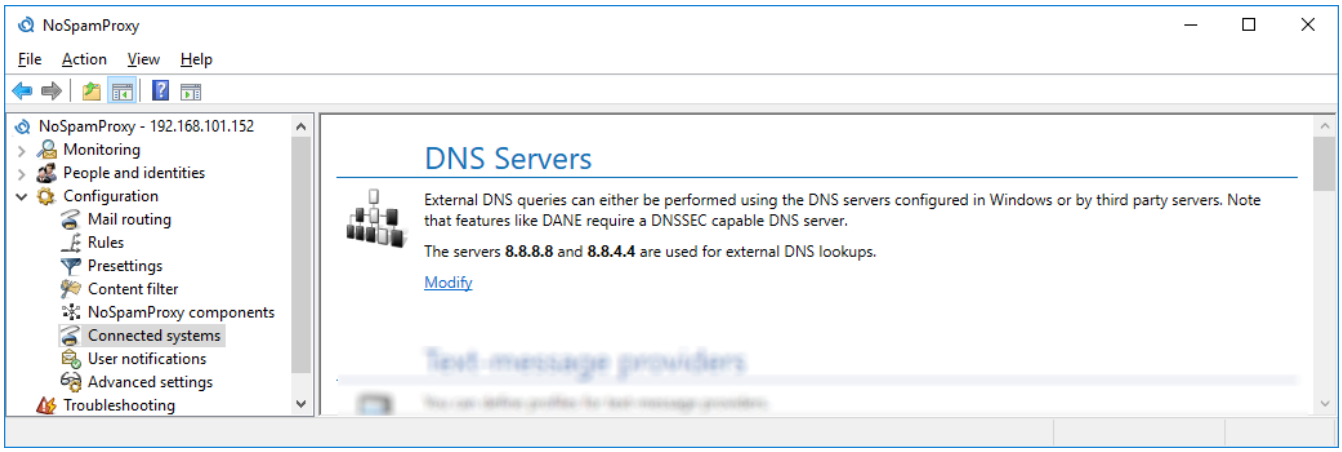
Picture 146: Select whether the old database should be deleted or retained

16. Connected systems

Connected systems comprises connections to products by third party providers which interact with NoSpamProxy.

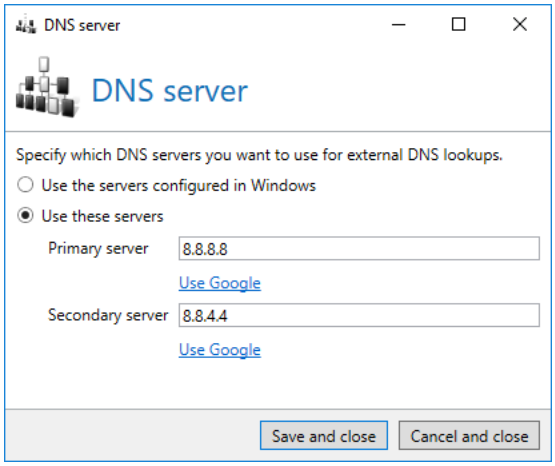
DNS servers

When applying DANE, you require a DNS server which supports DNSSEC. Since the DNS servers currently included in the delivery of Windows server operating systems do not support this function, you can establish a connection to this type of server here (Picture 147).



Picture 147: Connection to a DNSSEC enabled server

The configuration dialog provides the possibility to enter IP addresses of a primary and secondary server with DNSSEC support. With the help of **Use Google**, you can automatically enter the publicly accessible DNS server of Google into the configuration (Picture 148).

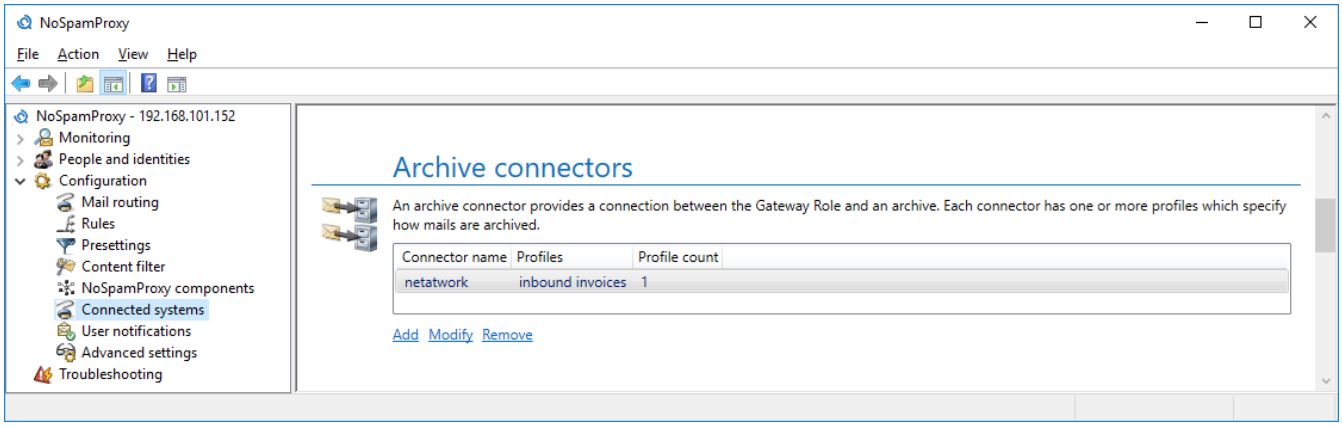


Picture 148: Configuration of a DNSSEC enabled server

DANE is used for the verification of the transport encryption during the delivery of emails to your partners. It can be configured in the Default partner settings.

Archive connectors

Via the archive connectors, emails and qualified signed documents can be transferred to an external archive system (Picture 149). Currently supported are the file system, a journalling mailbox as well as d.velop d.3. You can also use multiple archive systems at he same time.

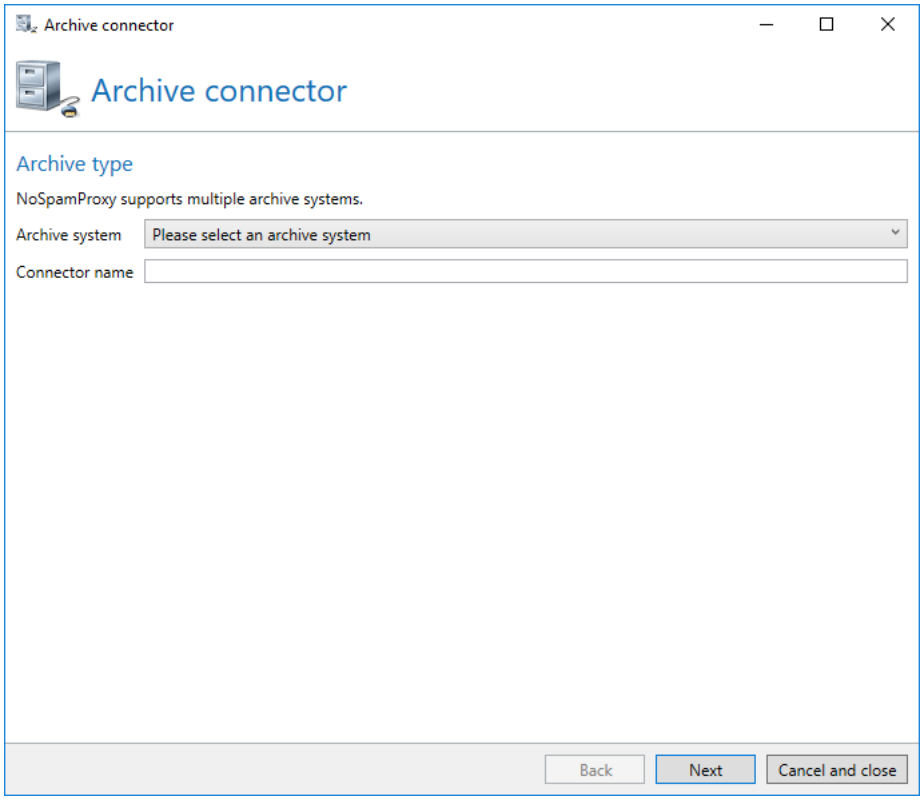


Picture 149: List of the configured archive connectors

The configuration consists of two parts: archive connectors and profiles. Connectors define the interface to an external archive system such as the file system. Within a connector, one or more profiles are created. Inside, properties such as the exact storage location for emails and documents can be

determined. Additionally, an assignment of email metadata to metadata of the archive system is implemented if required.

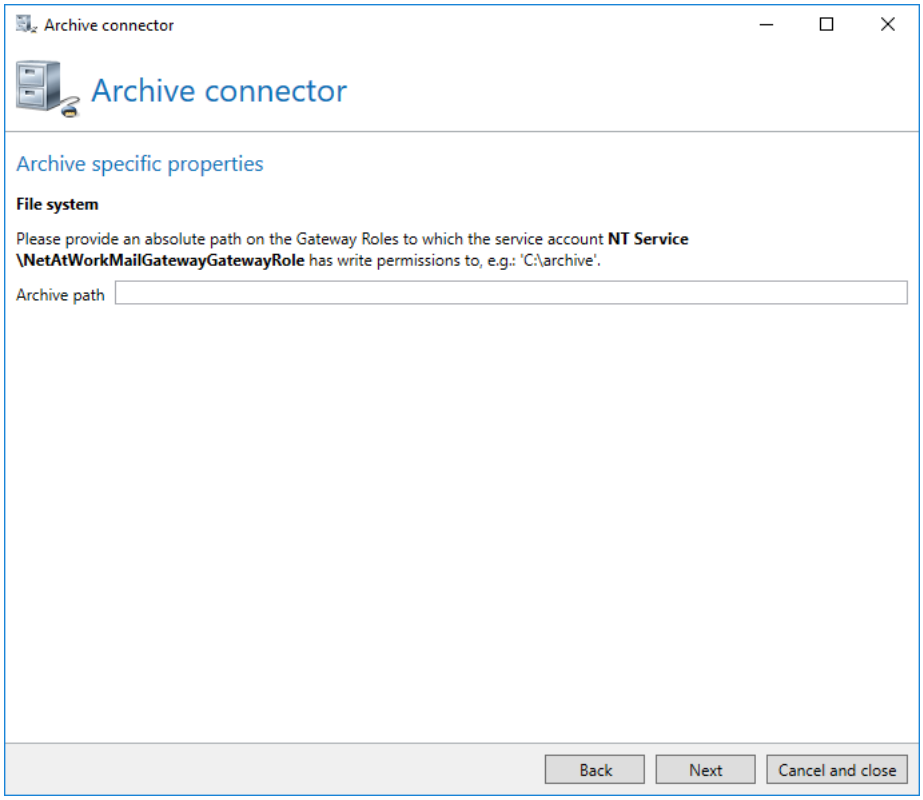
To create a new connector, click on **Add**. First, select the connector type and give the connector a new name (Picture 150).



Picture 150: General settings for the archive connector

The options to be configured in the second step depend on which archive system you have selected in the first step.

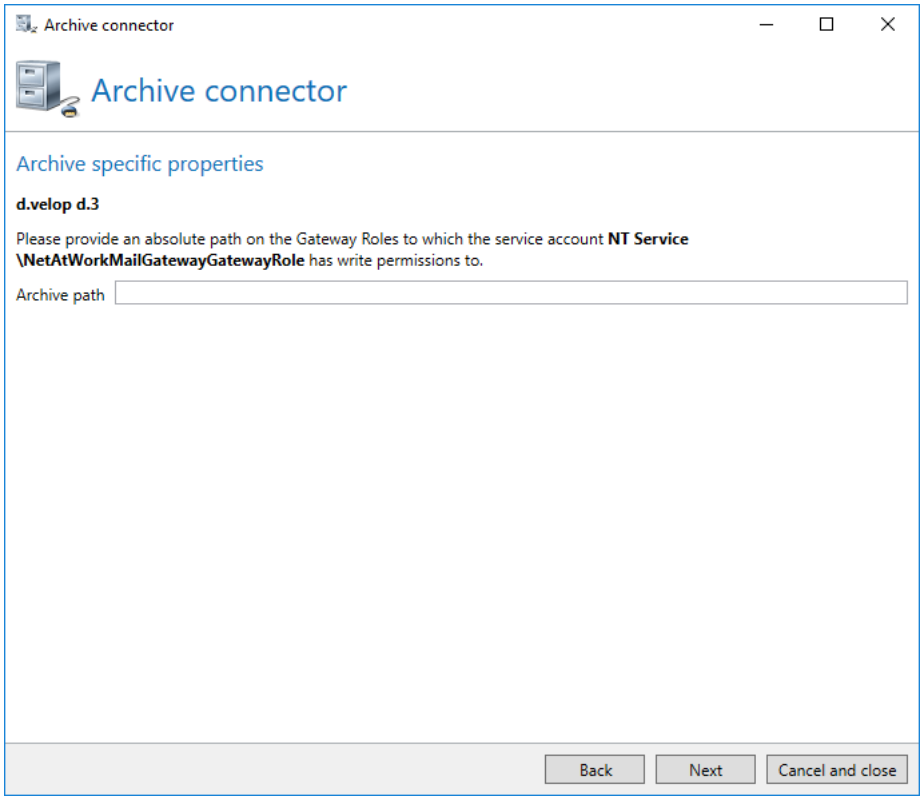
When archiving emails and documents in the **File system**, you only need to indicate a path. Emails and documents are stored in folders in this path (Picture 151).



Picture 151: Properties for the storage in the file system

The connector for the **Journaling mailbox** does not have any further settings on the connector. The profiles are displayed.

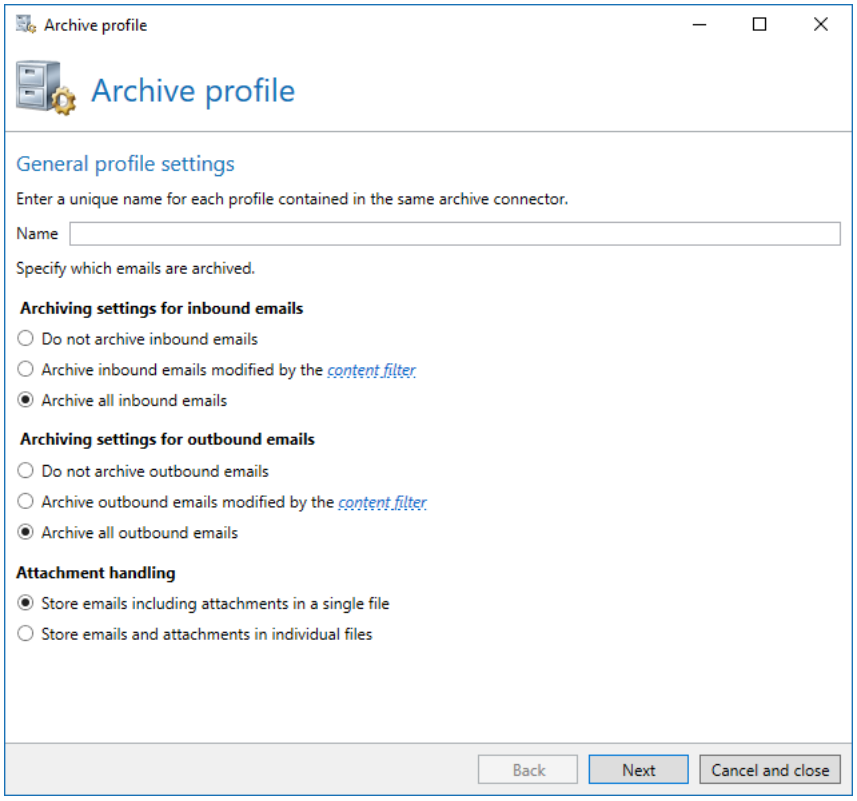
For a connector to a d.velop d.3 system, you only need to enter a path (Picture 152). Emails and documents are written into this directory and obtained from it by the d.velop d.3 system.



Picture 152: d.velop d.3-specific settings

On the next page, you can create profiles for this connector. Among other things, profiles enable you to allocate emails and documents within an archive system to different folders.

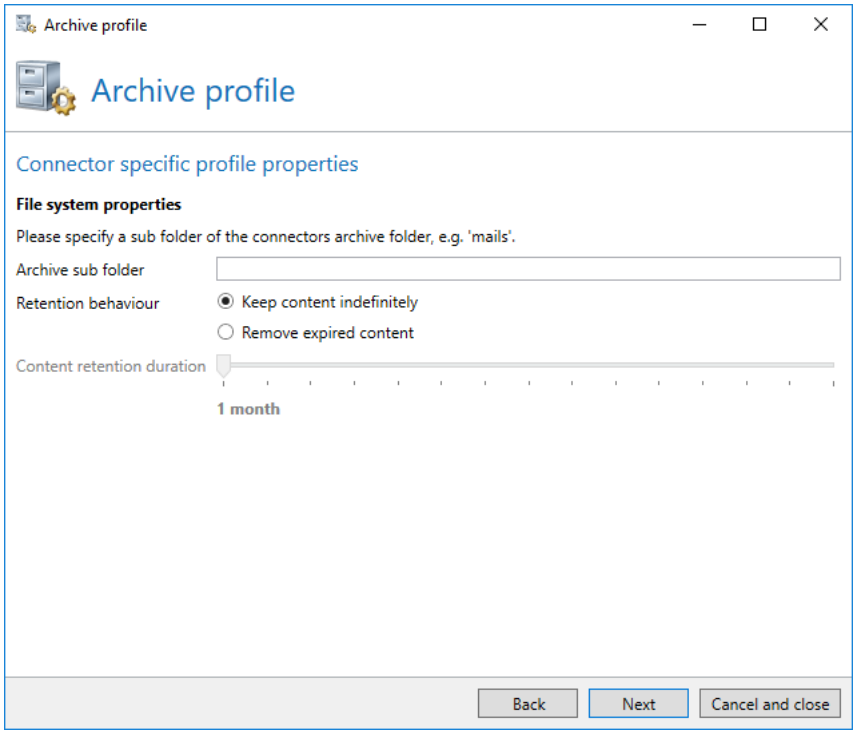
First, enter a name for the new profile. (Picture 153). Then, select which emails are archived by this profile.



Picture 153: General profile settings

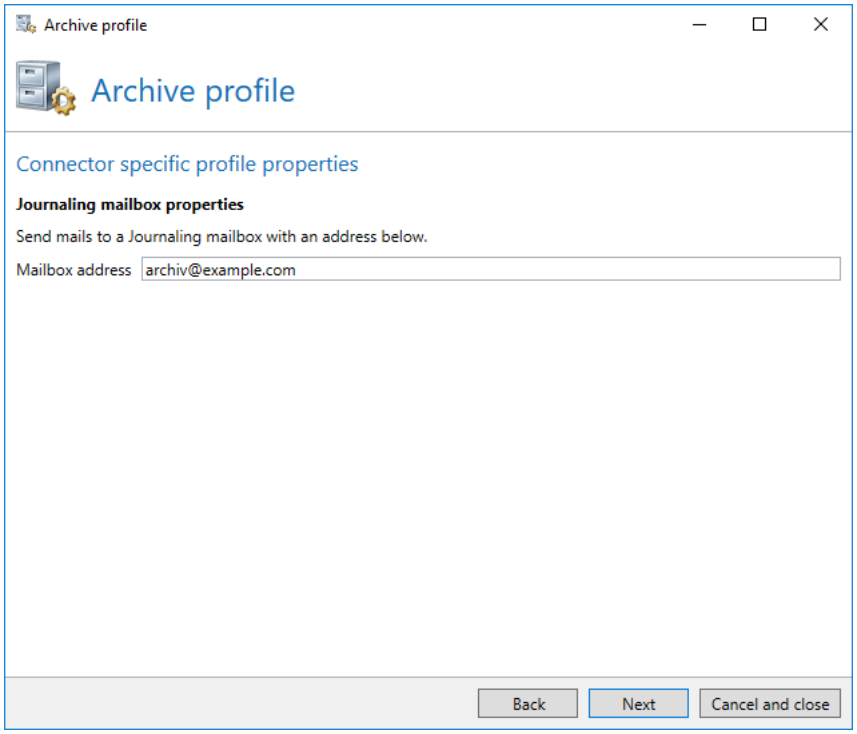
The content of the second page depends on the archive system you selected.

For storage in the **File system**, you can specify a subfolder for the emails stored by this profile.



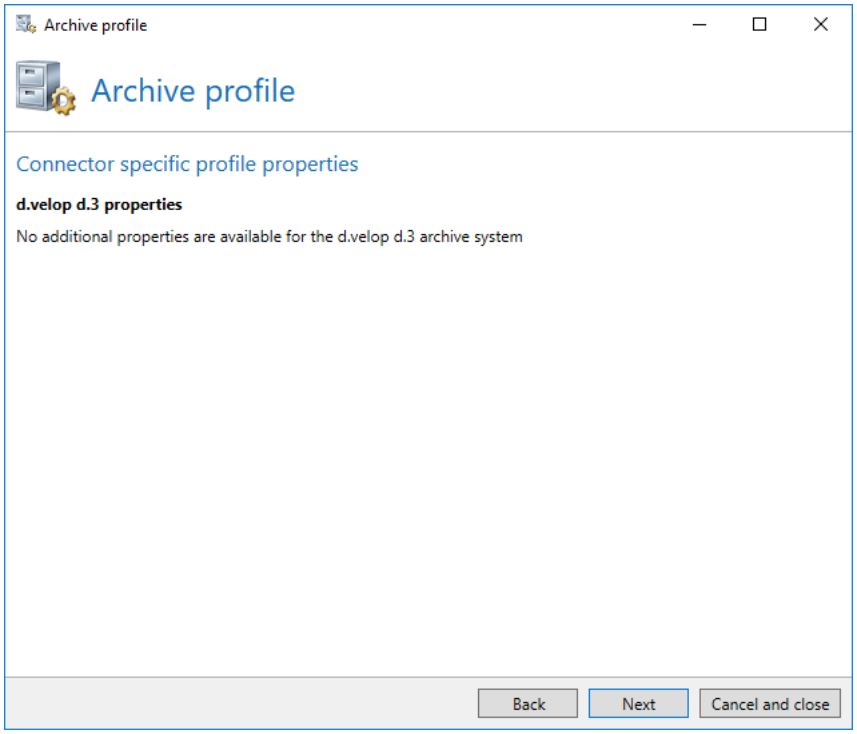
Picture 154: Properties for the storage in the file system

Journaling mailboxes require the email address of the target inbox (Picture 155).



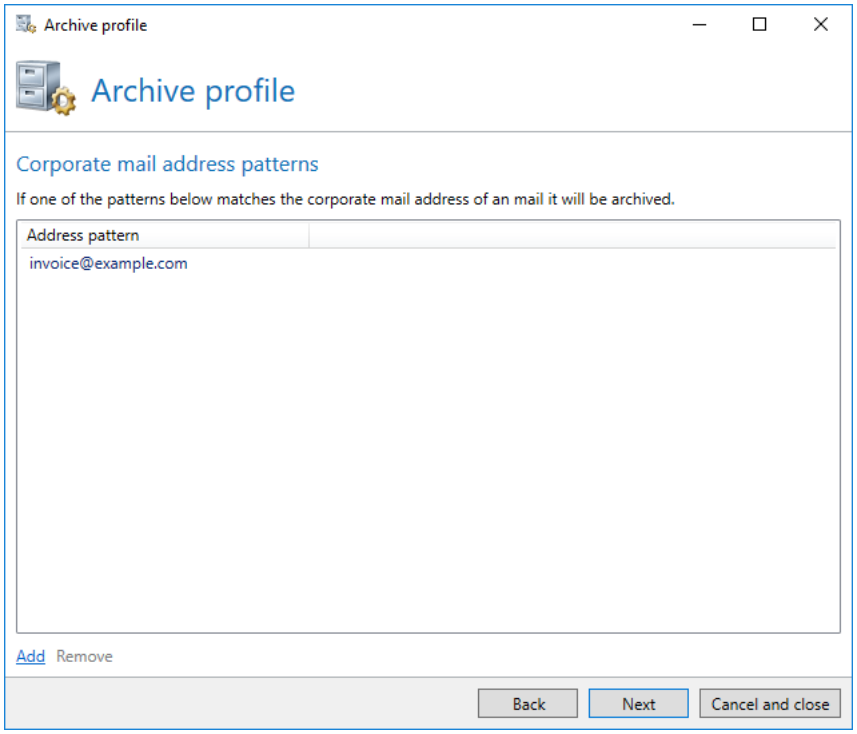
Picture 155: Properties for the storage in an journaling mailbox

For a connection to a d.velop d.3 system, no further configuration is required. In this case, the dialog is empty (Picture 156).

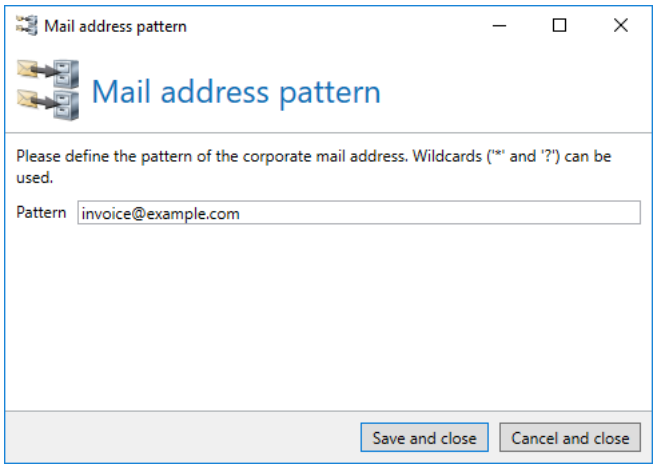


Picture 156: Properties for the storage in d.velop d.3 system

In the next step, you determine local email addresses this profile is responsible for. (Picture 157). When sending emails, the address of the sender is always used to determine which profiles are used for the archiving. As for emails to local addresses, the addresses of the recipients are used. When indicating the email addresses (Picture 158), you can also use wildcards ('*' and '?') to provide multiple addresses. Should several profiles correspond to the data provided here during an archiving process, the email is archived several times.



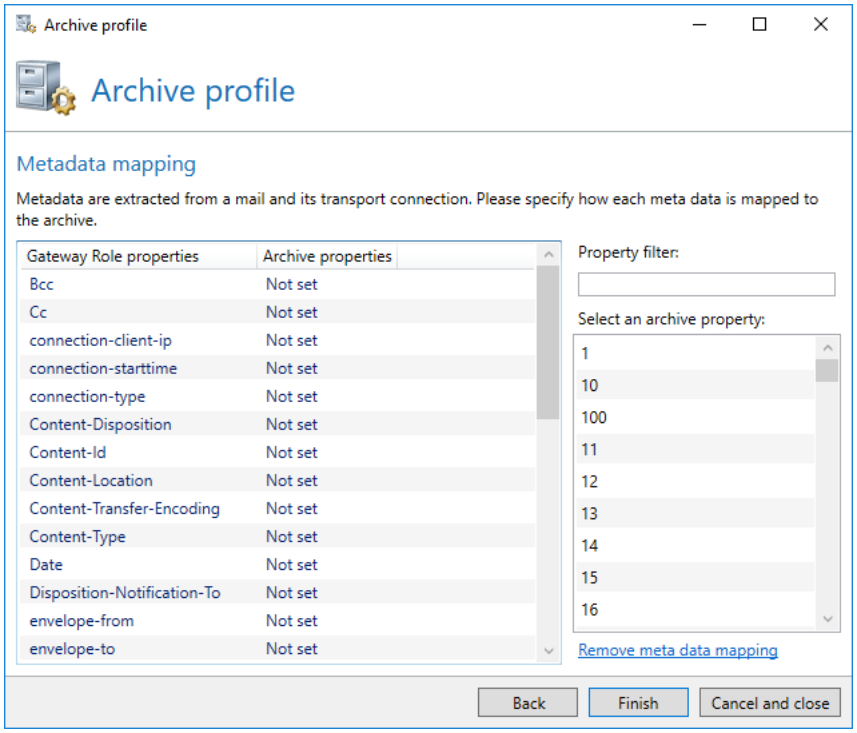
Picture 157: Assignment of profiles to internal email addresses



Picture 158: Create new assignment

In the last step, you define in a profile how metadata of an email are mapped to metadata in the archive. Among other things, metadata comprise the subject line, signature and encryption options and other email header information. To create a mapping of the values, initially select a value on the left. Afterwards, select a field from the archive from the list on the right. Depending on the selected archive system, the list with the available field can be very long. You can search for specific fields via the property filter. As soon as you select a field from the list, the mapping is established (Picture 159).

On a profile for an journaling mailbox, no metadata mappings are configured since the entire email is forwarded to the journalling mailbox and thus all metadata in the email are retained.

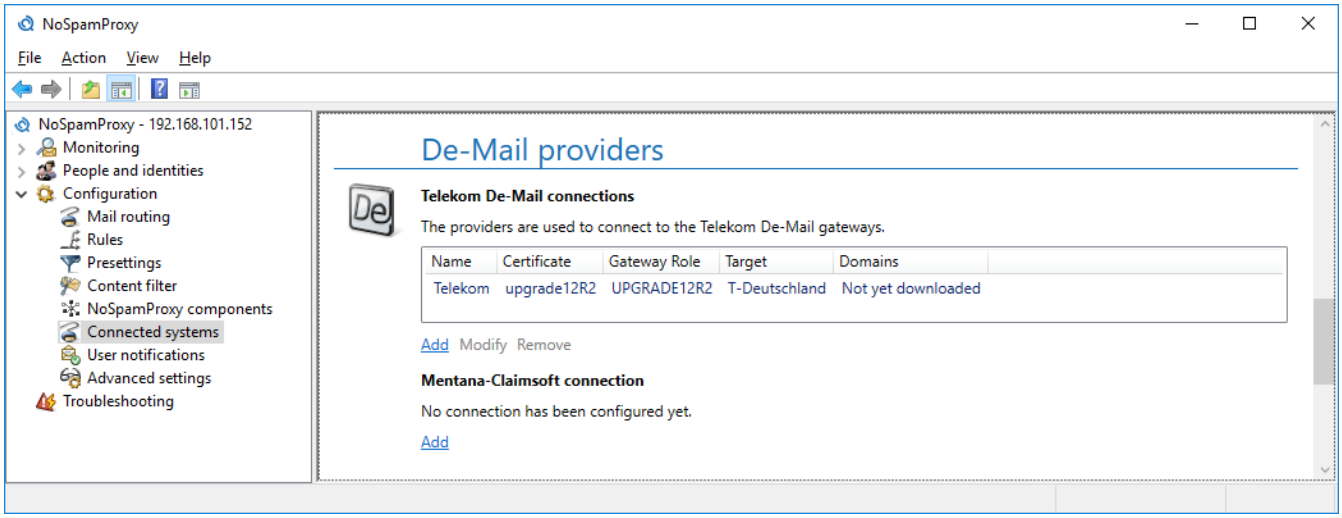


Picture 159: Metadata mapping

After you have created at least one profile, the configuration of the connector is completed.

De-Mail providers

Here, you can configure the connections to the De-Mail system (Picture 160).

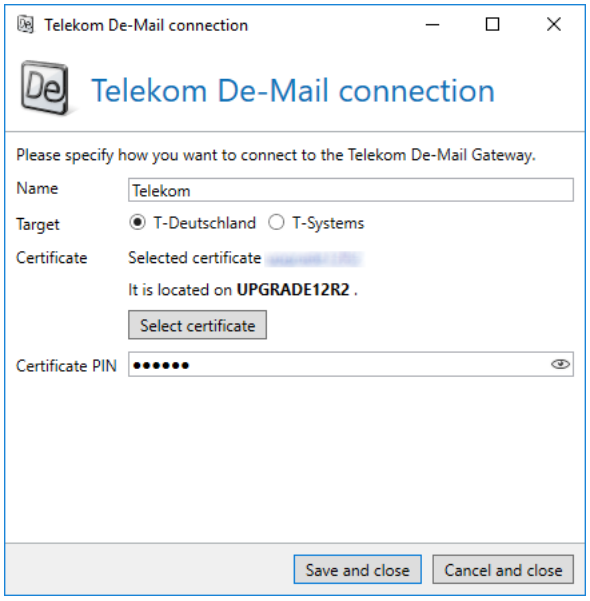


Picture 160: The list of the configured De-Mail connections

The information entered in this section is immediately available for the De-Mail send connectors as well as for the receive connectors. This means that you only need to configure the connection once and it is directly available for all connectors.

Telekom De-Mail connections

To create connectors for De-Mail via Telekom, you must first configure the connections to the service provider. (Picture 161).



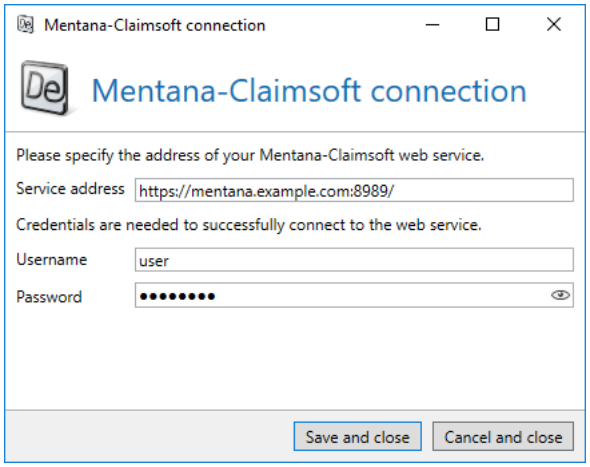
Picture 161: Configuring the connection to the Telekom De-Mail provider

In addition to the profile name, select whether you wish to establish the connection via T-Deutschland or T-Systems. Furthermore, select the certificate used for the protection of the connection to the service provider. Since the certificate is stored on a smart card, you must enter the PIN of the card as well.

By selecting the certificate, the profile is automatically linked to a Gateway Role. Connectors using the profile are automatically mapped to the Gateway Role on which the certificate is located.

Mentana-Claimsoft connection

A connection to the web service of this provider must be established for the De-Mail connectors of Mentana-Claimsoft (Picture 162).



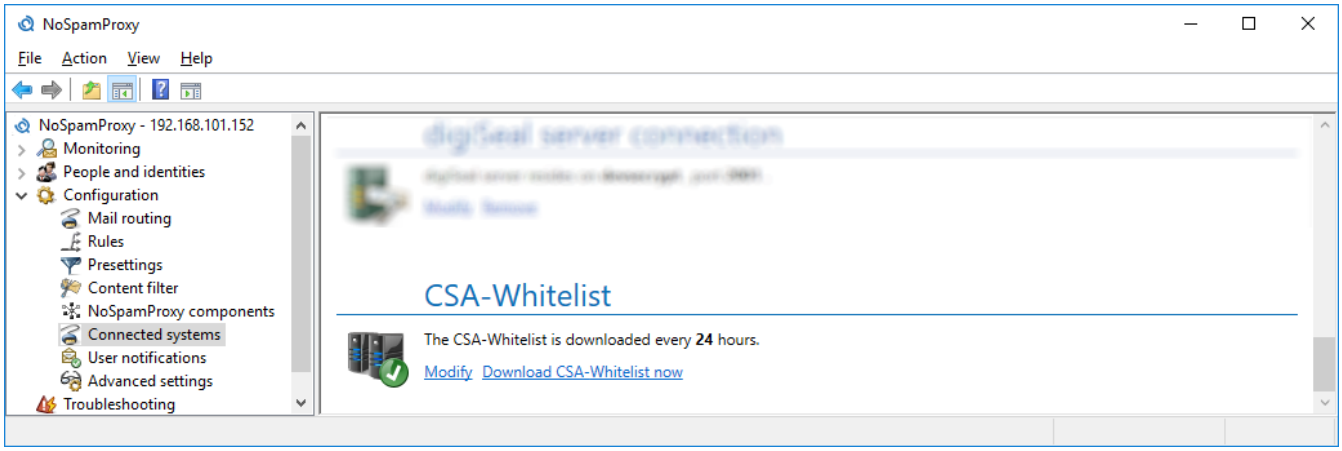
Picture 162: Connect to the Mentana-Claimsoft web service

Enter the address used for the web service in **Service address**. Enter the login credentials for access to the service into the fields **Username** and **Password**.

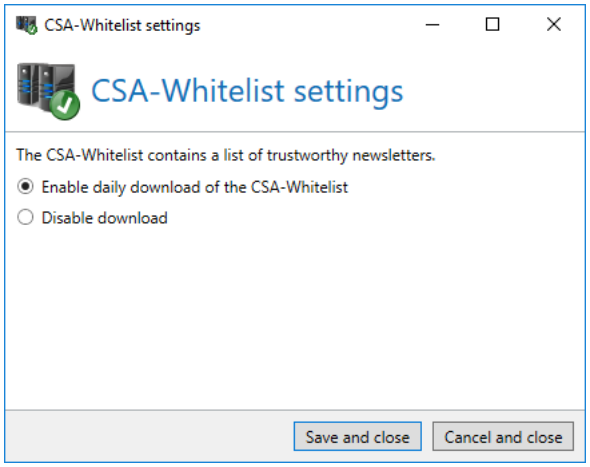
The information entered in this dialog is immediately available for the De-Mail send connectors as well as for the receive connectors. You only need to configure the connection once; it will be instantly available in all connectors.

CSA-Whitelist

To use the CSA-Whitelist action, you must configure the download of the list first (Picture 163). To do so, select **Modify**. The dialog for configuration opens (Picture 164).



Picture 163: Connection to the CSA-Whitelist



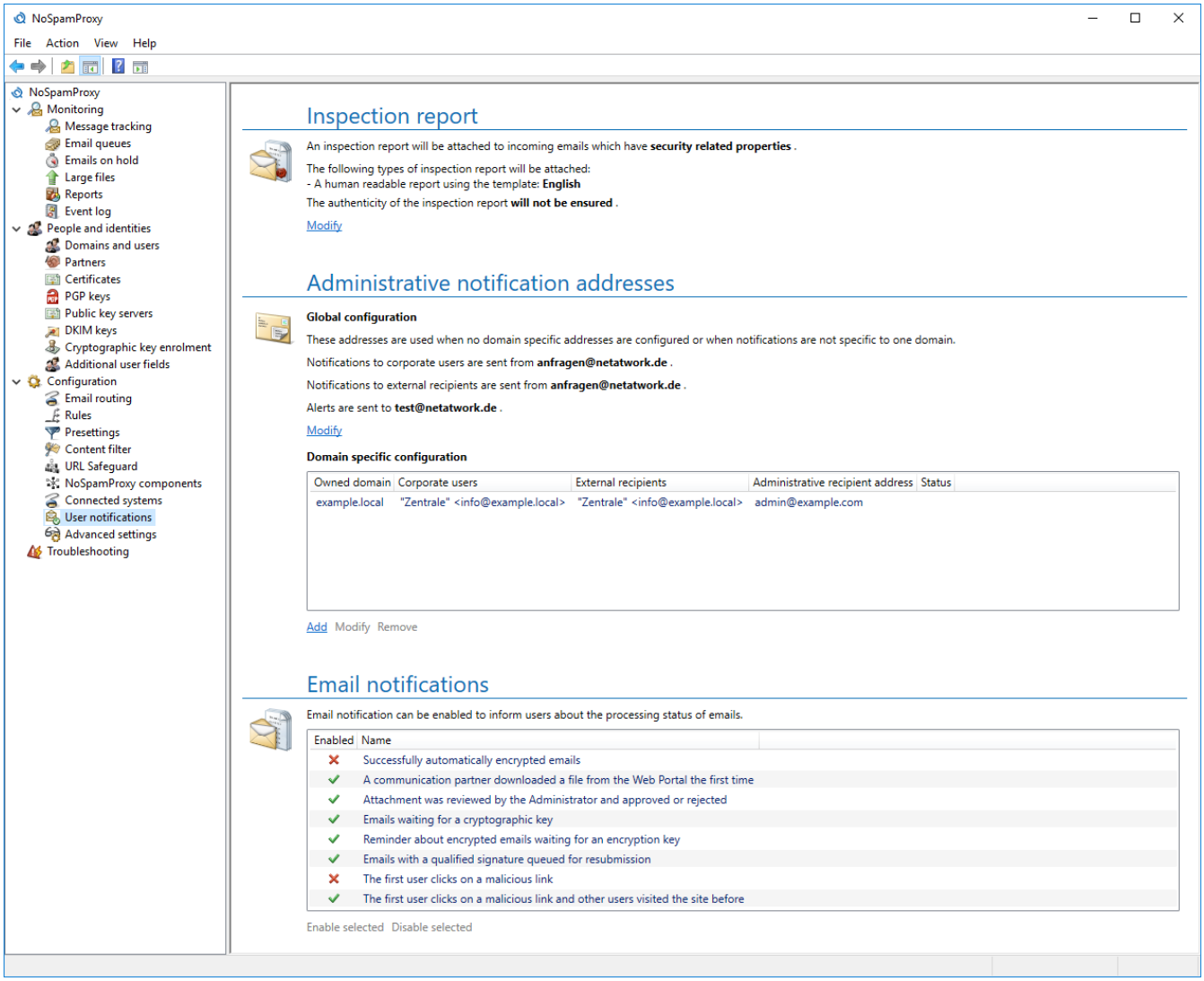
Picture 164: Configure the download of the CSA-Whitelist

Select **Enable daily download of the CSA-Whitelist** if you wish to use the CSA-Whitelist action. Otherwise, select **Disable download**.

The CSA-Whitelist is downloaded from the domain `service.nospamproxy.de`. In order for NoSpamProxy to be able to download this list, access to this address is required. Make sure to configure your firewall accordingly, if required.

17. User notifications

Under **User Notifications**, you can determine which messages are automatically sent to internal and external contacts by NoSpamProxy. Moreover, you can determine which sender addresses are used (Picture 165).



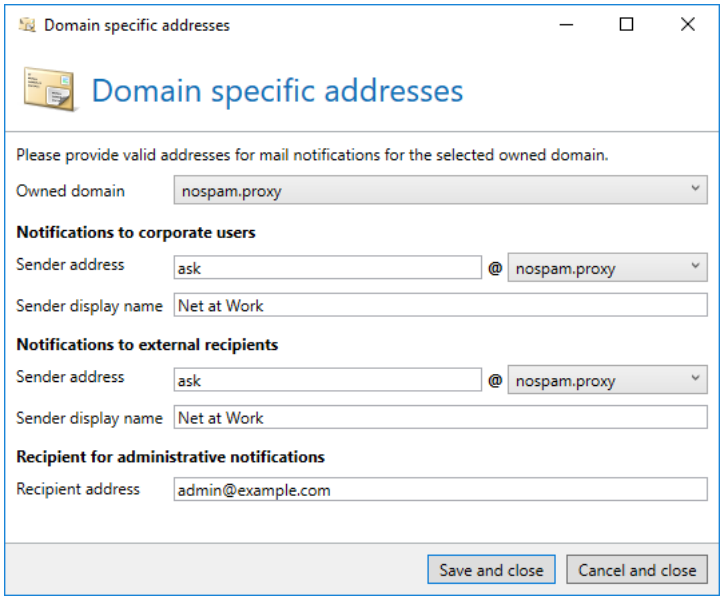
Picture 165: User notifications

Administrative notification addresses

In this section, addresses for notifications of NoSpamProxy are deposited (Picture 166). NoSpamProxy requires valid sender addresses to be able to send email notifications. Depending on whether the recipient is a corporate user or not, different sender addresses can be used. For notifications about

certain incidents, a recipient address is required for these notifications. Enter the address in the field **Recipient address**.

Under **Global configuration**, provide the addresses for all domains which have no individual entry or for notifications which are not mapped to a domain.



Picture 166: The global notification addresses

If a domain requires a configuration deviating from the global settings, you can add it in the list **Domain specific configuration**. The setting dialog is identical to the global configuration. Additionally, you need to select one of your owned domains to which this configuration should be applied.

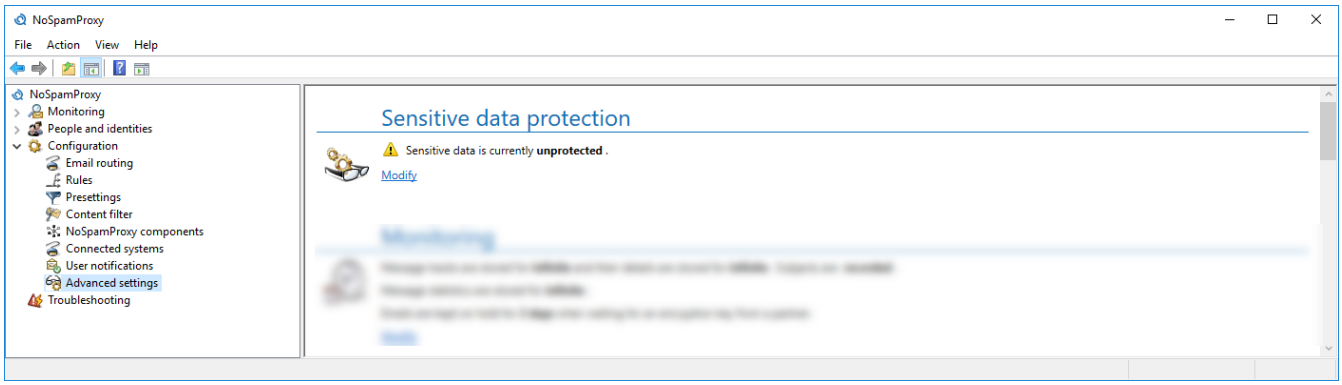
Email notifications

The configurable notifications are shown here. You can mark the individual notification and activate or deactivate it.

18. Advanced settings

Under "Advanced settings", you find configuration options which usually do not need to be adjusted .

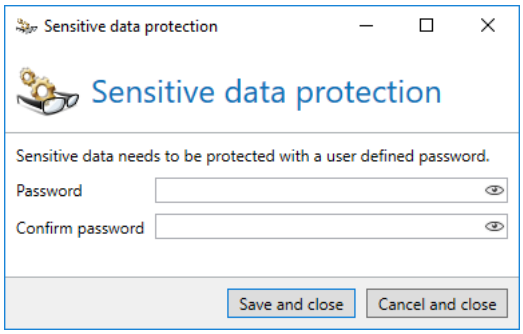
Sensitive data protection



Picture 167: Settings for the protection of sensitive data

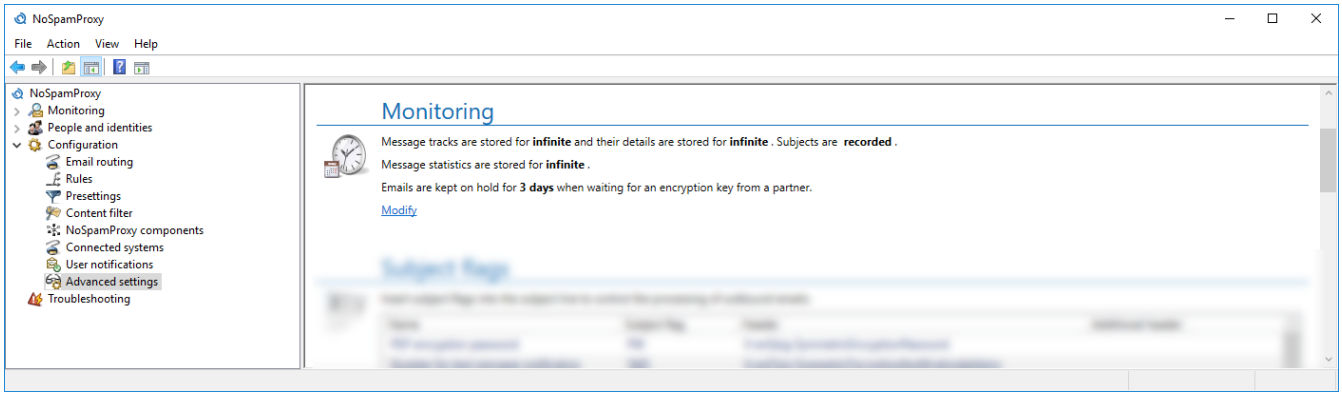
To protect sensitive data such as cryptographic keys or authentication information from access by third parties, the data must be encrypted through the use of a password determined by you (Picture 168). You can change the password at a later point in time, but the protection of data is irreversible.

In case the configuration with the encrypted password is deleted, there is no possibility of accessing the protected data. Make sure you always keep a safe copy of the password stored in a safe place.



Picture 168: The password for protection of your data

Monitoring

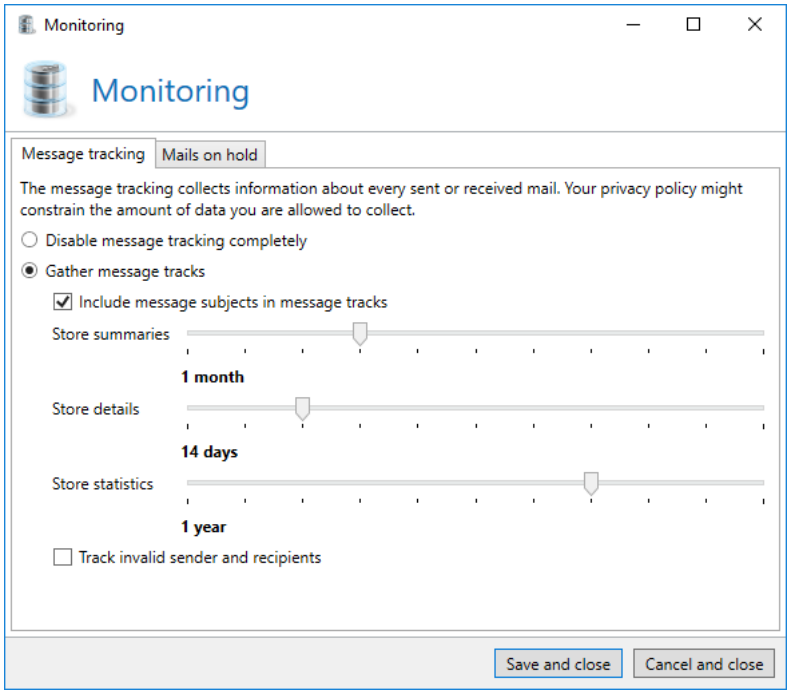


Picture 169: Monitoring settings

NoSpamProxy can log each connection in the message tracking in order for you to be able to access information on how specific emails have been handled. This function can be deactivated via the option **Monitoring**. If this option is activated, you can also decide whether the subject lines of emails are stored as well or whether they are excluded from message tracking. By default, both options are activated.

Always consider the data protection policies prevalent in your company during the configuration of this section.

To prevent uncontrolled growth of the message tracking and reports database, the Intranet Role cleans the database on a regular basis. In doing so, all elements which have exceeded a certain retention period are deleted from the database (Picture 170).



Picture 170: Adjustment of the retention period

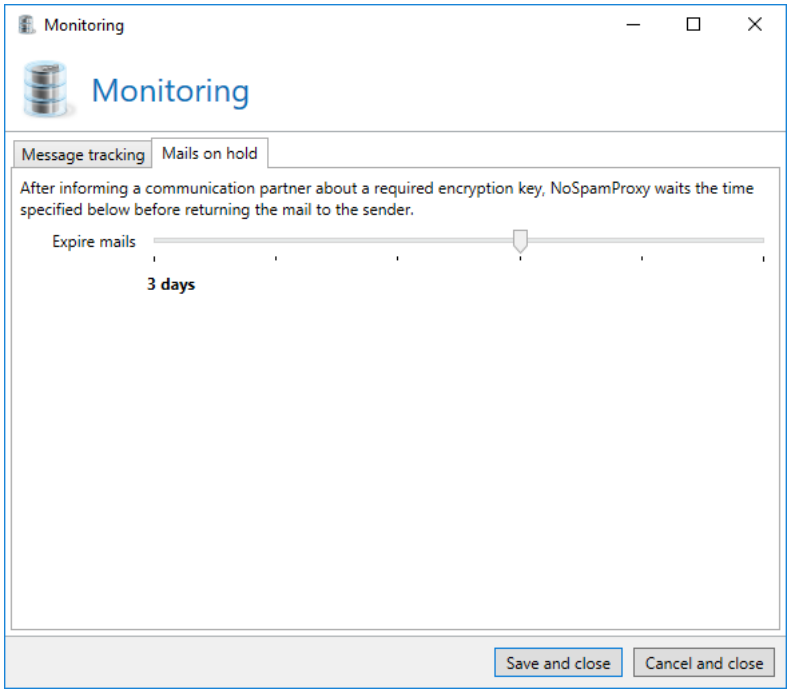
If all message tracking datasets and the statistical data should be removed, please select the option 'Disable message tracking completely' under 'Advanced settings' of the Gateway Role. In this case, no data is gathered at all. If you, for example, only wish to keep the statistical data, select the option **Message tracking datasets are deleted immediately** to delete all message tracking datasets at 2 o'clock in the morning.

The slider **Store summaries** controls how long emails are backtracked. The message overview information only provides information on whether and when the respective email was delivered and whether it was accepted or rejected (available in the overview of the message tracking). The retention period for the corresponding message details is set with the slider **Store details**. The assessment results of the individual filters, the origin of the email, the duration of the validation as well as other useful information are included in the message details. Since this information constitutes the largest part of the message tracking, it is possible to retain it for a shorter period than the overview information.

The slider **Store statistics** controls the content of the reports. With it you can set the interval between report creation. In order to be able to create a relatively convincing report, we recommend a minimum retention period of 12 months.

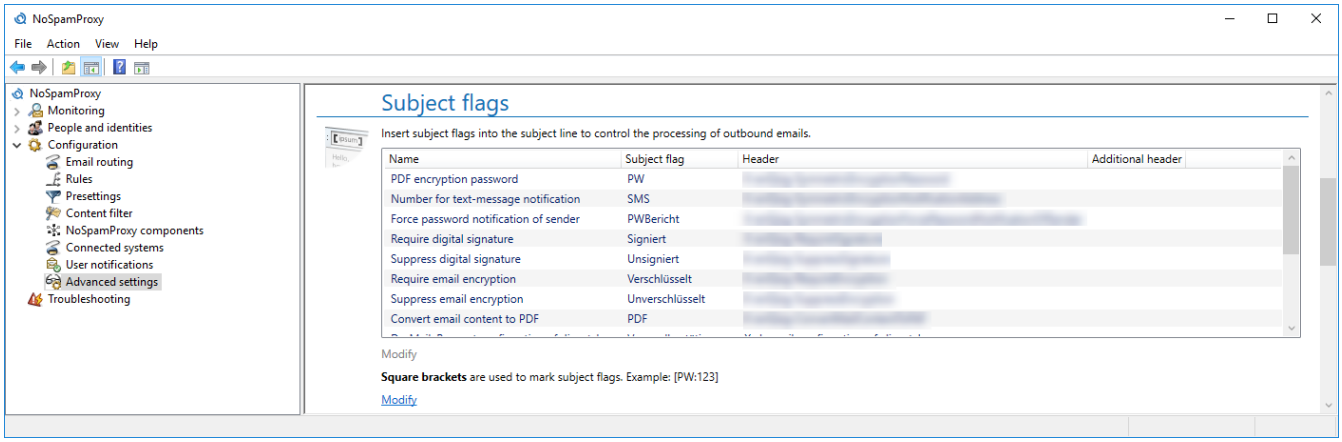
If you receive a large amount of emails or spam emails per day (e.g. tens of thousands), it is possible that the database size limit of your SQL server in the Express Edition is exceeded. In this case you should consider choosing shorter retention periods for message tracking datasets, or installing an SQL server database without this type of restriction.

Apart from the settings for the message tracking, you can configure how long NoSpamProxy withholds emails for which an encryption key is awaited.



Picture 171: Adjustment of the retention period for halted emails

Subject flags

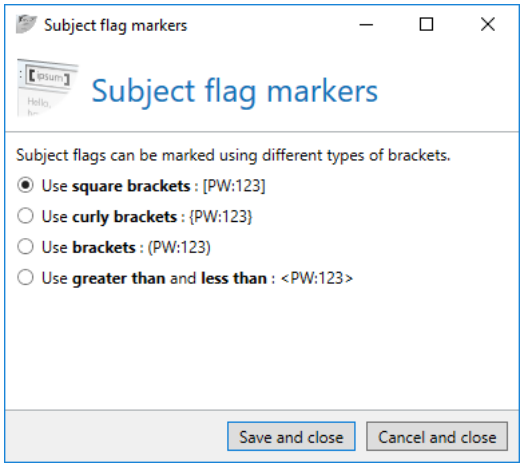


Picture 172: Settings for subject flags

The subject flags define keywords 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 by NoSpamProxy before dispatch.

Use the subject flags which define your tasks by providing the keywords from the following list in brackets at the beginning or end of the subject line. Blank spaces and capitalisation are ignored in keywords. This means that the following examples all show the same result. Alternatively, you can use the **Outlook Add-In of NoSpamProxy**.

By default, square brackets are used to mark the subject flags. Via the dialog for editing the marking, you can determine which type of mark should be used (Picture 173).



Picture 173: Configure the markers for subject flags

Examples for the use of subject flags in the subject line:

```
[pw:secret4312] I hereby send you the encrypted document
```

```
[ PW : secret4312 ] I hereby send you the encrypted document
```

Or several simultaneous flags within one bracket `[Unencrypted, PDF, PW:secret4312] I hereby send you the encrypted document`

Or several simultaneous flags within different brackets `[Unencrypted] [PDF] [PW:secret4312] I hereby send you the encrypted document`

Subject flags need to be placed at the beginning or the end of the subject line in order to be processed properly.

Depending on the functions licenced, other flags than those in the above examples might be available. The above advice is valid for all flags.

The following subject flags are available:

- **[AP]**
  Attachment password: Protects all attachments with a password which must be entered by the recipient before downloading the attachments. This feature is available in NoSpamProxy Large Files.

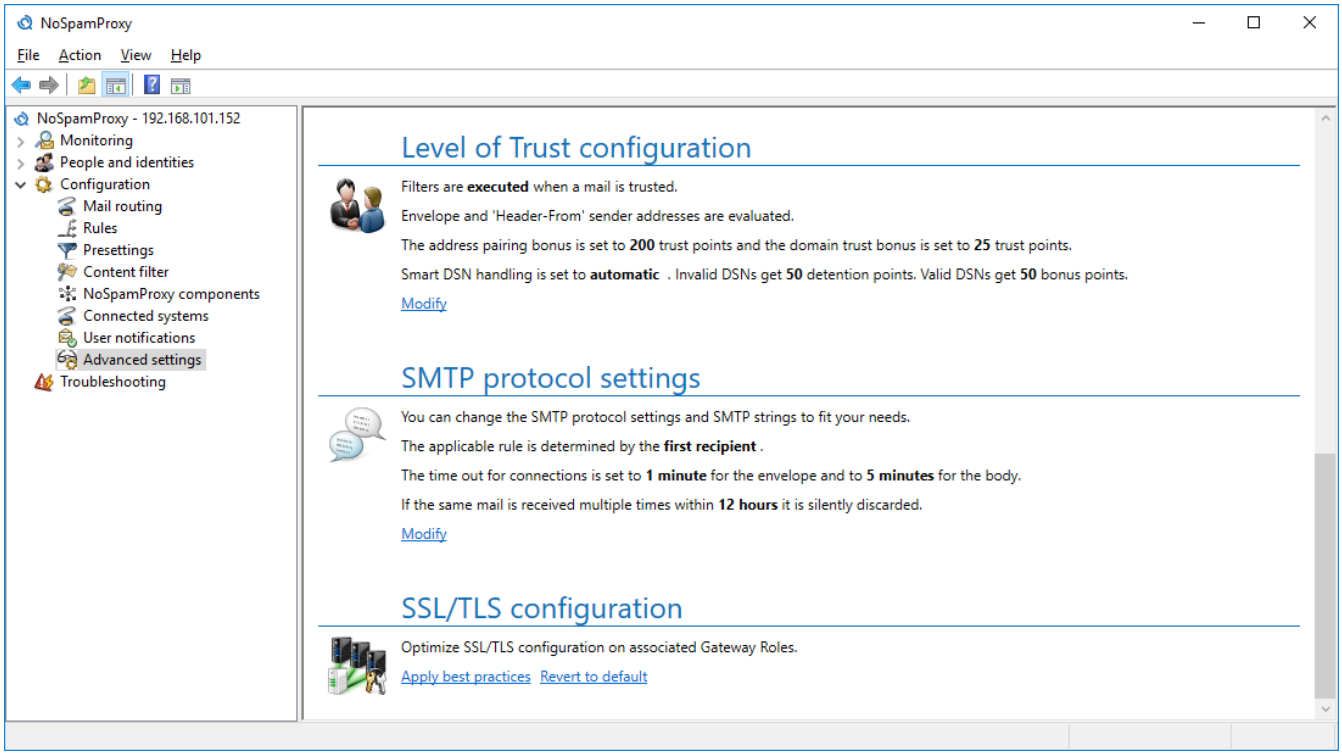
You can adapt the subject flags to your needs (Picture 174) as well as reset them to their default values.

In the Outlook Add-In, you can configure that the subject flags should be used instead of the X-Headers. In this case, do not implement any changes. Otherwise, the Add-In will no longer work.

Picture 174: Edit subject flags

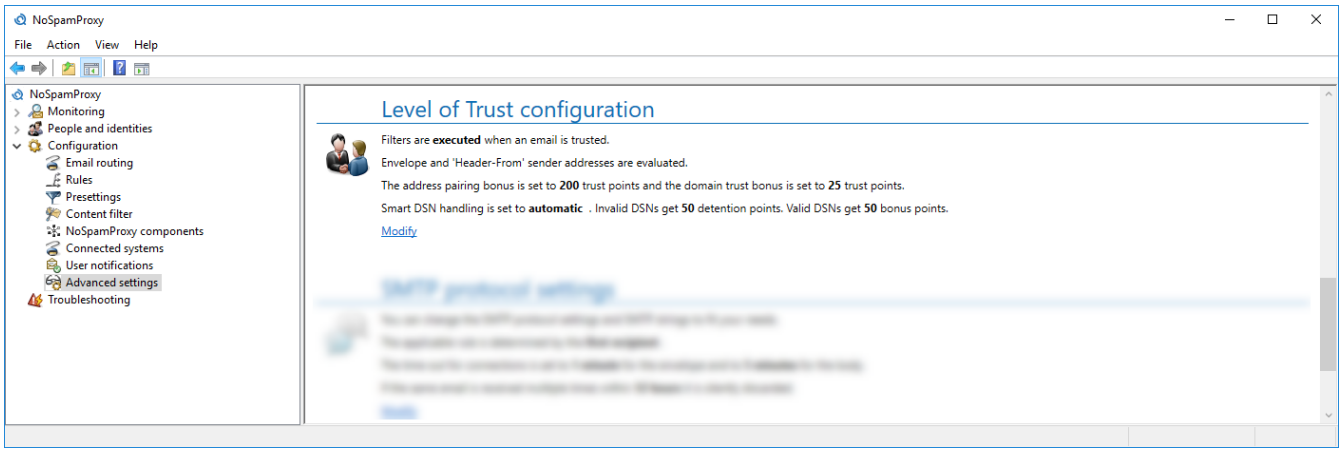
For automatic dispatch of emails, you can insert additional X-Headers into the message instead of Subject flags to provide this information. The X-Headers are explained in the following. On the client, you can use the corresponding X-Headers next to the subject flag. If you are already using a software which sets subject flags and employs them for the function in NoSpamProxy, you can define additional X-Headers in the edit dialog. It is then used in addition to the regular X-Header.

Instead of using the 'subject flags', you can install the NoSpamProxy **Outlook Add-In**. The Outlook Add-In is used instead of the subject flags with Microsoft Outlook.



Picture 175: Advanced settings of NoSpamProxy

Level of Trust configuration



Picture 176: Level of Trust configuration

The Level of Trust system is a multilevel concept which assesses the trustworthiness of your contacts or a domain. "Trust" must be earned by the sender. The most essential plus factor is a reliable and constant connection history.

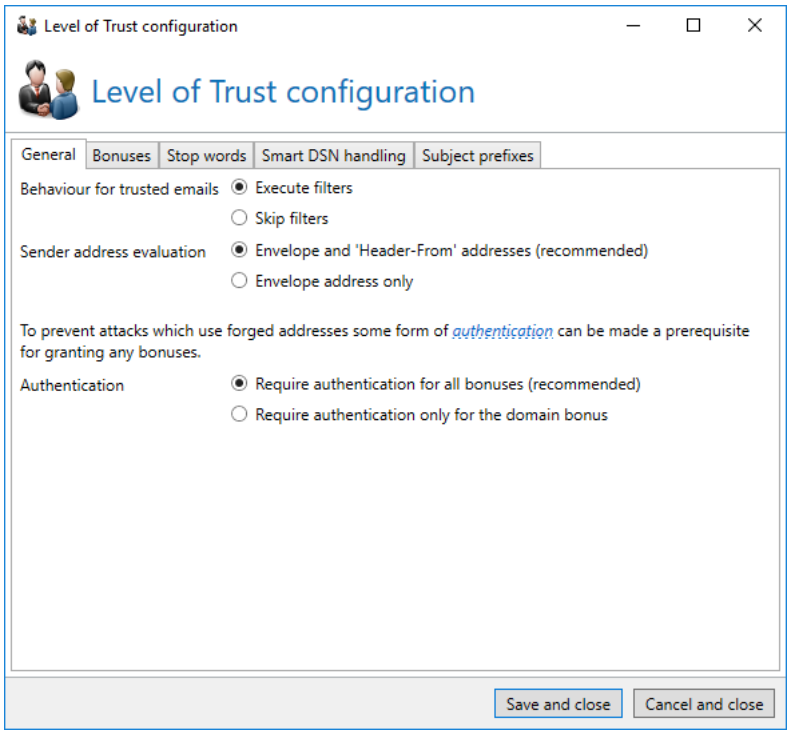
The system assesses different criteria such as sender addresses and checksums but, above all, the address relations between senders and recipients of emails.

For emails to external addresses, the communication relation (between sender and addressee) is stored in the database with a very high trust bonus. To protect these data, the relation is not stored in plain text but rather as a hash value (checksum) only. Moreover, the relation of sender, subject and domain of the recipient is of great interest. It is reasonable to additionally be able to assess a reply of a colleague or a representative and, if required, an alternative address as "good". Additionally, the trust in the domain of emails by the addressee is increased by a specific value. Thus, email replies from the addressee to other users of the system receive a bonus as well. If an email to local addresses is classified as spam, the trust in the domain is diminished.

If no communication takes place with a specific sender within a specific time, the Level of Trust is diminished automatically. This reduction of the value ensues for bonus as well as minus values. A longer period of "silence" is can have both a positive as well as in the negative effect; reliable, constant communication yields increasingly positive results while repeated spam attacks yield increasingly negative results.

The Level of Trust system must be activated per rule. The settings are, however, implemented globally in the menu "Level of Trust" (Picture 177).

General



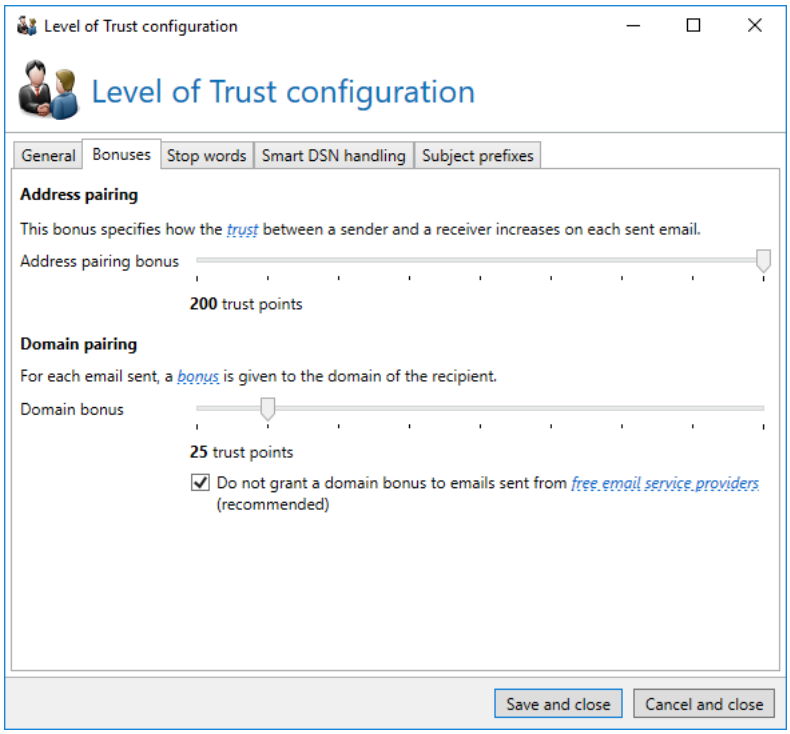
Picture 177: Defining the general settings of the Level of Trust system

If the option **Skip filters** is selected under **Behaviour for trusted emails**, emails to local addresses with a sufficient Level of Trust rating will be marked as trustworthy. In this case, all filters defined on a rule will be skipped. Only actions such as the Cyren AntiVirus action can prevent the acceptance of the email.

If the addresses in the email envelope and in the 'Header-From' field differ, you can configure which address is used by NoSpamProxy for analysis. If both addresses are validated and the envelope address permits delivery of the email, the result from the 'Header-From' address overwrites the prior result. As a consequence, a questionable validation rejects the email, regardless of it being detected in the email envelope or the 'Header-From' address.

If the option **Require authentication for all bonuses (recommended)** is selected under **Authentication**, address pairing and domain bonuses will only be granted if the DKIM, S/MIME and SPF checks returned positive results (see **Bonuses** tab).

Bonuses



Picture 178: Settings for address and domain bonuses

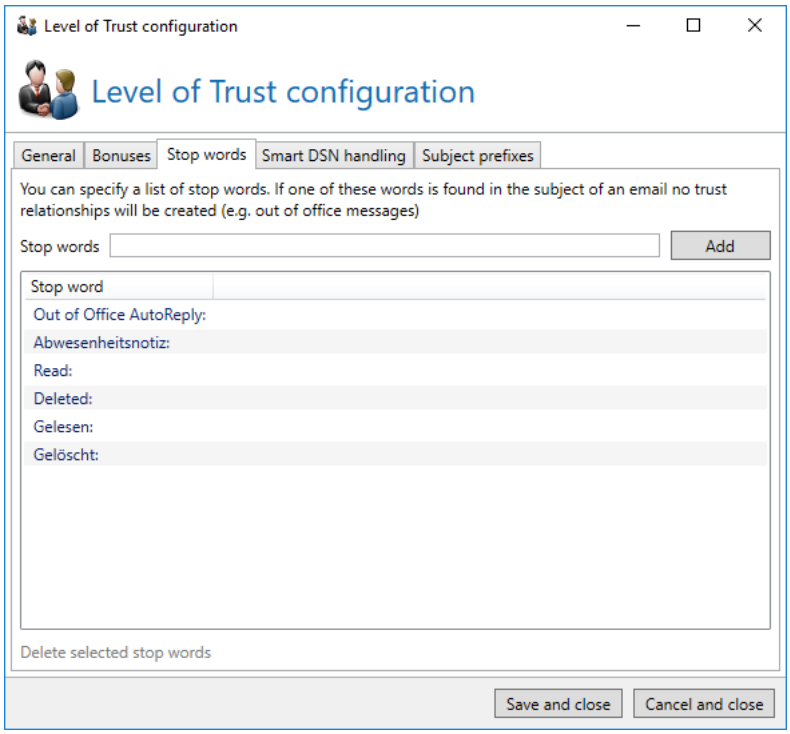
The setting **Address pairing** controls the number of points the trust between a sender and a recipient is increased per message (address relation). Using the slider, you can set a value between 0 and 200. One point equals (-0,1) points for the SCL.

For each email to external addresses, not only the so-called address pairing bonus is increased but also a bonus for the respective recipient's domain. Using the slider **Domain pairing**, you set by how many points the bonus is increased. This value should be smaller than the bonus for address relations. Here,

you can set a value between 0 and 200 with the slider as well. Similarly, one point equals (-0,1) points for the SCL.

Stop words

On the tab **Stop words**, you define the so-called stop words (Picture 179).

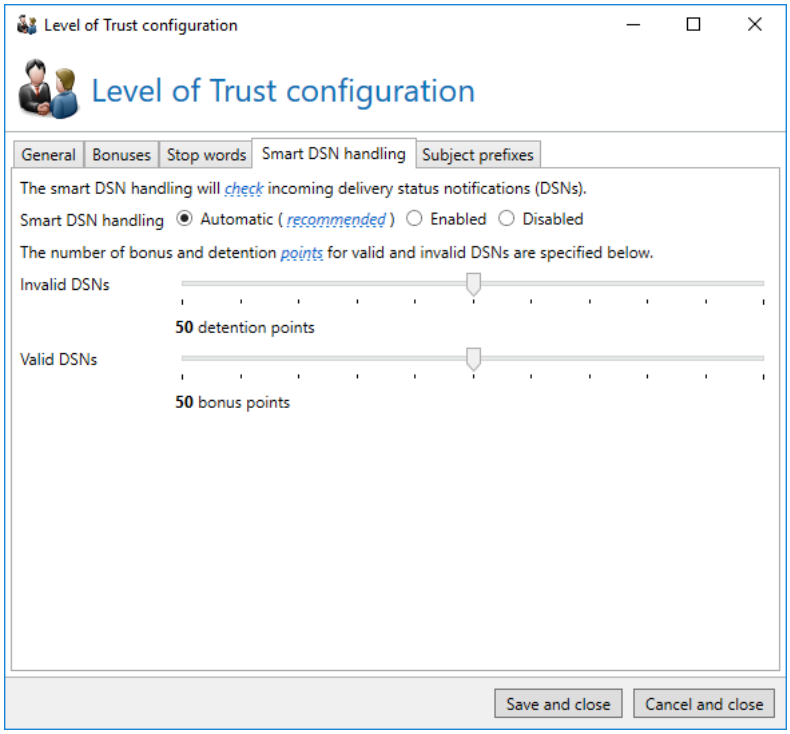


Picture 179: The defined stop words which prevent changes of the Level of Trust relations

As soon as the Gateway Role detects one of these words in the subject of a email to external addresses, the address pairing bonus as well as the domain bonus remain the same and are not increased. This setting is especially useful for automatically generated emails such as out-of-office replies.

Smart DSN handling

Smart DSN handling checks Delivery Status Notifications (DSNs) to local addresses. Since NoSpamProxy knows which emails were sent by the company, the software can also determine whether a corresponding email for the currently available DSN has left the company (Picture 180).



Picture 180: Configuring the Smart DSN handling

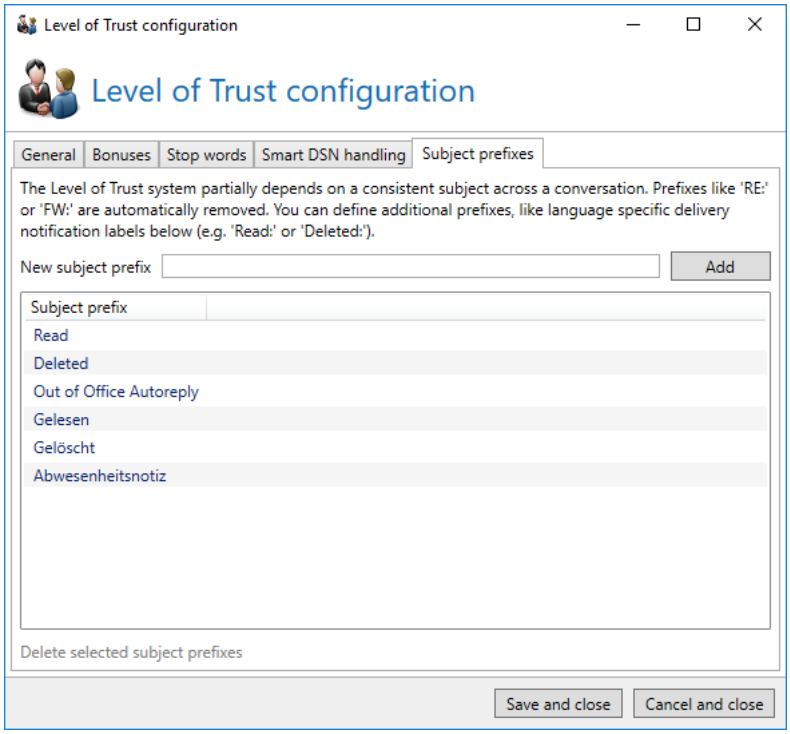
Example: A DSN arrives and NoSpamProxy determines that the original message for this DSN was sent from schmidt@example.com to schulze@netatwork.de. The Mail Gateway then checks whether an address pair schmidt@example.com/schulze@netatwork.de exists in the Level of Trust database. If this is not the case, the available DSN is not valid and receives minus points. If a matching address pair is found, the DSN receives bonus points.

In order for these checks to be implemented, two requirements must be met: First, an RFC-compliant DSN must be available. This means that the original message is attached to the DSN in order for NoSpamProxy to identify the original address pair. Moreover, it must be ensured that the Mail Gateway really knows all emails to external addresses. Under certain circumstances, this might be a problem in networks with distributed internet connections.

With the setting **Smart DSN handling**, you can influence the Smart DSN handling directly. If the radio button is set to **Automatic**, NoSpamProxy will first scan the Level of Trust database for elements older than 7 days. Only if this search was successful, the Mail Gateway will assess incoming DSN. This is the default setting. If you set the radio button to **Enabled**, NoSpamProxy will always assess the DSN even if no datasets are yet available in the Level of Trust database. To disable Smart DSN handling, set the radio button to **Disabled**.

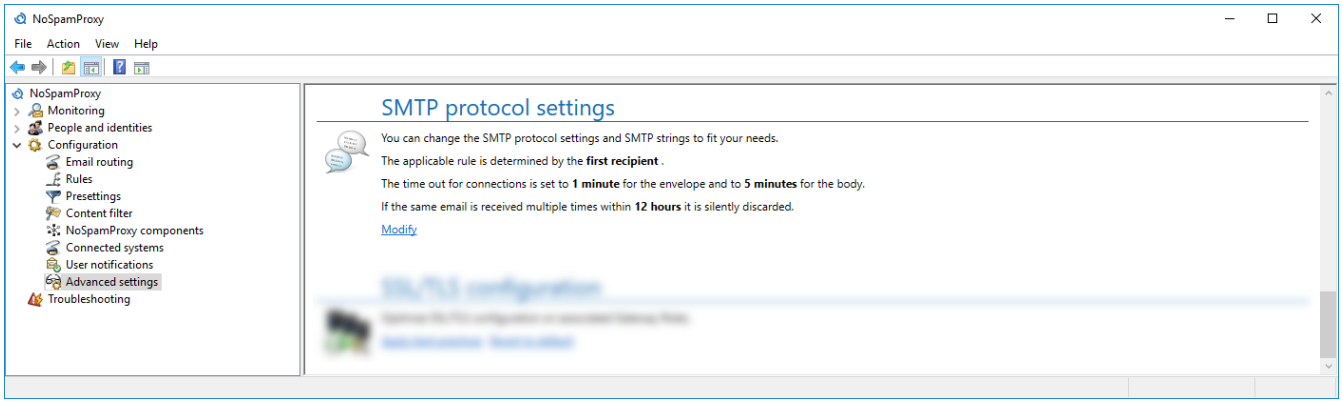
Subject prefixes

The Level of Trust system requires partially consistent subject lines of a conversation. Subject prefixes such as 'RE:' or 'FW:' need to be removed. On the tab **Subject prefixes**, you configure all prefixes used by your email system (Picture 181).



Picture 181: Define the subject prefixes which occur in the subject lines of your emails

SMTP protocol settings



Picture 182: SMTP protocol settings

The protocol settings regulate the behaviours for the receipt of emails, SMTP timeouts and SMTP status notifications.

Behaviours

If an email is sent to multiple recipients, it is possible that different rules are applied to this email, depending on the recipient. With the corresponding setting, NoSpamProxy can force the inbound system to send a separate email for each individual recipient.

This setting prevents conflicts with multiple addressed emails if an email is sent via one connection to two recipients which would then cause two different rules to be applied. Through the use of SMTP, it is not possible to provide independent feedback for individual recipients. It is only possible to close the entire connection.

Application of rules

Through the configuration of the option **Application of rules**, you can instruct NoSpamProxy to send the error message "Too many Recipients" to the inbound system if recipients are sent with colliding rules (Picture 183).

According to the RFC however, this is only permitted starting from the 101st recipient even if no email server issues have surfaced.

This setting effects that each email is sent with exactly one recipient. Thus, NoSpamProxy can apply the corresponding rule to each recipient. However, the emails are subsequently delivered by the sender several times.

The activation of this function allows you to manage the email assessment at the price of a multiple transfer as well as behaviour not necessarily RFC-compliant.

If this option is deactivated, the rule which applies to the first recipient is then applied to all recipients of this email.

The same result applies to all other recipients.

Duplicate email detection

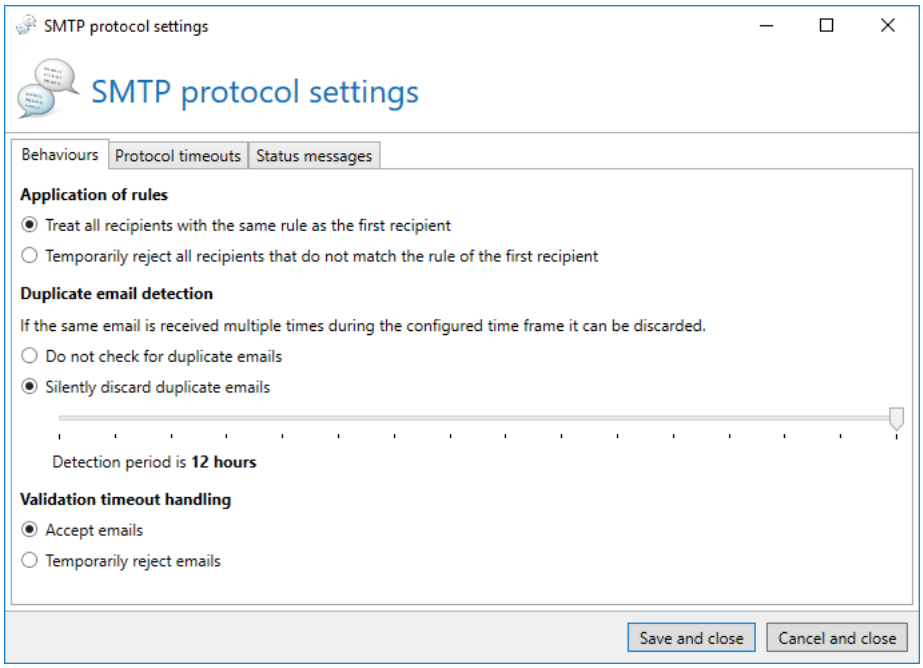
NoSpamProxy recognises if the same email is received multiple times. Sending the same email repeatedly usually occurs due to incorrect configuration such as email loops. You can set whether these emails should be discarded or not, as well as the time frame for the detection.

Validation timeout handling

You can specify how to handle emails whose validation time exceeds the maximum values configured under Protocol timeouts.

If the malware scan is not completed when a validation timeout occurs, the respective email will be temporarily rejected in any case.

Emails are always rejected if they have been temporarily or permanently rejected by an action.



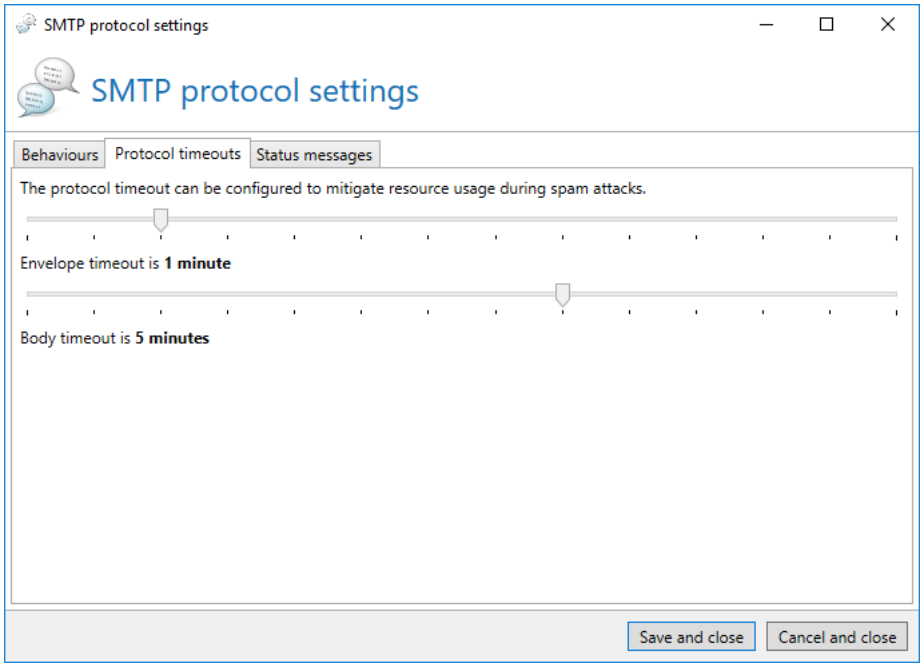
Picture 183: Behaviour for receipt of messages

Protocol timeouts

Adjusting the timeouts (Picture 184) has great impact on the resources required by your server for high email traffic.

In the section **SMTP protocol timeout settings**, you can determine when NoSpamProxy starts to disconnect due to idleness. This is determined for two sections within the SMTP protocol.

The setting **Envelope timeout is n seconds** controls the timeout for the commands within the so-called envelope part. This applies to all commands up to the DATA command (HELO/EHLO, MAIL FROM, RCPT TO). As soon as the DATA command has been sent, the setting **Body timeout is n seconds** is effected. A separation of the timeouts is useful since timeouts might occur more often during the transfer of the body part rather than the envelope due to intermediary filters and actions. The envelope is transferred very timely and fluently during normal transfer. A longer waiting period in this section of the email transfer more likely indicates a DoS attack or similar threats. As a result, you have the possibility to reduce the timeout of the envelope part in an emergency. You can set a value between 30 and 600 seconds with the sliders for the respective setting options.



Picture 184: Timeouts

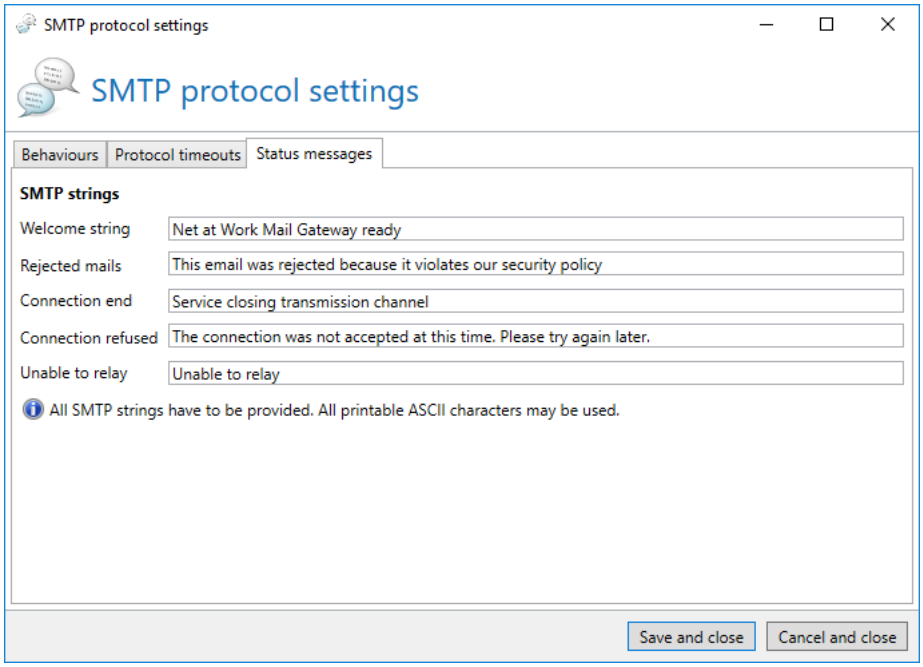
Status messages

The SMTP status messages (Picture 185) control which texts the Gateway reports to other servers.

The SMTP replies are details in the SMTP handshake which are usually not visible to the normal user. However, it might be useful to adjust the details according to your own needs. Thus, administrators can analyse emails more easily if they wish to detect any errors. For instance, the notifications "Rejected email" and "Blacklisted Address" are important details for the sender of a blocked email.

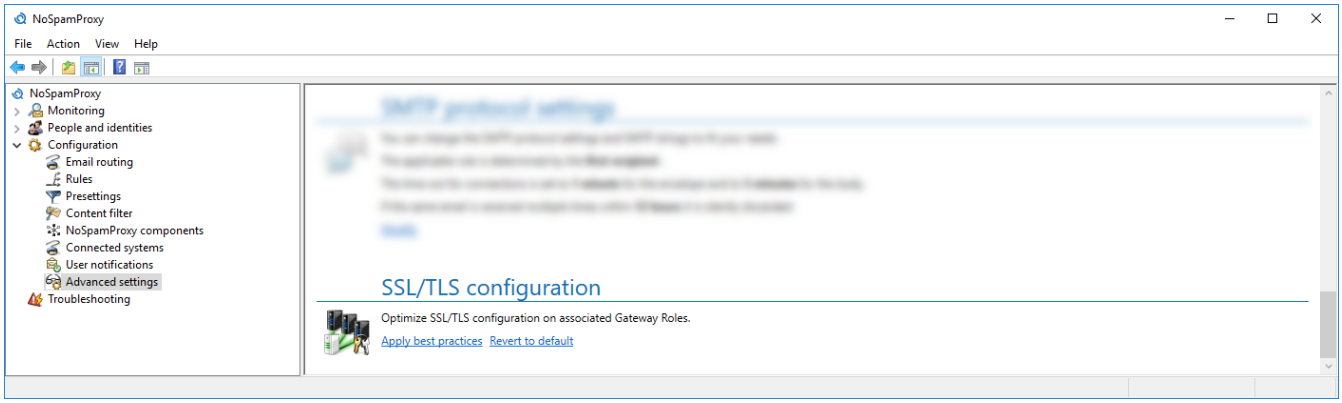
To change a notification, simply change the text by entering it into the field.

You must not use umlauts for SMTP notifications. Umlauts are not supported by the applied SMTP protocol.



Picture 185: Textual SMTP status notifications by NoSpamProxy to other servers

SSL/TLS configuration

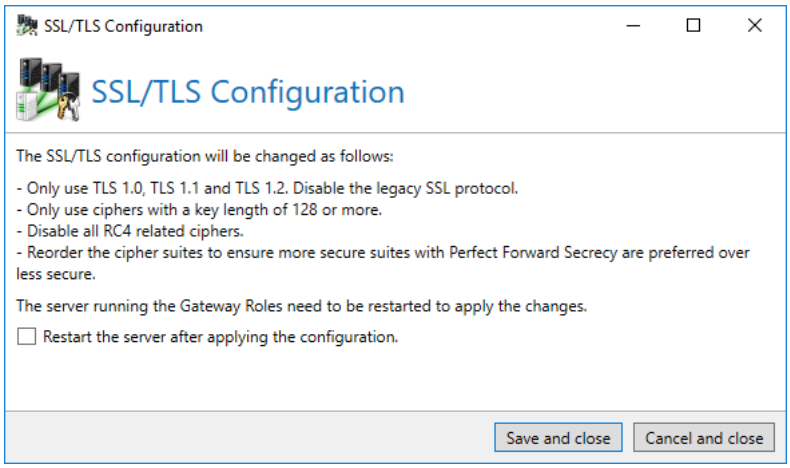


Picture 186: SSL/TLS configuration

Using transport encryption, the SMTP connection is secured via SSL or TLS. In doing so, the Gateway Role draws on the operating system and its settings are used for the connections. Lately, some encryption standards have proven to not be safe any longer (e.g. DES or RC4). It is thus useful to deactivate them. Some cipher suites support a feature called Perfect Forward Secrecy. In brief, it prevents that contents of connections can be decrypted by unauthorised third parties even if the private key of the server certificate is known. However, Windows does not preferably use this procedure in the

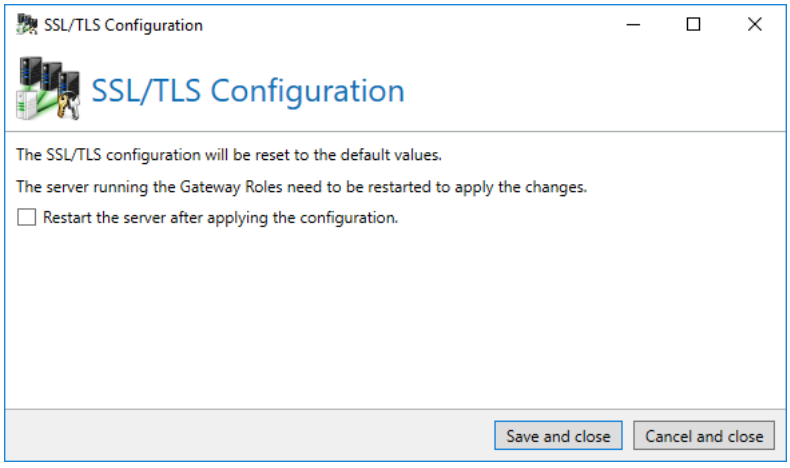
default setting. Thus, you can apply the settings recommended here (Picture 187). In order that the changes become effective, the server needs to be restarted. You can prompt this directly via the dialog.

This concerns a system-wide change which can also affect other programs.



Picture 187: Apply recommended settings for SSL/TLS configuration of Windows

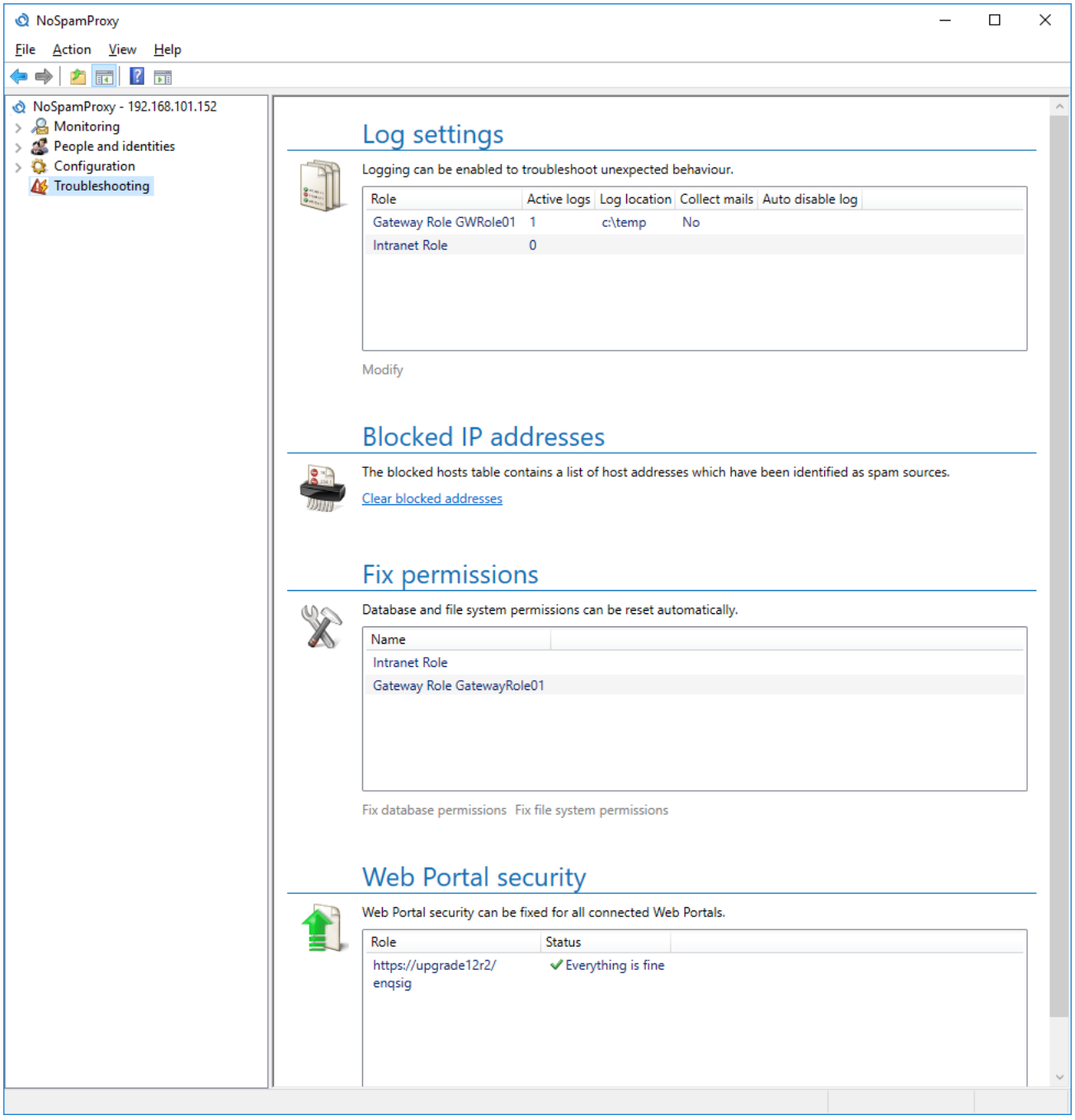
Furthermore, in this section, you have the possibility to recover the default values of Windows (Picture 188). Again, a restart of the server is necessary which can be prompted via the dialog.



Picture 188: Reset to default values for SSL/TLS configuration

19. Troubleshooting

The menu item **Troubleshooting** provides tools to create logs of the activities or a new database for the individual roles of NoSpamProxy. (Picture 189). If the old database has been damaged, it might be necessary to create a new database.

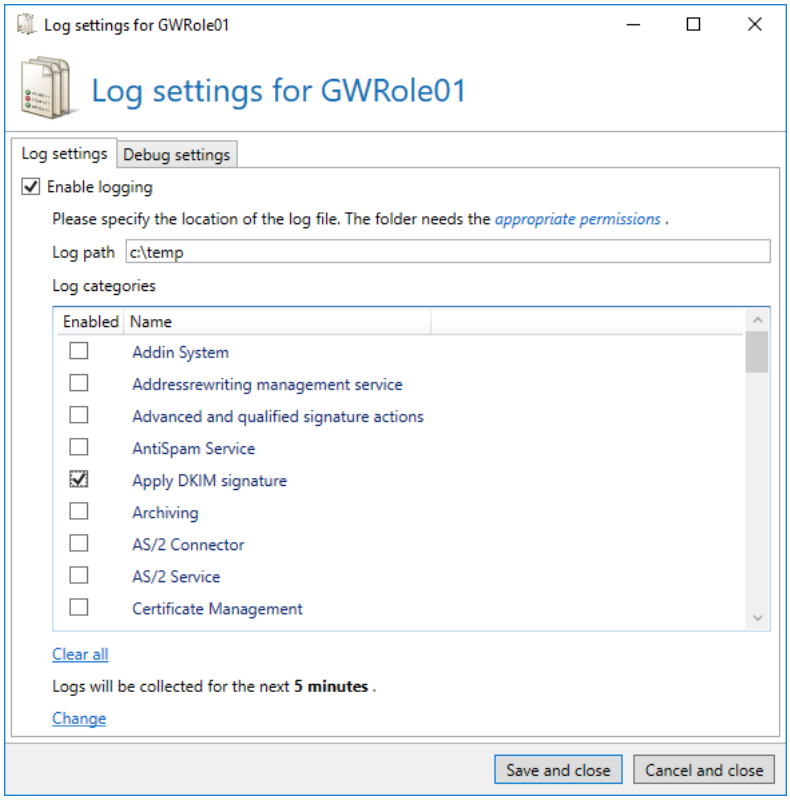


Picture 189: Tools for troubleshooting

Log settings

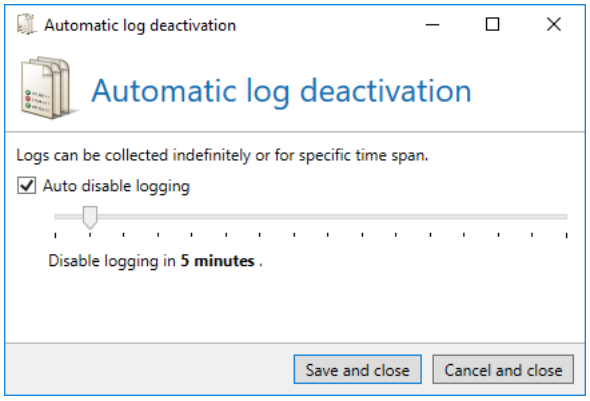
Configure the storage location for the log data in the first tab and select the categories for which you wish to activate logging (Picture 190).

Make sure you have at least 20% disk space available to store log files. If the available disk space falls below 20%, a warning is displayed.



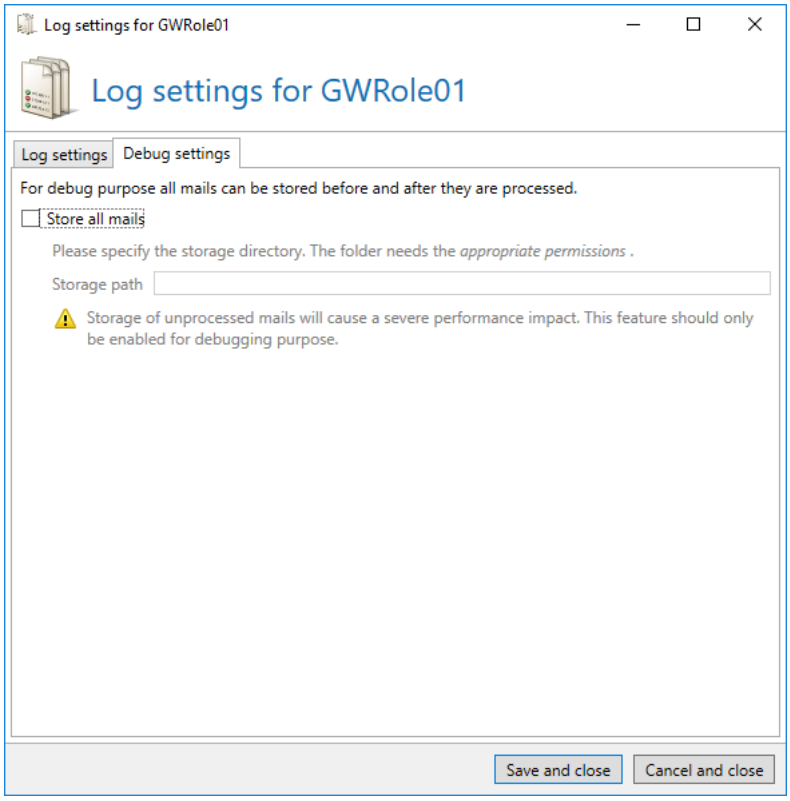
Picture 190: Configure the log settings

Additionally you can enable logging only for a specified timespan (Picture 191). Logging is automatically stopped when the time elapses and you can use the created log files immediately.



Picture 191: Auto disable logging

On the tab **Debug settings**, you can automatically store all emails to the hard drive before and after processing by NoSpamProxy (Picture 192). This tab is only available for Gateway Roles. You cannot configure this on the Intranet Role.

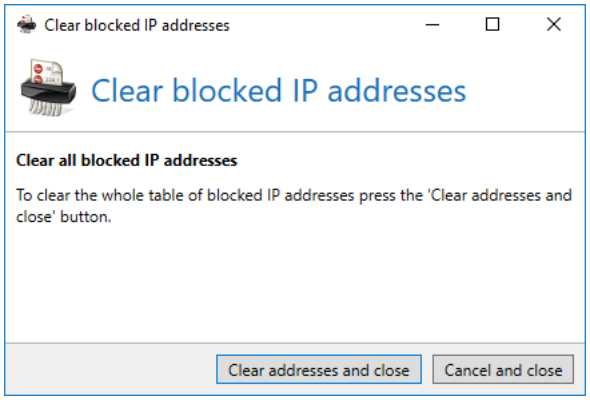


Picture 192: Store emails for troubleshooting

Please note that storing all emails on your hard drive might require a lot of storage space and may severely impact the server's performance. Only use this function for troubleshooting and deactivate it afterwards.

Blocked IP addresses

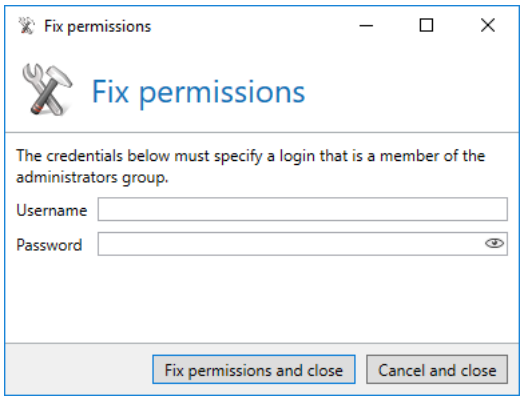
As mentioned before, NoSpamProxy blocks the inbound gateway for 30 minutes after rejecting a spam email. If a trusted IP address is mistakenly added to this blacklist, you can delete the list of the blocked gateways here (Picture 193).



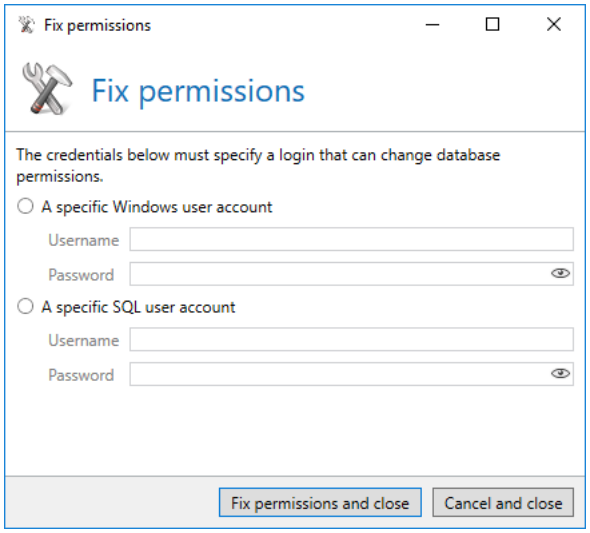
Picture 193: Delete blocked IP addresses via this dialog

Fix permissions

If the file system permissions of your NoSpamProxy were, e.g. by third party programs, changed in such a way that the function is impaired, you can correct this here. You can correct permissions in the file system (Picture 194) as well as on the used database (Picture 195).



Picture 194: Have permissions in the file system fixed



Picture 195: Have permissions in the database fixed

Web Portal security

For the security of all installed Web Portals, certain information must be synchronised. If you employ several Web Portals, the information must be synchronised after the installation of the second Web Portal. Such an incident is shown on the overview page. Additionally, you see here which Portal is concerned.

Select the function **Fix Web Portal security key** for all Portals which show the text **The security key is incorrect**.

As long as the keys are not synchronised, the forms on the Web Portal will display errors and be affected in their functionality.

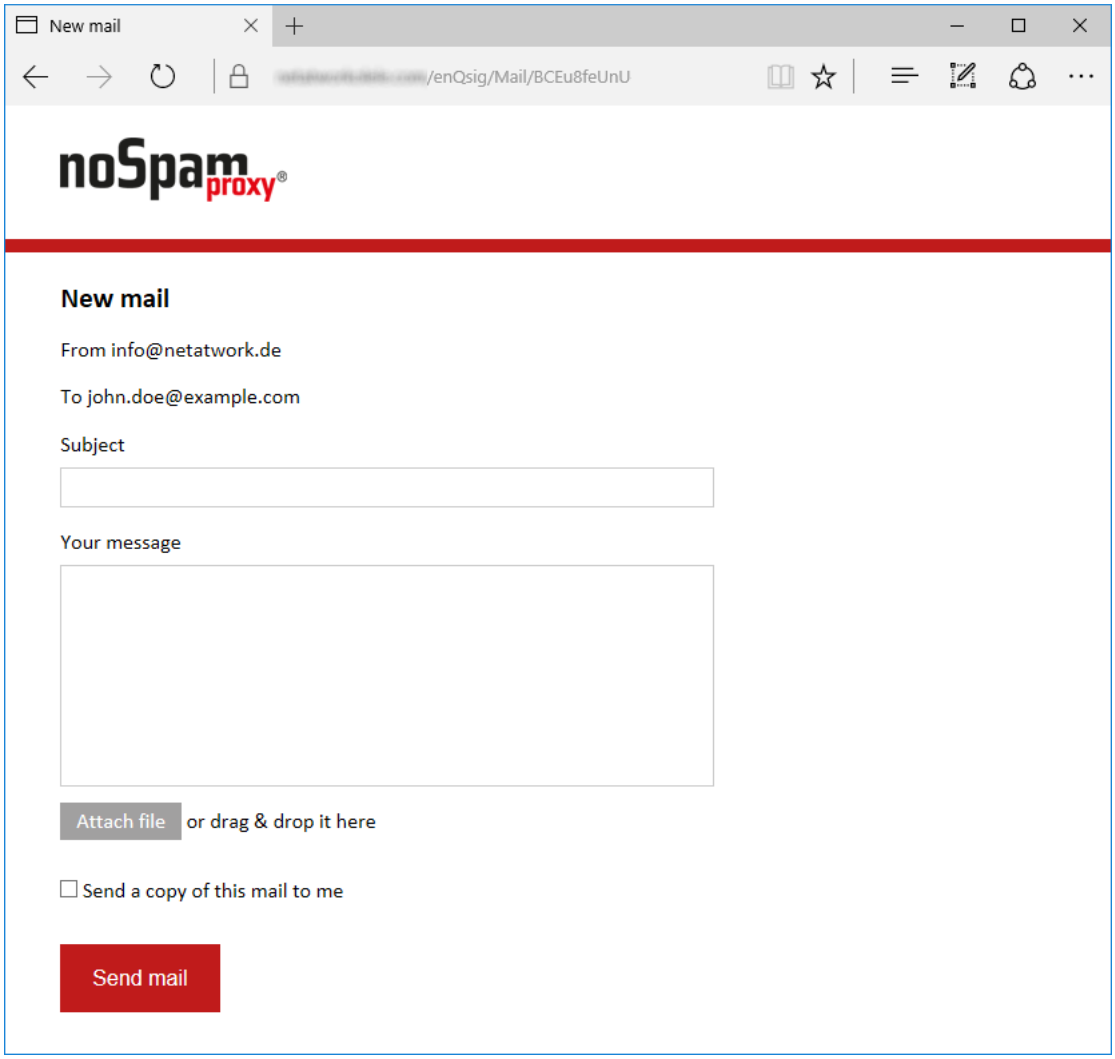
20. Web Portal

The Web Portal enables your communication partners to transmit large files to internal users. For this function, a valid licence for **Large Files** is required.

Large Files

If you possess a valid licence for **Large Files**, your users can offer external contacts the possibility to transfer files to you which are too large for email delivery. To do so, the internal user sends a response link to the recipient via the Outlook Add-In which can then be used to transfer files.

If your contact received an invitation for Large Files, he or she can send one or more files to the sender in a secure way via the Web Portal(Picture 196).



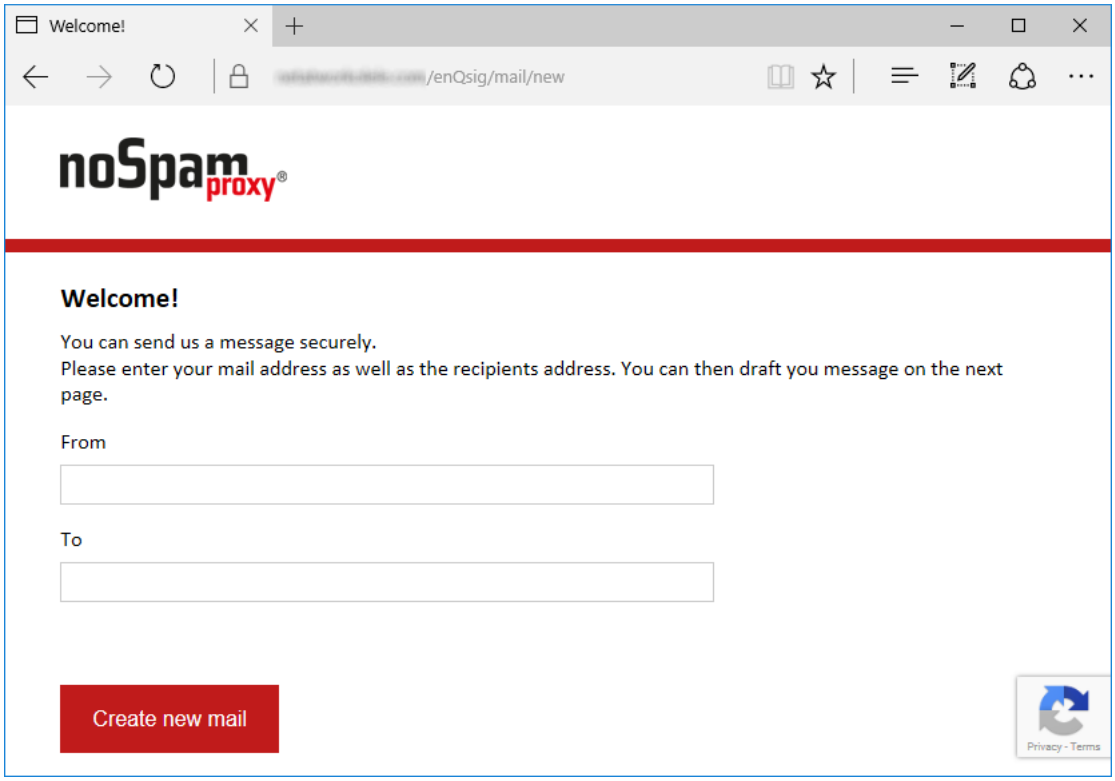
Picture 196: Transferring files securely via the Web Portal

Recipient and subject are predetermined and cannot be changed. The contact cannot send a message along with the attached files.

Depending on the configuration, files are either attached to the email directly or provided to the recipients via Large Files. The threshold values as well as the maximum size per attachment can be determined by the administrator.

Secure emails via the Web Portal without invitation

To enable external contacts to send secure emails to users of NoSpamProxy at any time, you can also use the Web Portal without invitation. In this case your partner only has to input his email address, a valid recipient address and when appropriate a CAPTCHA (Picture 197).



Picture 197: Dialog for new emails without invitation link

After successful validation of the sender and recipient addresses as well as the CAPTCHA, the email can be sent in the same way as described in the previous chapters.

21. Disclaimer

To use the Disclaimer feature a valid licence is required.

After you have configured the Disclaimer, you must add the action Apply disclaimers to an outbound email rule.

NoSpamProxy **Disclaimer** provides an integrated possibility to add email disclaimers to emails during their dispatch.

The disclaimers are created and configured through a website, making the installation of specialised applications as well as direct employee access to NoSpamProxy, the management console or your email server unnecessary.

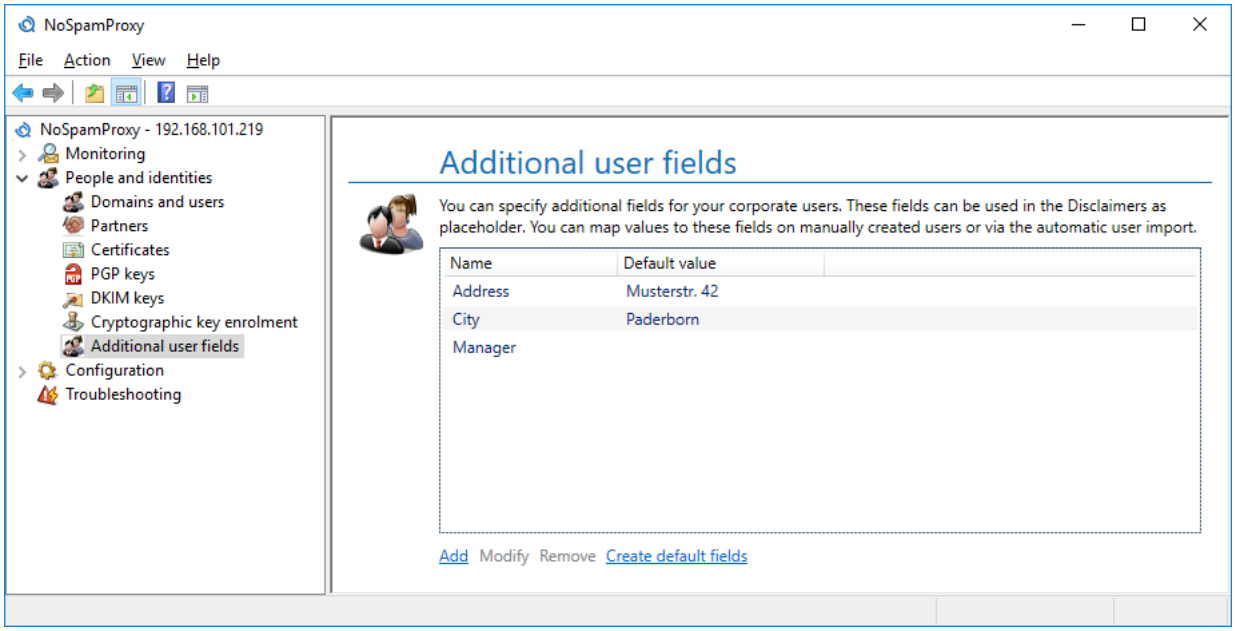
Open the Disclaimer website by clicking **Open Disclaimer webseite** on the dashboard.

The website is divided into two sections, **Templates** and **Rules**. A template determines the HTML and Plain Text content of a disclaimer. A rule determines when, how and where a template is added to an email. Through the flexible combinations of the created templates and rules, it is possible to set up a disclaimer from one or more templates and include it in emails.

You can also add placeholder to the content of a template. These must be provided by the NoSpamProxy administrator in advance. They are then replaced by the value deposited in the user object when the email is sent. By doing so, values such as names, phone numbers and departments can be added dynamically.

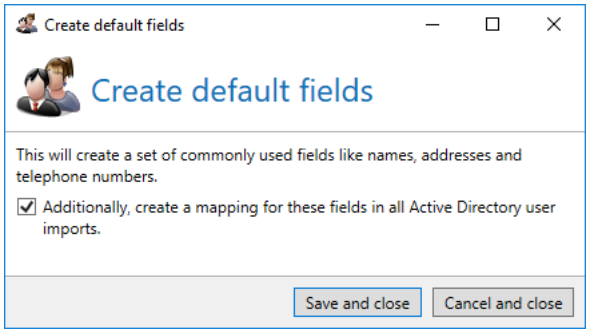
Providing placeholder

For editing the disclaimers, the administrator must first create the required **Additional user fields** which can be included in a template as placeholder for the definite value. To do so, go to **Additional user fields** and create the required fields (Picture 198).



Picture 198: The overview of all available user fields

For most application scenarios, the best way is to select **Create default fields**. Thus, the fields which are commonly used are directly entered into the list. When creating the fields, the mappings of the user fields to Active Directory fields can additionally be configured in the existing Active Directory user imports (Picture 199).



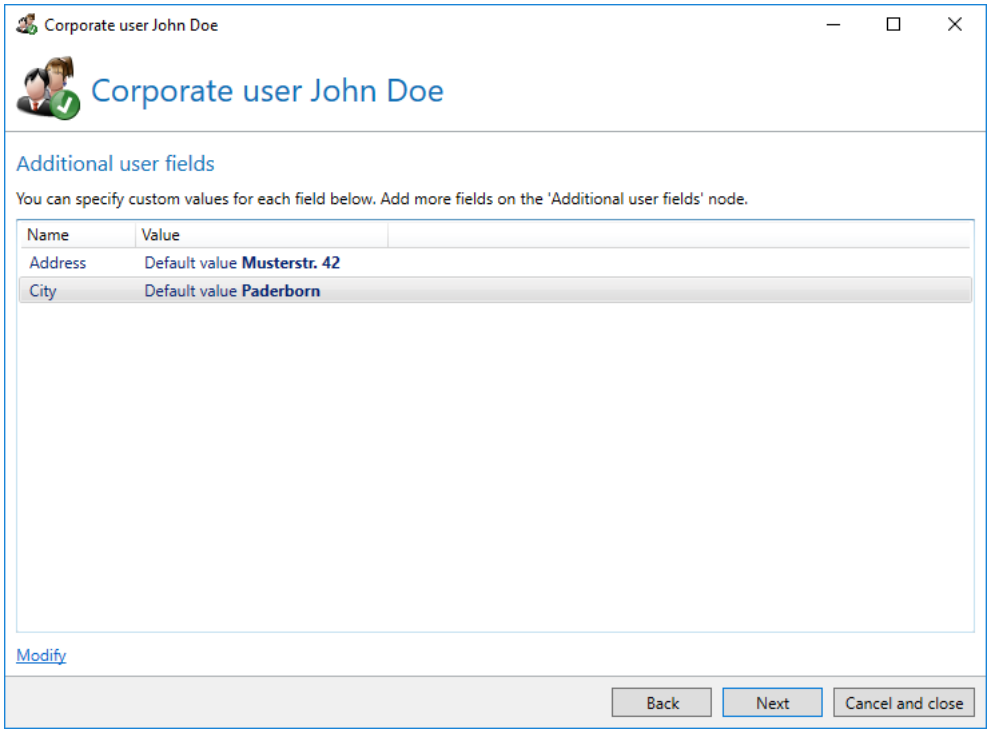
Picture 199: Creating frequently used default fields

The created fields can optionally be filled with default values at this point. These are always used if no custom values are mapped to the user. For instance, the phone number/email address of the head office can be entered into the field for the phone number/mail and so forth.

The created fields are immediately available in the manually entered company users as well as in the Active Directory user imports.

Additional user fields in manually entered users

Open a manually entered company user under **Domains and users**. On the page **Additional user fields**, you see the fields previously defined under **Additional user fields** (Picture 200).



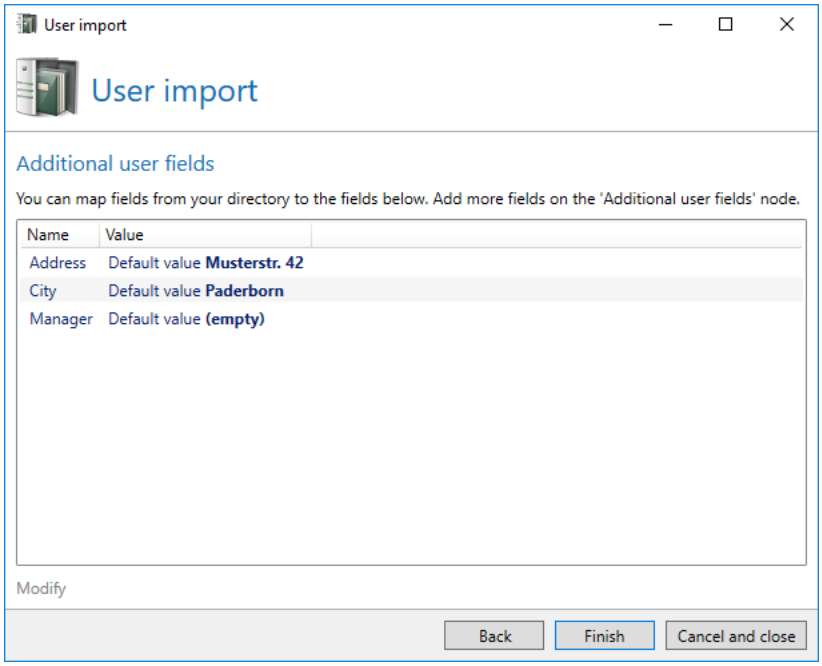
Picture 200: Additional user fields

You can either set a value for each field or apply the default value of the field.

Additional user fields in the user import

When importing from an Active Directory or a generic LDAP directory, you can fill additional user fields with values from the configured directory. This is useful if you wish to personalise disclaimer templates for your users (Picture 201).

First, define custom fields or create default user fields under Additional user fields . Subsequently, you can set for each field in this dialog from which field of the directory the data should be obtained.



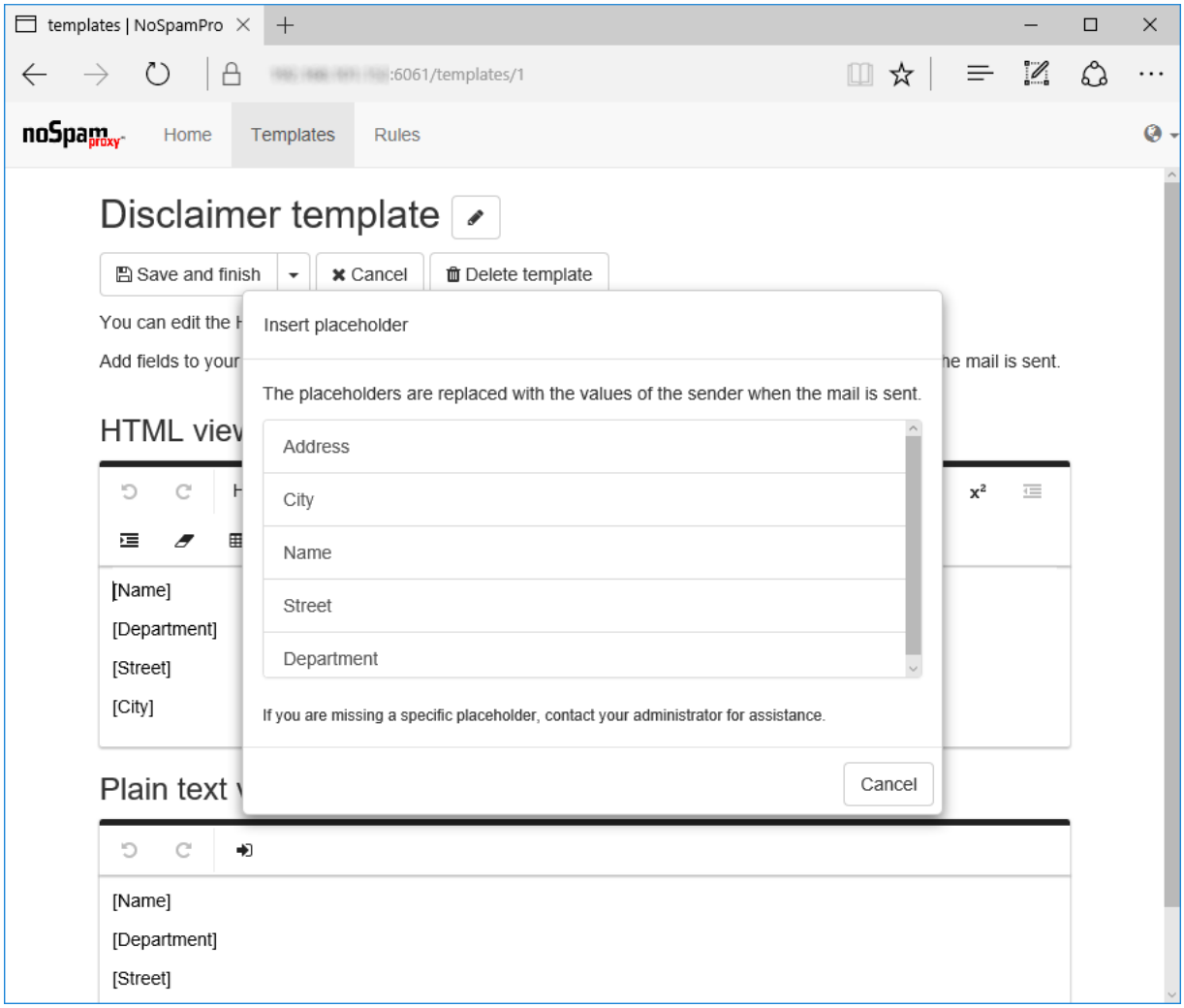
Picture 201: Configuration of additional user fields

To each field, you can either map a value from the Active Directory or apply the default value of the field.

The values you mapped in the Active Directory user import are only available during the next run of the user import.

Using the fields in the disclaimer

After you have created the fields under **Additional user fields**, they can be used in the templates on the disclaimer website. The creator of the templates sees a list with the names of the fields if he/she clicks on **Insert placeholder** in a template (Picture 202). The names of the fields can be re-named by the administrator even after having been used in templates already in order to, for example, improve the user experience.



Picture 202: The selection from the list of 'Additional user fields' configured by the administrator

After you have configured the Disclaimer, you must add the action Apply disclaimers to an outbound email rule.

22. Appendix

Multiple used settings in the configuration

Some settings are used in the configuration multiple times. To increase the readability of this manual, they are explained in detail here; references to this chapter are made in the descriptions of the actual use in the different configurations.

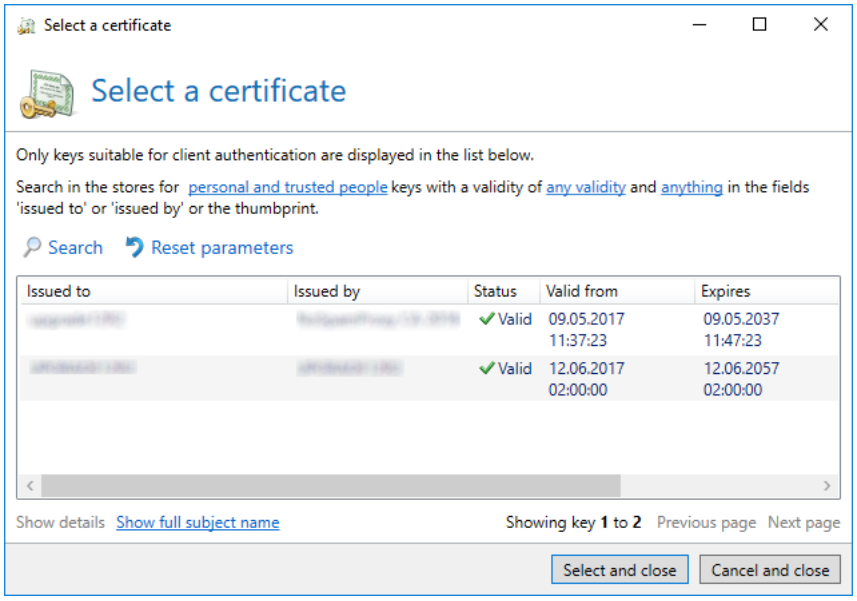
Passwords

Passwords in the client can be implemented in the following ways:

- **Simple password entry**
  The simple password entry is the most commonly used password entry. It offers the function to show the password in plaintext by clicking on the eye symbol next to the entry field. The display supports you in entering and checking the password. This entry is used for all entries where the administrator has previously entered the password him/herself.
- **Double password entry**
  For double password entry, you must enter exact the same password twice. This entry is required for very sensitive passwords where incorrect entries should be avoided. Similar to the simple password entry, the password entered can be viewed in plaintext by clicking the eye symbol. This entry is used, for example, to protect the sensitive data of NoSpamProxy.
- **Password entry without subsequent view**
  Here, instead of showing the password in the dialog, only a hint whether a password had already been entered or not is displayed. The administrator can delete the password if required or set it to a new value. This entry type ensures that passwords entered by third parties cannot be viewed via the client after the it has been entered. To avoid spelling mistakes, the concealed entry is always executed as double password entry. This entry is, for example, used in the encryption passwords of the external partners.

Selection of certificates

When selecting certificates, the dialog **Select a certificate** appears. (Picture 203).



Picture 203: The list of available certificates

Depending on the section in which you wish to select these certificates, certificates for the following purposes of use are displayed:

- **Email authentication**
  A certificate that is used to authenticate the sender of an email.
- **Server authentication**
  A certificate that is used to clearly authenticate a server.
- **Client authentication**
  A certificate that is used to clearly authenticate a computer which tries to connect to a server.

Here, all certificates from the certificate store of the local machine, i.e. the machine on which the role to be configured runs, are shown. Select the desired certificate and click **Select and close** in order to use the selected certificate or check all details of the selected certificate by using **Show details**.

It can be difficult to distinguish certain certificates, e.g. for De-Mail, due to identical entries in the field **Issued for**. To distinguish these certificates, select the function **Show full subject name**. Thus, the subject name of each certificate is shown without abbreviations.

Backup and recovery

To recover NoSpamProxy in case of a system failure, it is required to regularly back up all data relevant for the operation.

Operating system, driver and software

You should implement the backup of the Windows operating system with approved programs. Since NoSpamProxy has very few dependencies on the operating system itself, it is also possible to reinstall the replacement server after a failure. It is your decision whether reinstalling the operating system including all settings and applications or system recovery is more appropriate.

If you want to reinstall the operating system, you should document the programs and settings installed so far and have available the data storage devices.

Further information can be found in the online manuals and instructions on Windows Server and NTBACKUP by Microsoft.

NoSpamProxy licence

Your licence is stored as a file on the server in the directory

```
%ProgramData%\Net at Work Mail Gateway\Configuration\License.xml
```

and can be backed up through a normal backup process. You can also make a copy of the XML file and place it in a safe folder. The file is not blocked during operation and not overwritten.

Configuration files of roles

The configuration of NoSpamProxy is stored in an XML file on the server itself. This file can also be secured with customary backup software without problems.

However, the gateway resets this file if the configuration is changed; this may result in a conflict in case of a simultaneous backup.

While the configuration is written, NoSpamProxy creates the new file as a temporary file, names the original file, e.g. "GatewayRole.config.backup", and only names the temporary file "GatewayRole.config" afterwards. A regular file-based backup will create the most current copy or the version of the configuration changed shortly before.

We recommend you copying this file before implementing major changes to the configuration as well, in order to be able to easily return to the previous state.

The configuration files of all roles in the default configuration are listed below. Should you have installed NoSpamProxy in another path or have updated the program from a former version of NoSpamProxy, the path must be adjusted accordingly.

- **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\Configuration\ManagementService.config`

Databases of NoSpamProxy

NoSpamProxy stores most information in several SQL databases which you should back up as well. The roles of NoSpamProxy use the following databases to do so:

- **Gateway Role**
  `NoSpamProxyDB`
- **Intranet Role**
  `NoSpamProxyAddressSynchronization`
- **Web Portal**
  `enQsigPortal`

If NoSpamProxy uses your existing SQL server in Standard or Enterprise edition, you can configure a periodical backup of all databases with the Enterprise Manager. When using the SQL Server Express Edition, you must back up the database manually using a script and recover it when required.

Back up the database via the command line with the following commands:

For the database of the Gateway Role: `osql -S (local)\NoSpamProxyDB -E -Q "BACKUP DATABASE NoSpamProxyDB TO DISK = 'c:\NoSpamProxyDB.bak'"`

For the database of the Intranet Role: `osql -S (local)\NoSpamProxyAddressSynchronization -E -Q "BACKUP DATABASE NoSpamProxyAddressSynchronization TO DISK = 'c:\NoSpamProxyAddressSynchronization.bak'"`

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

This command backs up the database in a file without shutting down the database. You should consider scheduling a correspondingly adjusted invocation with Windows task scheduler as regular task.

The recovery is realised with the following lines:

For the database of the Gateway Role: `osql -S (local)\NOSPAMPROXYDB -E -Q "RESTORE DATABASE NoSpamProxyDB FROM DISK = 'c:\nospamproxydb.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

For the database of the Intranet Role: `osql -S (local)\NoSpamProxyAddressSynchronization -E -Q "RESTORE DATABASE NoSpamProxyAddressSynchronization FROM DISK = 'c:\NoSpamProxyAddressSynchronization.bak' WITH FILE= 1, NOUNLOAD, REPLACE "`

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

As a prerequisite, the database must already exist.

Since the SQL server itself permanently keeps the databases in use, they cannot be captured through a normal backup of the files such as via NTBACKUP.

Troubleshooting

NoSpamProxy is based on very simple functional principle. Its implementation as SMTP proxy connects the advantages of this principle to the simplicity of its operation. Nevertheless, it is possible the gateway does not work as you expect it to after the installation. The most common errors and test possibilities are described here.

Email support

You receive support by contacting the following email address:

support@nospamproxy.de

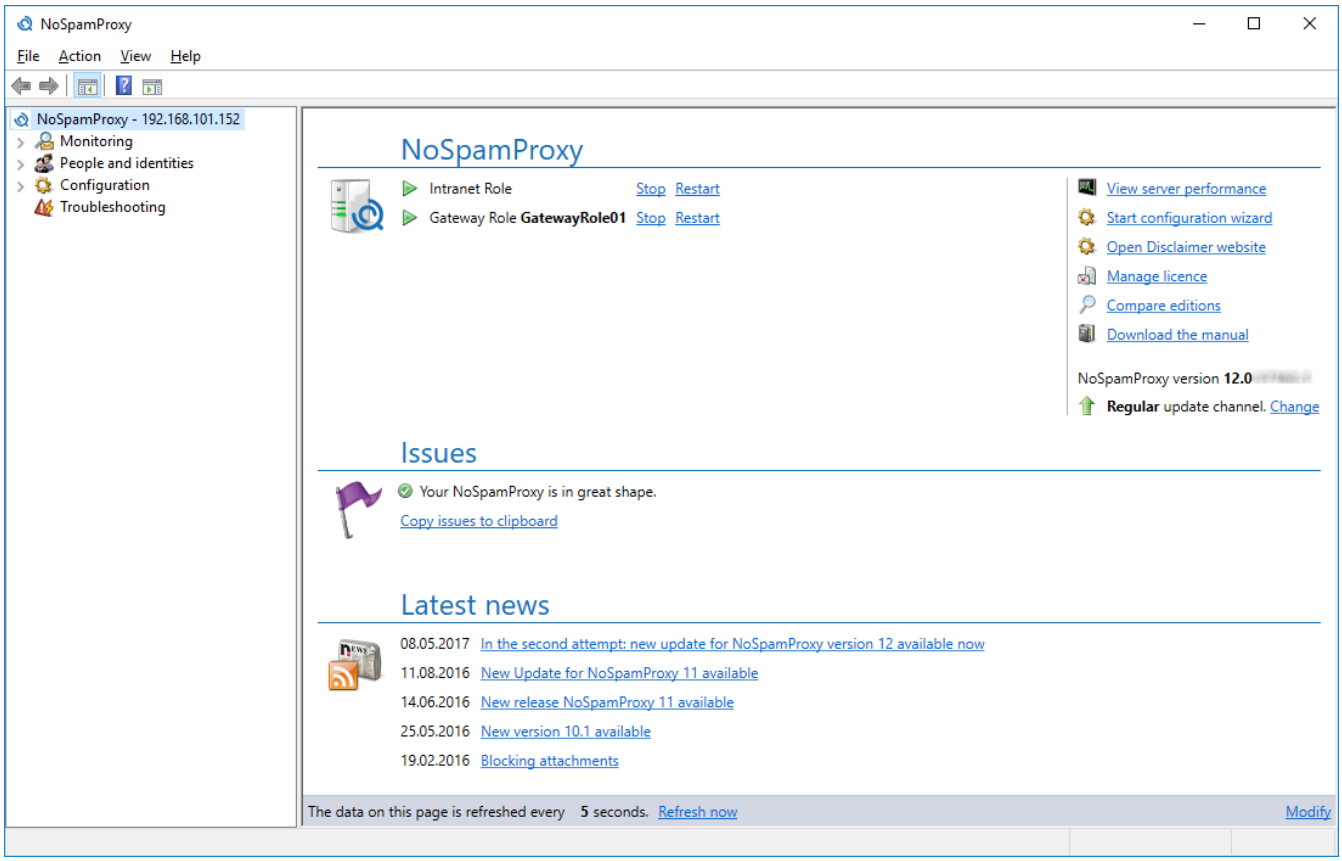
Please include the following information in your email:

- **Your customer ID**
  We gather and maintain all support cases in our ticket system. Your customer ID is the key to clearly map your support request. You received your customer ID after having requested a test licence or having purchased a licence. Should you not have your customer ID at hand, you can look it up in the licence file. The customer ID, "C12345" in our example, is located in an area called "ContactNumber": `<field name="ContactNumber">C12345</field>` You can provide this number as your customer ID as well.
- **The configuration of NoSpamProxy**
  The location of the configuration files is described in the file system in the paragraph Configuration files of roles. Please attach all of the files, especially the configuration file of the Gateway Role, to the email to our support team.
- **Network plan**
  A brief description of your infrastructure helps us to understand how you wish to use NoSpamProxy. Of particular interest are your SMTP domains, the IP addresses of the internal email server as well as information on how you receive and send your emails from the internet. Information on firewalls in the transfer routes are helpful as well.
- **Information on your internet connection**
  To apply NoSpamProxy, you must receive your emails via SMTP. Thus, external access to your system must be possible via port 25/TCP. Which components are between the Mail Gateway and the internet? A router with port filter and NAT or a full-featured firewall?
- **Information on the server**
  Which operating system and service packs have you installed? Do you have activated port filters or a firewall on the server?
- **Error description**
  Please describe the nature of the error or malfunction you encountered as detailed as possible.

We will try to help you as soon as possible. However, please read the following advice to recognise frequent errors and know how to fix them on your own.

Check NoSpamProxy

At first, your attention should be directed at the management client of NoSpamProxy. The status screen on the overview page provides you with a very quick overview of your system. Here, you can see immediately whether all settings have been entered correctly (Picture 204).



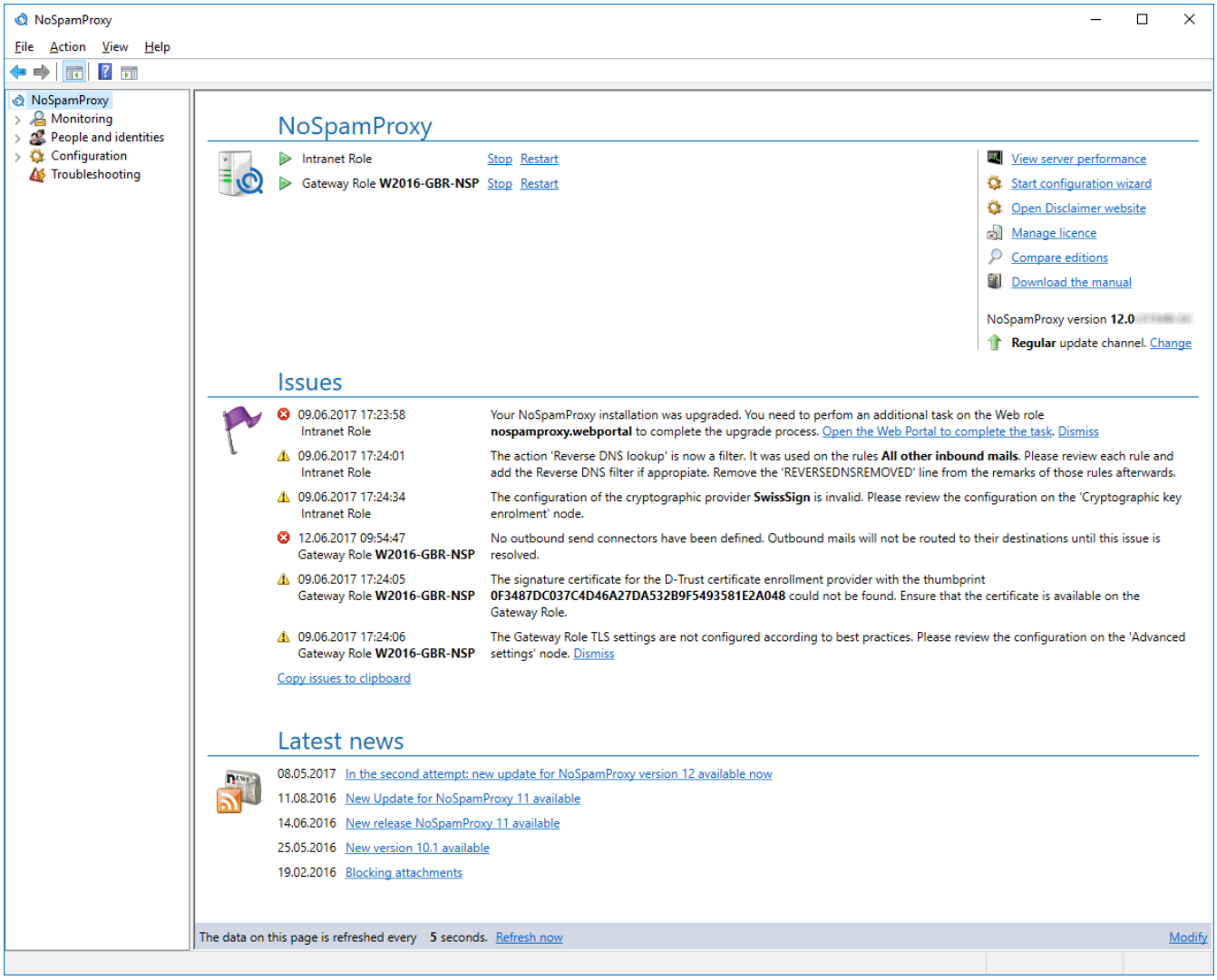
Picture 204: The overview shows the complete configuration of NoSpamProxy

Please check the following bullet points.

1. **Have all roles been started?**
   All roles should have the status "started". You can also start the roles via the client.
2. **Are errors displayed?**
   Errors in the configuration of a role are displayed in the overview of NoSpamProxy (Picture 205). Errors in a completely configured gateway should always be fixed.
3. **Are warnings displayed?**
   Warnings are supposed to be considered similar to errors with the difference that warnings can indeed occur under certain circumstances. Gather as much information on the warning as

possible and decide whether the warning is caused by your configuration of NoSpamProxy or whether it should be fixed.

4. **IP addresses and ports**
   Check whether the Gateway Role of NoSpamProxy accepts connections on the correct IP addresses and ports.
5. **Are emails being transferred at all?**
   On the status screen, you see the number of connections and transferred emails as well as the data volume. If all values are set to 0, NoSpamProxy receives no emails. You can query the same values with the Windows performance counters.
6. **Messages in the event protocol**
   NoSpamProxy shows you error messages in the Windows event viewer which impair its function.



Picture 205: Errors in the configurations of NoSpamProxy

Test NoSpamProxy

The basic functions of NoSpamProxy can be tested with two programs which are part of Windows:

- **TELNET**
  The dispatch of an e-ail via SMTP is very simple and can also be tested manually with TELNET.
- **NSLOOKUP**
  This program serves to troubleshoot in case of DNS resolution issues. NoSpamProxy uses DNS intensively, e.g. to request RBL lists or check certificates for validity.

TELNET

If an email server sends an email to another email server this is done via TCP/IP via the port 25. You can also implement this communication manually with TELNET and test the behaviour of the remote email server or that of the own NoSpamProxy. You can easily send an email via SMTP using the program TELNET. To do so, initiate the connection by entering

```
TELNET name-of-mail-server 25
```

Now, the email server should confirm the establishment of the connection with a 220 message.
You are now connected to your email server and can send emails as follows. Enter the following commands, always followed by the Enter key <CR>. Wait for the confirmation of the email server after each command.

```
HELO name.of.sender server<CR>
```

```
MAIL FROM: mail address@sender.de<CR>
```

```
RCPT TO: mail address@target domain.de<CR>
```

```
DATA<CR>
```

Now, enter everything without awaiting server response:

```
Subject: This is the subject<CR>
```

```
<CR>
```

```
and this the body<CR>
```

```
. <CR>
```

The last line only contains a full stop. This signifies the end of the email; the email server confirms the receipt of the email. Using the command `QUIT`, the connection to the email server is severed.

NSLOOKUP

The program NSLOOKUP is the means to check the DNS name resolution. Simply start the NSLOOKUP in a DOS window with the corresponding options.

Examples:

```
nslookup -q=A www.microsoft.com
```

You receive the list of the IP addresses which operate the website of Microsoft.

```
nslookup -q=MX netatwork.de
```

You receive the email servers which accept emails for the domain `netatwork.de`.

```
nslookup -q=A
```

```
nslookup -q=A 3.4.5.80.dnsbl.sorbs.net
```

You receive the information from the list "Sorbs" that this server name has the IP address `127.0.0.10` and is thus listed among the dynamic IP addresses.

As a result, NSLOOKUP is a useful tool to identify errors in the DNS configuration of the Windows Server.

Frequent errors and their causes

NoSpamProxy is developed in such a way that only interfaces can be bound and used which have been configured. Particularly in the case of systems with many network interface cards and IP addresses it is important to implement the configuration conscientiously. As a consequence, be sure to check the following settings:

- **Port and IP address**
  Ensure that NoSpamProxy accepts connections on the addresses which you intended for it. Maybe there just are transposed numbers in the configuration?
- **Telnet on 127.0.0.1 port 25 does not work**
  Please keep in mind that NoSpamProxy does not work on the localhost address if you have bound the service to a specific IP address.
- **Firewall**
  Is there a firewall or a port filter on the server which may prevent a connection to NoSpamProxy on TCP/IP level? Test the availability of NoSpamProxy on the server itself with a TELNET command on the IP address. By doing so, you exclude an external firewall for test purposes.
- **Other services?**
  NoSpamProxy tries to use the provided interfaces during start up. This is not possible if another program is already using the corresponding resources. The gateway shows a corresponding error message in the event viewer and in the status page.

NoSpamProxy Protection does not filter

If NoSpamProxy Protection is installed correctly and emails are passed through but not blocked, please check the following:

- **Licence installed**
  If NoSpamProxy Protection does not find any valid licence, all connections are set to "pass", this means emails are passed without any further consideration of the rules.

- **Rules**
  Check whether your rules meet your requirements and whether filters and restrictions are set accordingly. The decision "pass" passes all emails of this rule. The order of the rules is important as well. The rules are processed sequentially. The first matching rule is applied and all others are not regarded. For testing, it is recommended to define, for instance, a rule at the beginning of the rule set which rejects emails to a specific email address. This could be realised by using the correct setting in the tab "Email flow", for example. A test email to this recipient must be rejected by NoSpamProxy Protection. If this happens, the IP address of the test system is added to the blacklist; you can be sure that NoSpamProxy Protection already works in principle. However, you must research into your rules in more detail now.
- **Email message tracking**
  Message tracking offers you detailed information on the processing of an email. Each email processed by NoSpamProxy Protection can be found in the message tracking. There, you can also easily find the rule and the filters or actions applied to an email including the categorisation. In case of malfunction or receipt of a "False Positive" result regarding email processing through NoSpamProxy Protection, sufficient advice should be found in the message tracking.

NoSpamProxy rejects all emails to local addresses

NoSpamProxy prevents unauthorised forwarding of emails (Relaying) and is protected against external and internal misuse very well. Similar to a firewall, this means, however, that you have to first activate the respective functions you require. This comprises two settings:

- **Owned domains**
  You need to enter all the domains you operate into the corresponding list in the gateway. Based on the default rules, NoSpamProxy only accepts external emails for these domains. If you have not entered any domains here, the gateway does not accept any external emails. **Exception:** You have changed the default rules so that this protection is no longer ensured.
- **Corporate email servers**
  In order for emails to external addresses to be delivered by NoSpamProxy, all email servers from which the gateway is supposed to forward emails must be entered in the list of the corporate email servers. If email servers are missing in the list, it is not possible to forward emails from these servers.

If NoSpamProxy rejects external emails, the email server which tries to deliver the email creates a non-delivery report. You can also transmit an external email to the gateway yourself by using the TELNET test method and interpret the status message of NoSpamProxy which states the reason for the rejection. Moreover, message tracking offers you a helpful tool for error encirclement.

SQL database is not available

If you have selected the corporate users as recipient criteria in the rule in order that emails to invalid email addresses are rejected, NoSpamProxy temporarily rejects the email as soon as it cannot access the corresponding SQL table. Make sure that the SQL server service is started properly and the gateway can access the database without errors. Among other things, you can find error messages in the event viewer of NoSpamProxy and in the overview page.

NoSpamProxy Protection does not find any viruses

NoSpamProxy Protection can scan all emails for virus-infested attachments and, depending on the setting, reject the entire email or only remove the attachments. Two requirements need to be met in order for NoSpamProxy Protection to be able to scan emails with attachments for viruses:

- **Installed virus scanner**
  Any virus scanner which monitors accesses to the file system in realtime and prevents the attempt to store a virus-infested file must be installed on the server of NoSpamProxy Protection.
- **Action 'File based virus scanner' must be integrated**
  This action is not integrated by default since it only makes sense in combination with an installed virus scanner. Since NoSpamProxy Protection cannot determine whether a virus scanner is installed, we do not wish to evoke an impression of security without having proof. To use the function of virus protection, you must install a file based virus scanner and integrate the action into the respective rules. You can check the function of the file based virus scanner by installing the EICAR test virus via the page http://www.eicar.com/ or by having it sent to you.

Smart card cannot be administered via RDP

If you use certificates that are stored on a smart card, you cannot manage the smart card in an RDP session. It only works in a session directly on the host. In virtual environments based on Hyper-V, for example, the SCVMM admin must be used while in VMware environments, you would use the VMware admin.

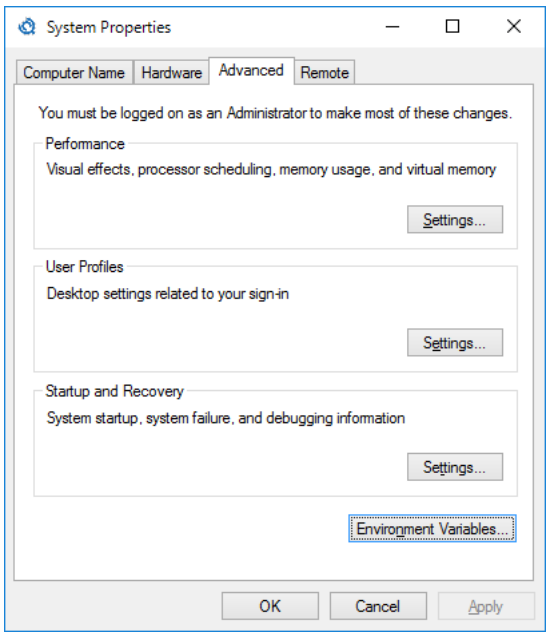
Exchange management console no longer starts

If NoSpamProxy and Exchange 2010 are installed on the same server, the Exchange management console does no longer work properly. The reason for that is the .NET Framework. The Exchange management console requires an older version of the .NET Framework while the NoSpamProxy management console works with version 4.7.2 exclusively.

If NoSpamProxy and Microsoft Exchange are installed on the same server, make sure that Exchange supports the respective version of the .NET Framework before installing or upgrading. The Exchange Server Supportability Matrix offers an overview of supported versions.

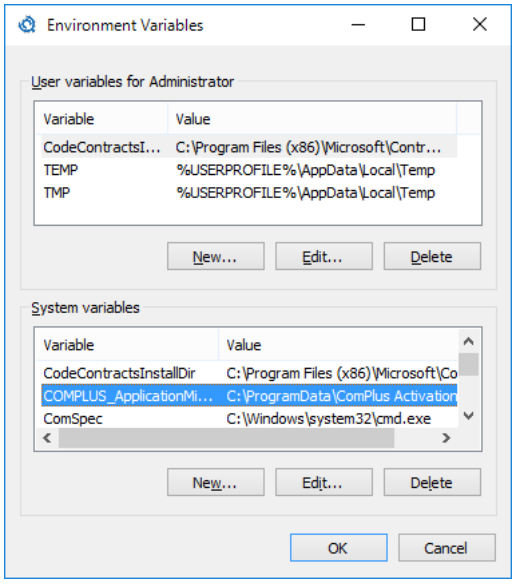
In order for the correct .NET Framework version to be used, NoSpamProxy creates an environment variable with the name `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath`. This variable refers to a path where a configuration file with corresponding settings is stored. When invoking any management console, the respective variable and thus the configuration file are used. Opening the Exchange MMC causes the known problems. To be able to further use the Exchange MMC, only the following workaround is available: The environment variable is deleted permanently and the NoSpamProxy MMC must be invoked via a batch file in which the required environment variables are defined in advance. The advantage is in this case that the environment variable is only applied to programs invoked from the context of the batch file.

Open the 'Advanced system properties' via `Start -> Execute -> sysdm.cpl` (Picture 206). Select the button **Environment Variables...** in the tab **Advanced**.



Picture 206: Advanced system properties

The window with the 'Environment Variables' opens (Picture 207).



Picture 207: The environment variables of the systems and user signed in

Select the entry `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` in the section **System variables** and click on **Edit**. Copy the path from the field **Value** into the clipboard and delete the complete entry afterwards. Close both dialogs by clicking on **OK** respectively. Open Notepad and paste the path you have just copied into the clipboard. Additionally, add the following lines (copy the following text consecutively without any additional blanks into one line):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```

Paste the path from the clipboard into the first line. The Notepad file should then be set up analogously as follows (copy the following text consecutively without any additional blanks into one line):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=C:\
ProgramData\ComPlus Activation Configurations\mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```

Note that the depiction of the batch file is falsified by automatic word wrap. The command must be contained in one line.

Finally, adjust the path to the MSC file of the management console (if required) and store the Notepad content as NoSpamProxy-MMC.bat. If you start the batch file, one should be able to successfully open the NoSpamProxy MMC. Starting from Windows 2008 R2 with activated UAC, however, you must execute the batch file always as administrator. The Exchange MMC should now open without problems as well.

Checking the connections

NoSpamProxy by default works as SMTP proxy and is thus dependent on the availability of the inbound email servers. There are several factors which might prevent availability of the gateway or the email server. Causes might be:

- **Lacking name resolution**
  Depending on the setting, NoSpamProxy uses the provided IP address or the server name of the email server. If the server name is provided, it must be resolvable via DNS.
- **Incorrectly configured email servers**
  Ensure that the email servers also accept connections from NoSpamProxy. Especially after a switch to NoSpamProxy, it is possible that the email server only accepts emails from the former system. Moreover, it must be ensured for the email Smarthost for external addresses that the gateway may use this Smarthost as relay.
- **Obstructed routes**
  Check whether NoSpamProxy can establish the connection to the other email servers or whether a firewall on the NoSpamProxy server, the target server or on the route to them prevents connection.

To check the connection to other servers, you can use the program Telnet which has already been described. The following four tests are available:

- **Simulation: NoSpamProxy to internal email server**
  Start the program `TELNET ip-address-of-internal-mail-server 25`. Your internal email server must reply. If this is not the case, you must check the network connection, firewall rules and the internal email server. As long as NoSpamProxy cannot connect to this internal email server, it will not accept any external connection.
- **External simulation**
  Start a TELNET connection on NoSpamProxy to the IP address of the server indicated as external and create an email. NoSpamProxy must identify this connection as "external". As soon as you have entered the envelope (HELO, MAIL FROM, RCPT TO, DATA), the gateway will check the data gathered so far and establish a connection to the internal email server. You can view this, e.g. in the status overview of NoSpamProxy as well.
- **Forwarding to external addresses**
  Analogous to the connection to local servers, NoSpamProxy must send emails to external addresses via an email server as well. Check with `TELNET target server 25` whether this server of NoSpamProxy is available and accepts emails. This email server must allow NoSpamProxy to send emails to the internet, this means to use this server as relay. If this server is not available, NoSpamProxy does no longer accept any internal connections.
- **Internal connection**
  This test is implemented from your internal email server. Start `TELNET IP-address-of-NoSpamProxy 25` here. This time, NoSpamProxy needs to accept your test data.

Performance counters

The performance counters are a very versatile means of checking functions of NoSpamProxy in realtime. Not all performance counters are displayed via the management console client but can rather be viewed via the Windows program "Reliability and performance monitoring" ("perfmon.exe") . By using this, you can monitor the work of NoSpamProxy as well as that of your operating systems. This can also be realised automatically through another software such as the Microsoft System Center Operations Manager . For instance, you can view how often emails with a specific threshold value (SCL) have been blocked or which file volume the emails have.

The performance counters are not displayed in the client except for a few exceptions in the "server performance" node. They rather serve the automatic monitoring of NoSpamProxy through third party software products.

The values available for NoSpamProxy are listed below. Independent of the selected language of the operating system or that of NoSpamProxy, the names of the performance counters are always in English.

NoSpamProxy Globals

- Accepted emails
- Blocked connections

- Delivery failures
- Rejected at envelope level
- Rejected at body level

NoSpamProxy Network Utilization

- Bytes Sent
- Bytes Received
- Active inbound connections
- Active outbound connections

NoSpamProxy Assigned Spam Confidence Levels

- SCL lower than 0
- SCL between 0 and 0.9
- SCL between 1 and 1.9
- SCL between 2 and 2.9
- SCL between 3 and 3.9
- SCL between 4 and 4.9
- SCL between 5 and 5.9
- SCL between 6 and 6.9
- SCL between 7 and 7.9
- SCL between 8 and 8.9
- SCL between 9 and 10

NoSpamProxy Actions

- Number of times run
- Permanently blocked
- Temporarily blocked
- Active outbound connections

NoSpamProxy Performance

- Average Response Time
- Filter requests awaiting execution
- Average action execution time
- Average filter execution time
- Average filter queue time
- Pagefile usage

Settings via the configuration file

Direct changes to the configuration can put NoSpamProxy into a state where it can no longer be started.

Activate the option 'Delivering invalid emails'

If NoSpamProxy cannot check emails due to incorrect setup, the email is rejected. This function can be activated and deactivated via the configuration file.

Activate this option only if you are absolutely sure it is necessary and you know what you are doing. Affected emails cannot be checked for spam and viruses by the Gateway Role.

To activate the option, open the configuration file of the Gateway Role of NoSpamProxy. The path to the file is generally named `%ProgramData%\Net at Work Mail Gateway\Configuration\GatewayRole.config`. Please consider that you cannot safe the file before the service of the Gateway Role is stopped. Otherwise, all changes are discarded.

Please search for the following line in the file:

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

In the section **netatwork.nospamproxy.proxyconfiguration** search for the following key **dispatchInvalidMails**. Make sure that it looks like displayed below; otherwise add it as shown below:

```
<dispatchInvalidMails isEnabled="true" />
```

The lines should appear as follows:

```
<dispatchInvalidMails isEnabled="true" />
</netatwork.nospamproxy.proxyconfiguration>
```

Save the file and restart the Gateway Role afterwards.

Processing of RTF files during content filtering

RTF emails as well as attached files are encoded and transferred as TNEF files, a proprietary Microsoft format (Transport Neutral Encapsulation Format). These encoded emails including all attachments are then converted into a single attachment named `winmail.dat` by default.

In case one of the file types included in the winmail.dat attachment was selected during the configuration of a condition for content filtering, NoSpamProxy will open the TNEF container and add the individual attachments to the email.

A notification about the processing of the TNEF container and the subsequent modification of the email is added to the Message tracking dialog.

SMTP RFCs

Most protocols used on the internet are based on ideas and agreements between certain groups of people; these ideas and agreements were declared to be the standard at some point. These documents have the abbreviation RFC (Request for Comment). In the early years of the internet, several people of different companies and institutes have worked on various projects and provided their ideas and protocol definitions for discussion due to a lack of a central coordination authority.

NoSpamProxy uses the SMTP protocol. The details on how SMTP works and which reaction has to follow which action are described in corresponding RFC documents.

The following list shows the most important RFC documents:

- RFC 1123 for important additional information
- RFC 1893 und RFC 2034 for information about enhanced status codes
- RFC 2821 Simple Mail Transfer Protocol (SMTP)
- RFC 2822 Internet Message Format
- RFC 2554, AUTH, Authentication
- RFC 3207, STARTTLS, Start transport layer security

SMTP Error codes

All responses an SMTP server reports to the other system start with a number. The text following the numerical indication is optional, can change from email server to an email server and is not evaluated by applications; it exclusively serves as help for administrators during troubleshooting.

SMTP Error codes are described in these RFCs:

- RFC 2821 Simple Mail Transfer Protocol (SMTP)
- RFC 2822 Internet Message Format
- Q257186 XIMS: SMTP Reply Codes (RFC 821)
- Q257167 XIMS: SMTP Reply Code 451

The return codes set up as follows. Each code is three-digit. The first number indicates the classification of the report:

- 1yz = ok
- 2yz = accepted
- 3yz = intermediate ok (intermediate report)
- 4yz = tempor error (preliminary negative)
- 5yz = permanent error

The second number defines the source of the report:

- x0z = Syntax
- x1z = Info

- x2z = Connection
- x3z/x4z = not defined
- x5z = Mail system

The most frequently occurring error numbers are listed here again:

- 200 (non-standard success response, see RFC 876)
- 211 System status, or system help reply
- 214 Help message
- 220 <domain> Service ready
- 221 <domain> Service closing transmission channel
- 250 Requested mail action okay, completed
- 251 User not local; will forward to <forward-path>
- 354 Start mail input; end with <CRLF>.<CRLF>
- 421 <domain> Service not available, closing transmission channel
- 450 Requested mail action not taken: mailbox unavailable
- 451 Requested action aborted: local error in processing
- 452 Requested action not taken: insufficient system storage
- 500 Syntax error, command unrecognised
- 501 Syntax error in parameters or arguments
- 502 Command not implemented
- 503 Bad sequence of commands
- 504 Command parameter not implemented
- 521 <domain> does not accept mail (see RFC 1846)
- 530 Access denied
- 535 SMTP Authentication unsuccessful/Bad user name or password
- 550 Requested action not taken: mailbox unavailable
- 551 User not local; please try <forward-path>
- 552 Requested mail action aborted: exceeded storage allocation
- 553 Requested action not taken: mailbox name not allowed
- 554 Transaction failed

To allow for a more exact differentiation between the individual cases of error statuses based on the third digit, enhanced status messages were introduced. They enable the return of more than 10 different status codes.

They are specified in more detail in the following RFC document:

- Q256321 RFC 1893 (Q256321) for Enhanced Status Codes for Delivery Status Notification (DSN) messages

The response of a server can look as follows:

```
250 2.1.0 user1@example.com....Sender OK
```

Behind the three-digit message 250, the detailed message 2.1.0 follows.

SMTP Time-outs

When two systems connect, delays in processing can always occur. Nowadays, an overloaded line rarely is the cause for delays.

As a rule, the inbound email server must accept and store the data; this will take some time. It does not send its status message before having concluded these activities.

NoSpamProxy also accepts an email partially which takes some time to start the corresponding actions based on the rules. Only after completion the inbound system receives a message to continue the transfer or interrupt the connection.

These maximum waiting times are defined in the "RFC 2821- Simple Mail Transfer Protocol" as well.

The following times are recommended:

- **First 220 message after the connection establishment: 5 minutes**
  The sender must differentiate between a connection not accepted and a delayed response due to high load. The TCP/IP stack very frequently accepts a connection, however, the SMTP server delays the dispatch of the 220 message until the system allows processing of further emails.
- **MAIL-command: 5 minutes**
  After a maximum of 5 minutes, an email server must have replied to the "MAIL FROM".
- **RCPT-command: 5 minutes**
  After a maximum of 5 minutes, an email server must have replied to the "RCPT TO".
- **DATA: 2 minutes**
  After a maximum of 2 minutes, an email server must react to the command "DATA". This is an important value for NoSpamProxy since the processing of the envelope filters must not take longer. Usually, the email server replies with a "354 Start Input".
- **Data block: 3 minutes**
  The transfer of the actual email ensues via TCP/IP blocks. The confirmation of a block must not tarry for more than 3 minutes.
- **DATA conclusion: 10 minutes**
  After the transfer of the email, the sending email server sends a final line a email server must only containing one full stop and waits for the confirmation. The inbound email server has up to 10 minutes to reply to this signal with "250 OK" or another message. Thus, NoSpamProxy has the exactly same amount of time to evaluate the email through different filters, change it through actions and deliver it to the internal email server. Only if the inbound email server has confirmed the email with "250 OK", it also undertakes the responsibility for further delivery. The gateway only sends this message if the internal email server has completely accepted the email. NoSpamProxy is not responsible for the further transfer.

- **Recipient time-out: 5 minutes**
  Vice versa, there is a time-out. If the inbound email server has transmitted its response, the sender is required to transfer the next commands. If the next message stays out, however, the recipient should at least wait for 5 minutes before the connection is interrupted.

Glossary

- **API**
  Programming interface which enables third party applications to access a software system. http://de.wikipedia.org/wiki/Programmierschnittstelle
- **C number**
  The C number is your distinct licence number. It helps the support team of Net at Work in processing your requests as soon as possible.
- **CER**
  File extension for indicating files containing public certificates.
- **DER**
  File extension for indicating files containing public certificates.
- **FQDN**
  Fully qualified domain name. A computer with the name `mailserver` in the DNS domain `example.com` has the name `mailserver.example.com` as FQDN. http://de.wikipedia.org/wiki/FQDN#Fully_Qualified_Domain_Name_.28FQDN.29
- **OCSP - Online Certificate Status Protocol**
  An Internet protocol to request the status of a certificate at a validation service. Through an OCSP service, e.g. invalid certificates can be declared invalid even before the expiration of their validity. http://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol
- **Public certificates**
  Public certificates are certificates which do not contain any private key. These certificates can only be used for encryption. http://de.wikipedia.org/wiki/Digitales_Zertifikat
- **Personal certificates**
  Personal certificates are certificates which contain a private key and a public key. With these certificates, one can sign and decrypt messages which were previously encrypted with the public key of this certificate. http://de.wikipedia.org/wiki/Digitales_Zertifikat
- **Placeholder**
  A placeholder (or wildcard) refers to reserved characters serving for the replacement by other characters. The asterisk '*' stands for any number of characters (even zero). Example: Searching for 'max*', finds all words starting with 'max', 'maximal', 'maximilian' etc. Searching for 'm?x', finds 'mix', 'mux', 'max', 'm4x' etc.
- **Signing**
  The procedure of signing proves the authenticity of a message by creating a checksum for the message with the help of the private key. The public part of the certificate is attached to the message and transmitted to the recipient. The recipient can check the checksum with the help of the public key.
- **P12**
  File extension for indicating files containing private certificates.

- **PFX**
  File extension for indicating files containing private certificates.
- **RFC**
  Technical and organisational documents for determining the communication standard in the Internet. http://de.wikipedia.org/wiki/Request_for_Comments
- **S/MIME**
  Standard for signing and encrypting an MIME-encapsulated email by an asymmetric cryptographic system. http://de.wikipedia.org/wiki/S/MIME
- **StartTLS**
  A procedure to initiate email encryption on the transport level. http://de.wikipedia.org/wiki/STARTTLS