Net at Work
Building IT-Excellence.

NoSpamProxy 13.2

Outlook Add-In User Manual

- Protection
- Encryption
- Large Files

Imprint

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

Trademarks

13 February 2020

Contents

1. Using the NoSpamProxy Outlook Add-In

Installation notes

When installing the Outlook Add-in via MSI file, it must be located on a local hard disk. Installation via a UNC path is not possible.

Functions of the Outlook Add-In

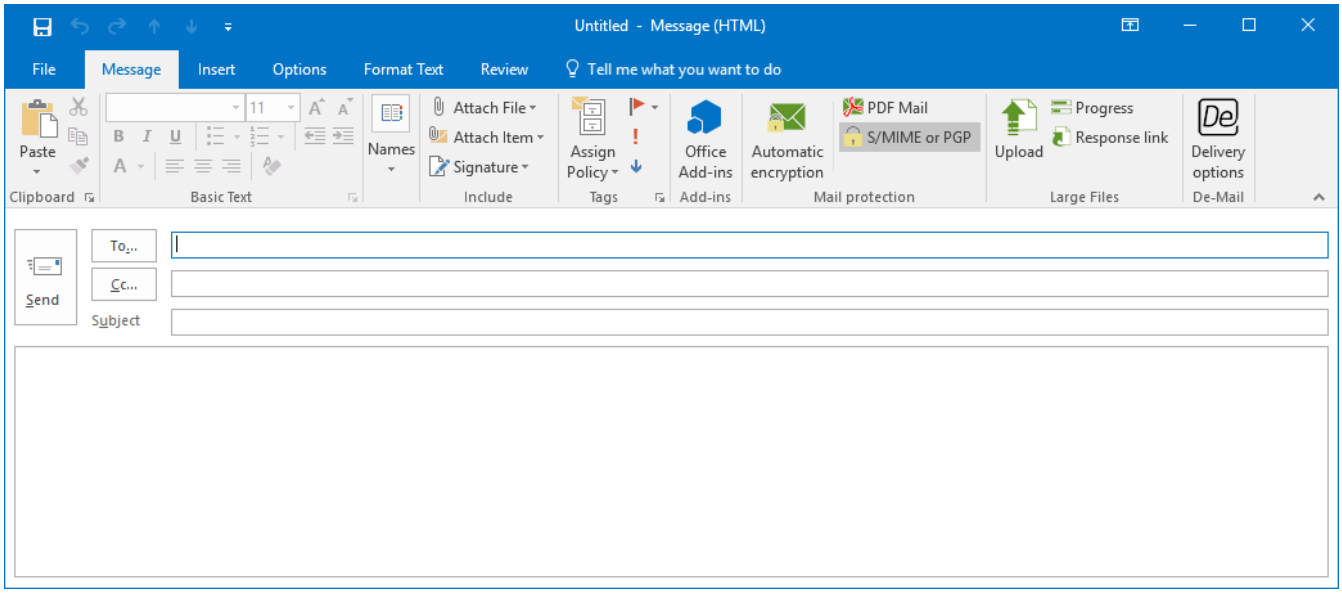
The functions of the Outlook Add-In are displayed on the main ribbon. The add-in offers support for Composing Mails as well as Reading protected mails.

Composing Emails

The following functions are available:

- **Automatic encryption**
  Protects the email using one of the available security measures.
- **PDF Mail**
  Converts email content including all attachments into a password-protected PDF document.
- **S/MIME or PGP**
  Allows signing and encrypting of emails via cryptographic keys such as PGP key pairs or S/MIME certificates.
- **De-Mail**
  Shows all delivery options for De-Mails.
- **Large Files**
  Transfers large files via the NoSpamProxy Web Portal. This capability creates a link through which the recipient can download sent files securely via SSL. Password protection can be added to the link created.

When composing new emails, available functions are displayed on the **Message** tab on the main ribbon (Picture 1). The functions are divided into three sections: **Email protection**, **De-Mail** and **Large Files**.

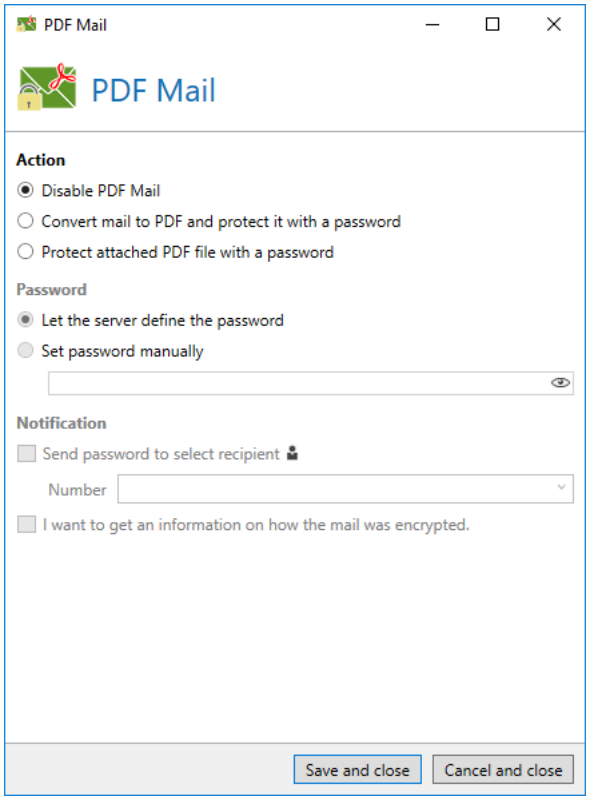


Picture 1: The New email window with installed Outlook Add-In

- The section **Email protection** offers options for protecting email content including attachments. The PDF Mail option allows for secure delivery of emails without applying cryptographic keys via the item PDF Mail. The item S/MIME or PGP controls the use of cryptographic keys. Automatic encryption facilitates the delivery of encrypted emails to users not in possession cryptographic keys. In this case, NoSpamProxy Encryption automatically selects the suitable delivery type and securely delivers it to the recipient.
- The dispatch type and confirmations for De-Mail can be set by clicking Dispatch options under **De-Mail**.
- In the section **Large Files**, you can select documents or other files you wish to transfer via the button **Upload**. The Outlook Add-In supports users by automatically selecting whether and how the file is transferred based on the email address of the sender. This is effected through content filters to be configured by the administrator. These content filters enable the add-in to immediately notify the user of blocked file types or files that exceed their maximum size. The filters also ensure that company requirements for allowed files are met, and that files are automatically transferred via Large Files when using the Outlook function **Attach file**. The button **Progress** provides you with information on the upload progress of the file to the Web Portal of your company.

PDF Mail

In the section **Action** in the **PDF Mail** (Picture 2) dialog you can select whether attached PDF documents are secured with a password or whether PDF protection is also added to the email. In this case, the attachments are included in the email itself. By default, the option **Deactivate PDF Mail** is selected.



Picture 2: PDF Mail dialog

The **Password** option lets you automatically generate passwords, or set passwords for NoSpamProxy Encryption manually. The password is sent to sender or recipient depending on the settings in the section **Notification**.

In the section **Notification** the recipients of the password can be determined. The options are listed in the following table:

Text message	Request report	Action by NoSpamProxy
No	No	The sender of the email receives the password which can be forwarded via text message or phone to the recipient of the protected PDF mail.
No	Yes	A message including the password is sent to the sender.
Yes	No	An SMS including the password is sent to the recipient.
Yes	Yes	A text message including the password is sent to the recipient; a message including the password is sent to the sender.

In order to send the password via text message to the recipient, please use the function **Send password to** and select the desired recipient via the image at the end of the line. If recipients have been entered into the "To" field of the email in the Compose email dialog, the contact data of the first recipient is entered into the **Send password to** field automatically. Please check the phone number after the selection of a text message recipient or enter the phone number for the text message receipt directly into the drop down list.

The following phone number formats are valid and can be used:

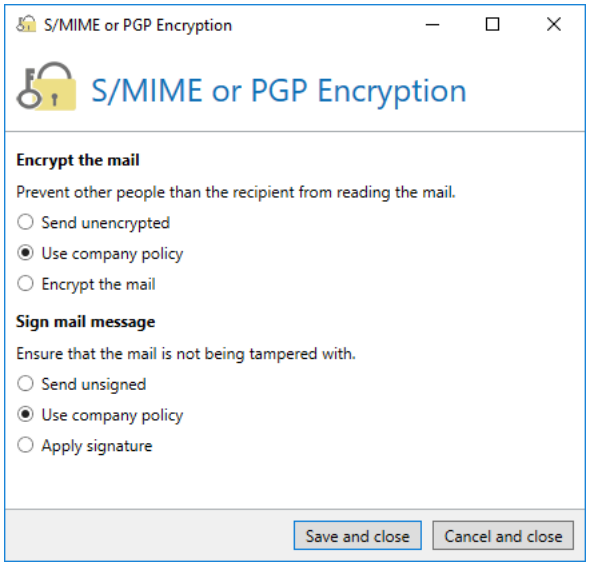
```
+49 (code without 0) number
e.g.: +49 (1234) 567890
e.g.: +49 1234 567890

0049 (code without 0) number
e.g.: 0049 (1234) 567890
e.g.: 0049 1234 567890

code without 0 number
e.g.: 01234 567890
```

S/MIME or PGP

The dialog for **S/MIME or PGP** (Picture 3) provides settings for the digital email signature and encryption with cryptographic keys such as S/MIME certificates and PGP key pairs.



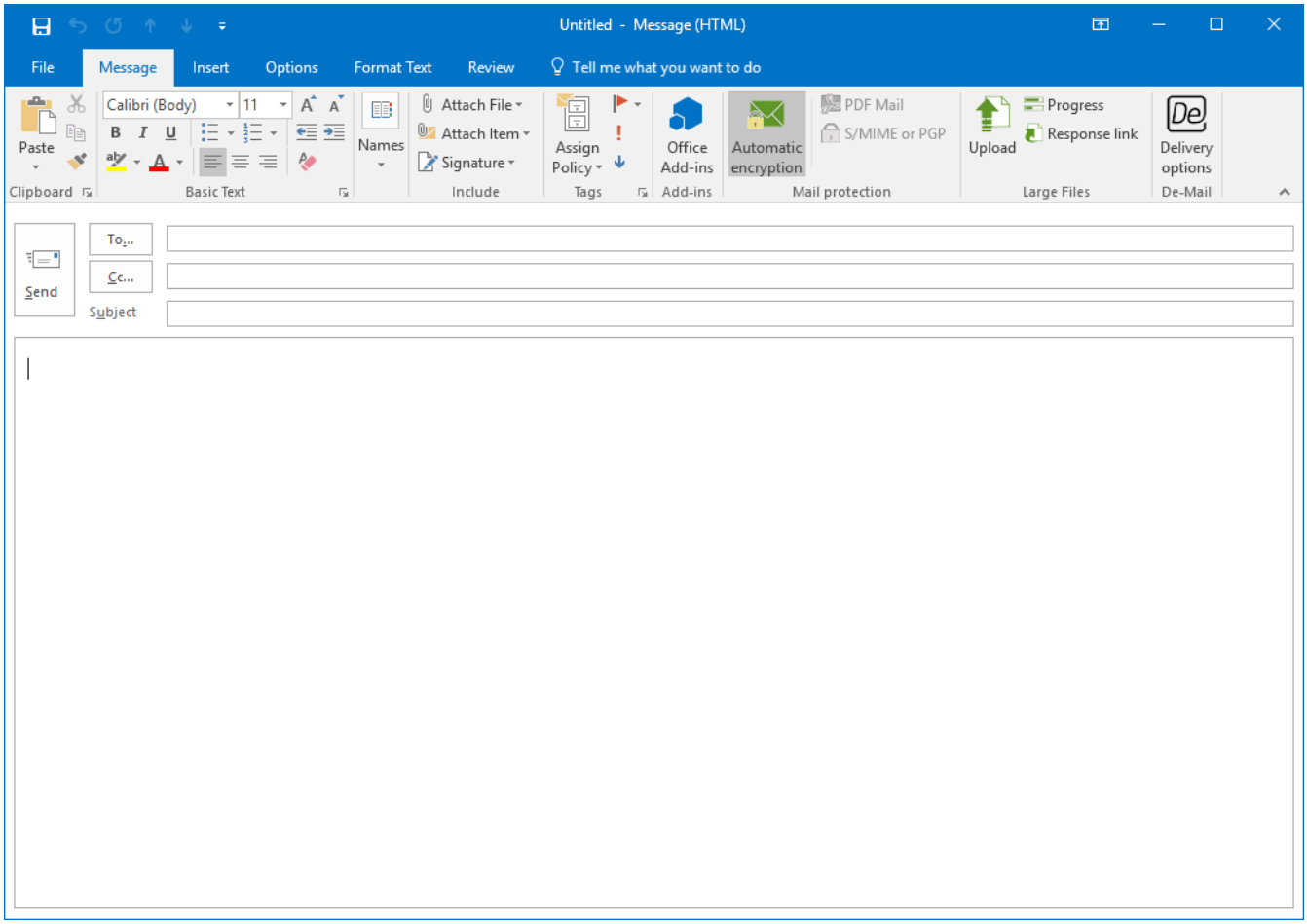
Picture 3: Dialog for S/MIME or PGP

In the dialog for **S/MIME or PGP** (Picture 3), you can set whether signature and encryption should be enforced, suppressed or configured based on the company policy.

If an action is set in this dialog that is in conflict with the existing configuration of NoSpamProxy Encryption, the email will not be delivered.

Automatic encryption

The function **Automatic encryption** is the simplest way of securely transferring emails. (Picture 4).



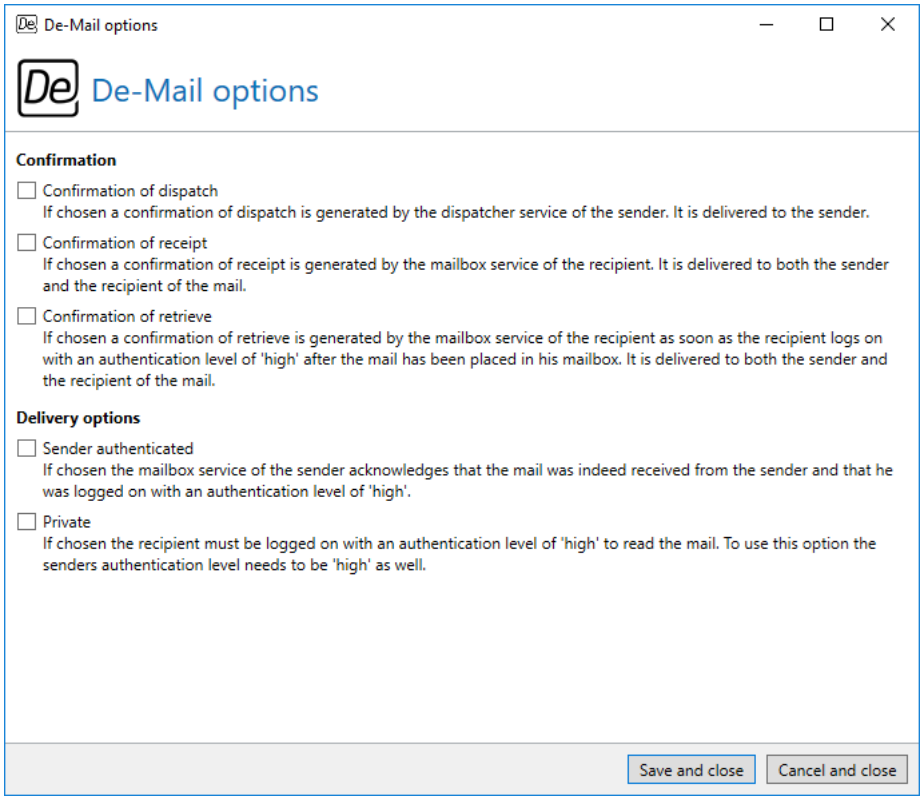
Picture 4: The function 'Automatic encryption'

In case **Automatic encryption** is selected, an email signature and encryption through cryptographic keys for the respective e-ail is requested. If the encryption via certificates or PGP keys is not possible, the email will be secured through "PDF Mail". For PDF Mail, a password is created automatically and delivered to the sender of the email. In doing so, the entire email content including all attachments is

embedded into the protected PDF document, facilitating the secure delivery of emails to all recipients, even if they are not in the possession of cryptographic keys.

De-Mail

Via the button **Dispatch options** in the section **De-Mail** you open a dialog for configuring confirmations and delivery options for De-Mails (Picture 5).



Picture 5: De-Mail dialog

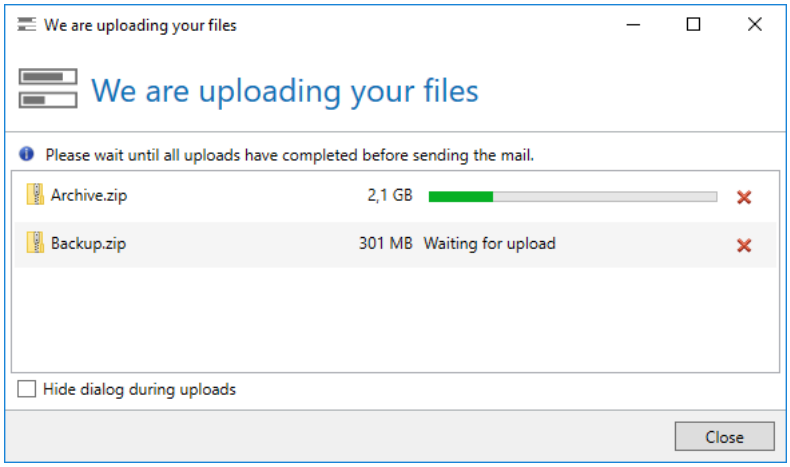
In the section **Confirmation** you configure confirmation notifications for dispatch, receipt and retrieval of messages. The section **Dispatch type** defines how De-Mail messages are transferred.

Large Files

To securely transfer such documents to recipients, you can transfer the files via the NoSpamProxy Web Portal. To do so, click on **Upload** under **Large Files** on the main ribbon and select the files you wish to transfer. The files are then transferred to the Web Portal in the background. As soon as the transfer is completed, a link for each selected file is attached to the email. This link can be used to download the file to a computer.

To check the progress of the upload, click on the button **Progress** (Picture 6). Potential issues occurring during file transfer are also displayed here, for example if the file you selected exceeds the maximum

size set by your system administrator. By clicking on the **red X**, you can cancel the file upload or remove files that have not yet been uploaded.

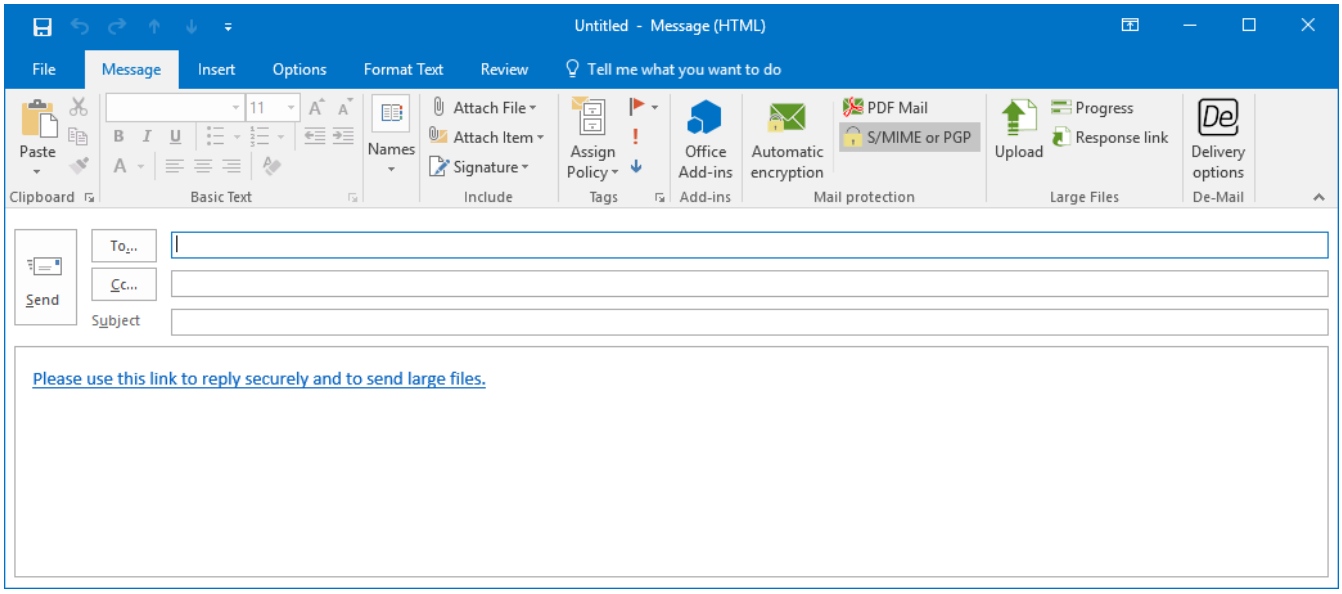


Picture 6: Two files uploaded to the Web Portal

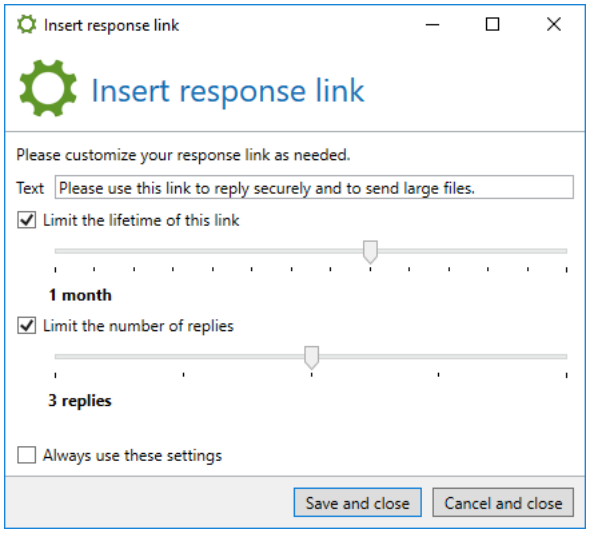
As usual, you can also attach files to the email via the button **Attach files** or via Drag and Drop. Depending on the settings, the file is either attached to the email directly or transferred via the Web Portal.

The "Attach file" button can, depending on your email server settings, attach files of a maximum of 20MB to the email. By default, files larger than 2MB are replaced with an HTML file which points to the Web Portal. This file is used to download the original file from the Web Portal. The "Upload" button in Large Files never attaches files to the email directly but always uses the Web Portal. The upload function is not limited in size but determined by the administrator of NoSpamProxy. Thus, if allowed by the administrator, the upload of files with sizes of up to several gigabytes is possible.

You can also add a **Response link** to the email. Via this link, the recipient(s) can reply via the secure Web Portal and transfer large files (Picture 7). Upon clicking the button, the dialog (Picture 8) opens. This dialog is used to determine the text for the link. In addition, you can restrict the period of validity for the link. For example, you can set that the recipient(s) can only use the link for one month and three replies. If you restrict the replies to a certain number, each recipient has the possibility to exhaust the selected number of replies. Via the button **Always use these values**, you can determine whether the values you just set are also used as default values for future links in this dialog.



Picture 7: Reply link in the email



Picture 8: Reply link

Protecting Large Files links with a password

You can protect large files links with a password by configuring a password protection either through an appropriate content filtering action in NoSpamProxy or through manual activation during composition. The password requested for download is always the password stored in the individual partner user entries.

Settings in NoSpamProxy

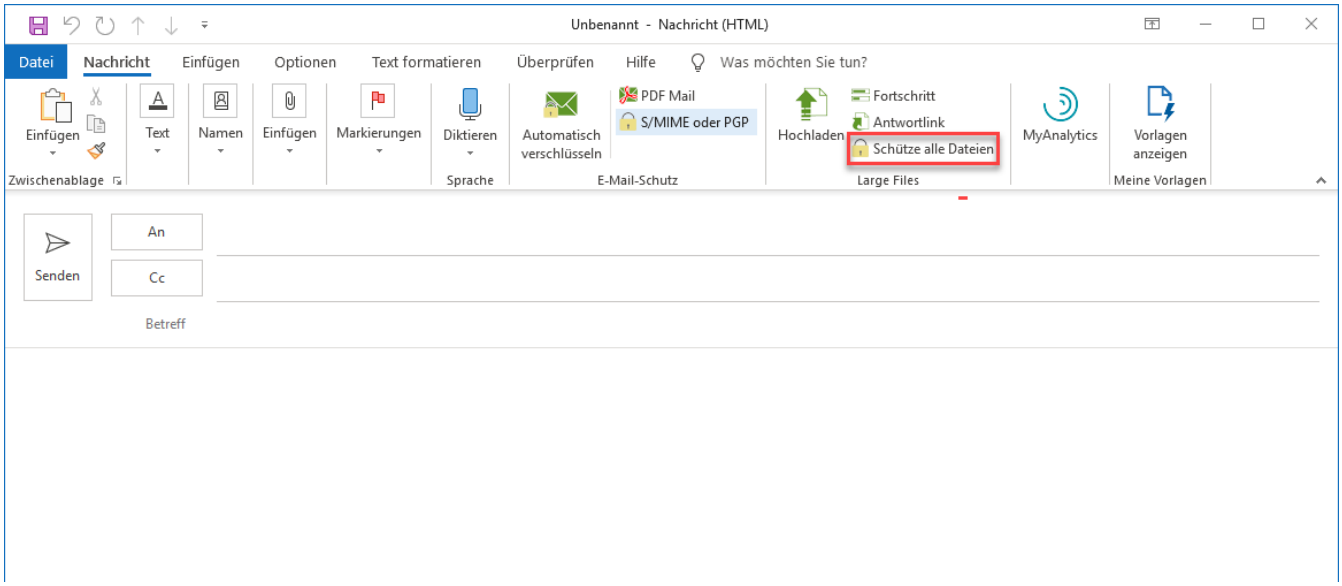
In order to enable password protection of Large Files links, you must make the following settings via the NoSpamProxy console:

- Make sure that under **Configuration/Rules**, for an outbound email rule on the **General** tab you have selected the option **Enabled** under **Content filtering**. Please refer to the **Rules** chapter in the NoSpamProxy manual.
- Decide under **Configuration/Content filter/Content filter actions** on the tab **Attachments** of an action, whether you want to require password protection for all outbound emails or let the respective user decide. Please refer to the chapter **Content filter actions** in the NoSpamProxy manual.
- Make sure that under **Configuration/Content filter/Content filters** you have created a content filter entry for a content filter that triggers the desired action for **Untrusted or outbound emails**. Please refer to the **Content Filter** chapter in the NoSpamProxy manual.
- Make sure that the appropriate outbound policy (content filter) is configured for corporate users. You can set this as a default user setting, at the user level, or for individual email addresses. See **Domains and users** in the NoSpamProxy manual.
- Make sure that the appropriate outbound policy (content filter) is configured for partners. You can configure this as a default partner setting, at the domain level, or at the user level. See **Partner** in the NoSpamProxy manual.

Enabling password protection

In the window for a new email, click **Protect all files** under **Large Files** in the ribbon. The password protection for Large Files links is then activated for the respective email. The password requested is the password stored in a partner for the respective user. Please refer to the chapter **User entry of a partner domain** in the NoSpamProxy user manual.

If **Protect all files** is disabled, the password protection has already been preset by your administrator in the content filter action.



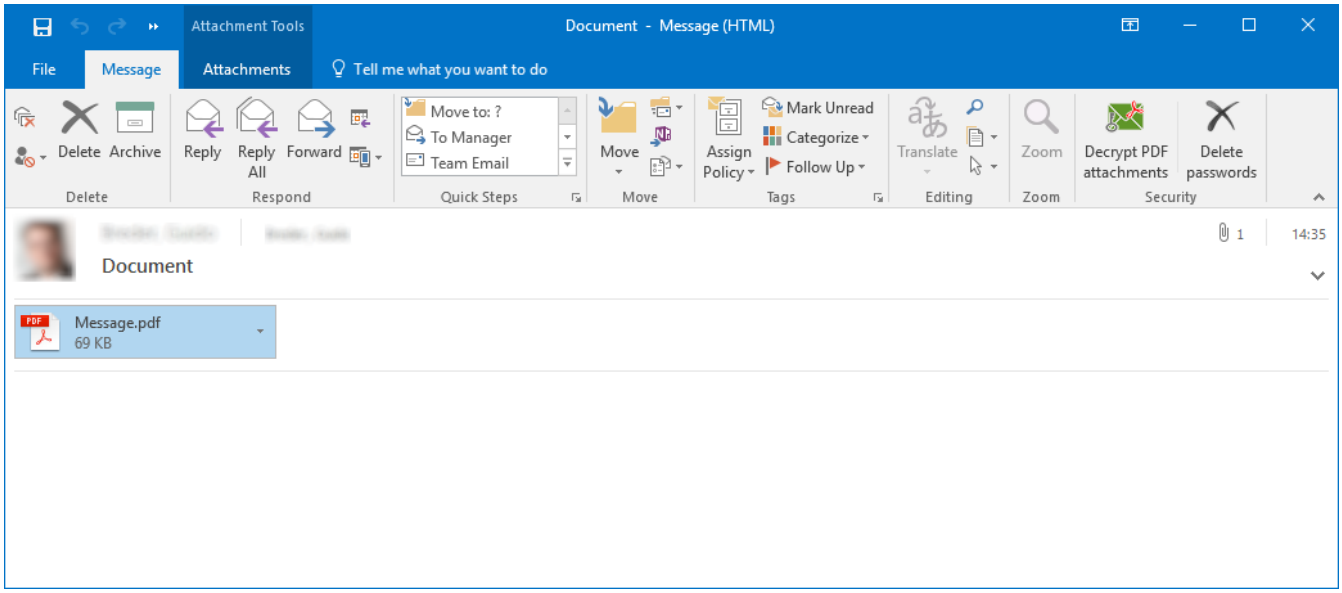
Picture 9: Enabling password protection for Large Files links

Reading Emails

When reading emails the following functions are available:

- **Decrypt PDF attachments**
  Decrypts password-protected PDF attachments and removes the password.
- **Delete passwords**
  Deletes stored PDF decryption passwords.

When reading an email, available functions are displayed on the main ribbon. The functions for the PDF encryption can be activated by either selecting or opening emails with one or more PDF attachment(s) (Picture 10).



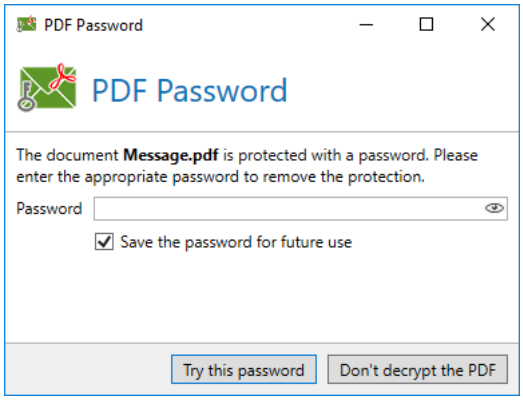
Picture 10: Email with PDF attachment in reading mode

Decrypting PDF attachments

To open password-protected documents at a later point in time, the password must be archived. Losing passwords results in PDF documents which cannot be opened.

The Outlook Add-In lets you remove password protection of PDF files. If you select the function, the following steps are executed:

1. The Outlook Add-In checks all PDF attachments for password protection.
2. The Outlook Add-In attempts to decrypt password-protected attachments using stored passwords.
3. For attachments which cannot be decrypted with stored passwords, the password is requested (Picture 11). You can either provide the password or skip the decryption by clicking **Do not decrypt this PDF**.



Picture 11: Dialog for password entry

The dialog for the password entry also offers options for storing passwords for later use. Select the option **Store password for later use**, then select **Try this password** to add the entered password to the list of stored passwords after successful decryption. The setting of the option **Store password for future use** is stored in any case.

Documents for which decryption failed are displayed along with their file name and the reason for the failure. PDF files which do not have any password protection and thus need not be decrypted do not appear in this list.

For successfully decrypted documents, a report is attached to the email. The default file name is "PDF decryption report.txt". The content appears as shown in the following example:

```
The following attachments have been decrypted on 15-06-2016 01:48:46 pm
Invoice.pdf
Contract.pdf
```

Deleting passwords

Previously stored passwords for PDF decryption can be deleted via this function.

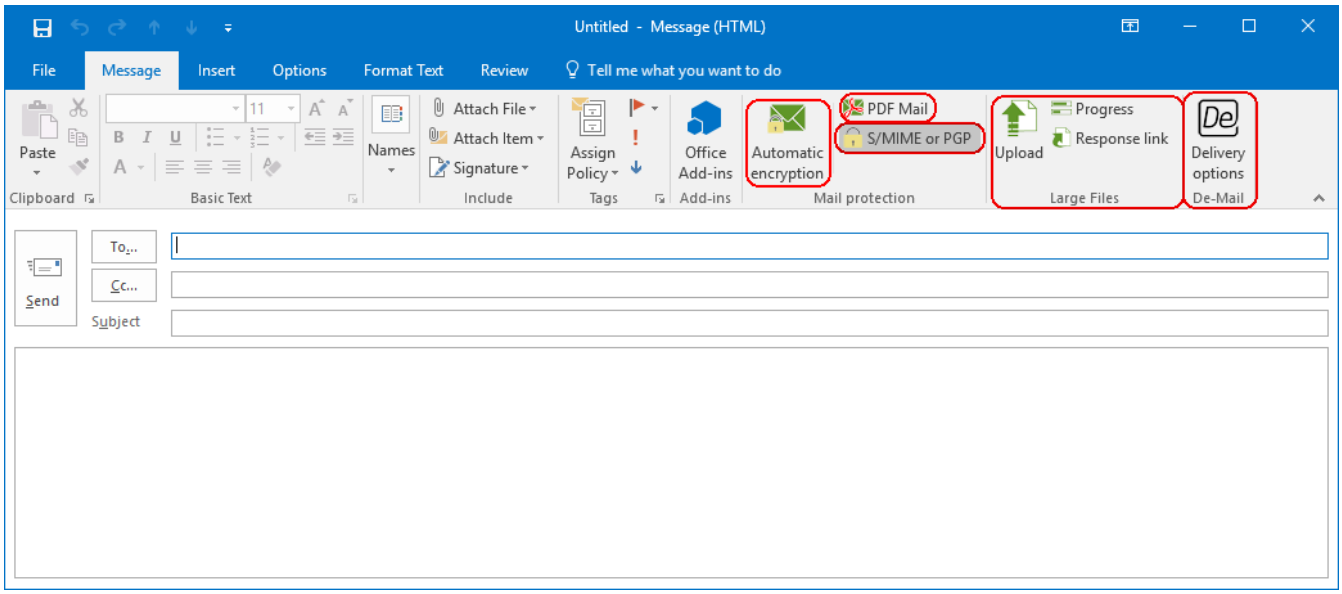
2. Hideable sections

Specific sections of the Outlook Add-In are configurable. If functions of the Add-In are not available in your company, the respective sections can be hidden. The functional scope of the add-in can be adjusted to your company's requirements. Find more information on showing and hiding sections under NoSpamProxy - Outlook Add-In group policies. The configurable sections are listed in the following chapters.

Composing Emails

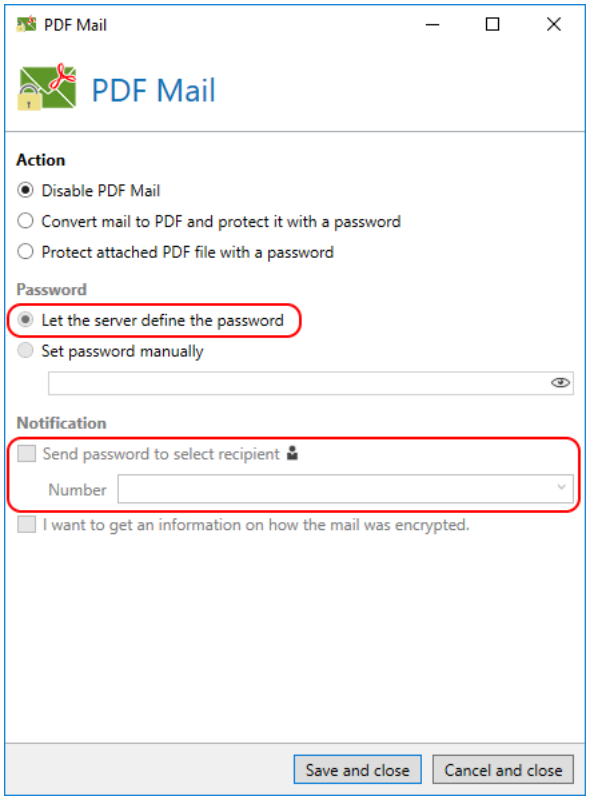
All functions on the ribbon can be shown or hidden (Picture 12). The function for **De-Mail** is hidden by default.

The section for Large Files is only shown if an URL was configured for the connection to the Web Portal. The **Options** button is hidden if the options have already been set via group policy.



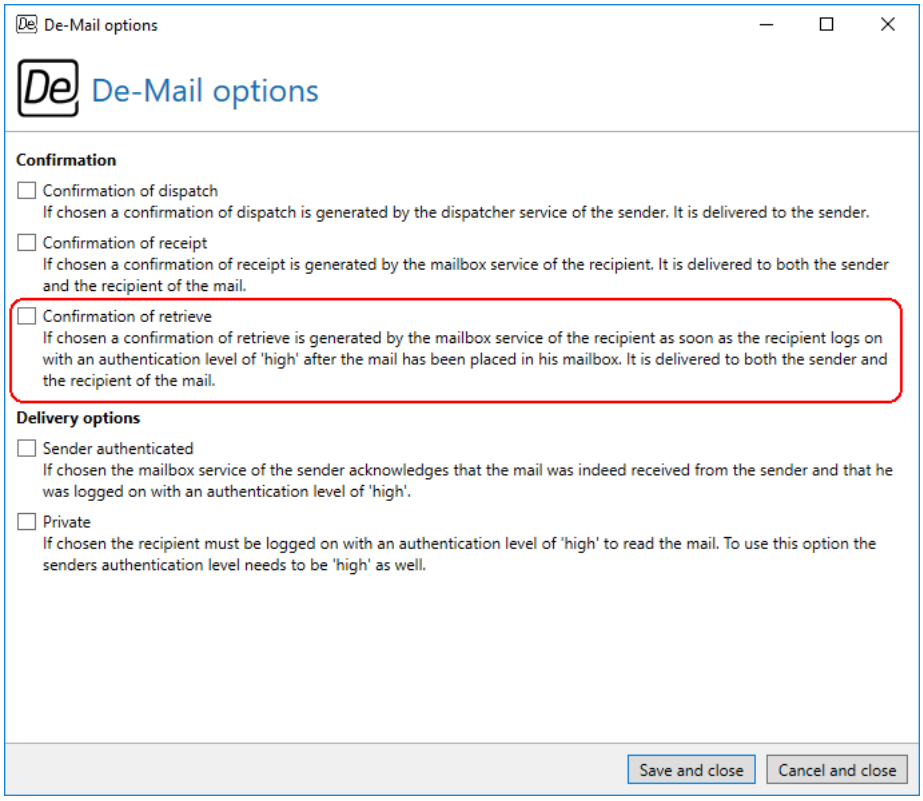
Picture 12: Functions available when composing emails

In the **PDF Mail** dialog, the automatic assignment of passwords and the dispatch of text messages can be hidden (Picture 13).



Picture 13: Hideable functions in PDF Mail dialog

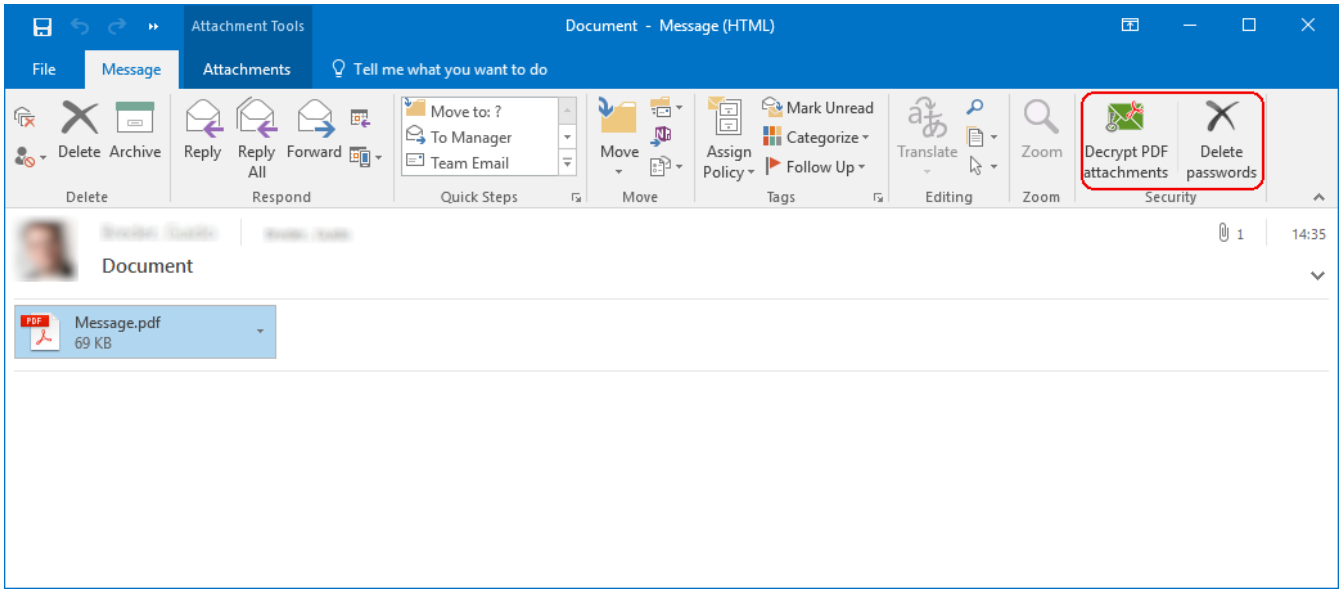
The option **Pickup notification** in the **De-Mail** dialog (Picture 14) is not available to most users of the De-Mail portal. It is hidden by default.



Picture 14: Hideable functions in De-Mail dialog

Reading mails

The section on decrypting PDF attachments and deleting stored passwords as well as the creation of a password reset email can be shown or hidden (Picture 15).



Picture 15: Functions available when reading an email (bordered red)

3. 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.