



Outlook Add-in

Version 14

Legal information

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

Copyright © 2023 Net at Work GmbH

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

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® and Azure® are registered trademarks of Microsoft Corporation. NoSpamProxy® and 32Guards® are registered trademarks of Net at Work GmbH. All other trademarks used belong to the respective manufacturers or owners.

THIS DOCUMENT WAS LAST EDITED ON NOVEMBER 27, 2023.

Content

Overview of the functions	1
Functions of the Outlook Add-In when composing emails	1
Functions of the Outlook Add-In when reading emails	2
Encrypt automatically	4
PDF Mail	5
S/MIME or PGP	10
Large Files	12
De-Mail	18
Decrypting PDF attachments	20
Hideable areas	22
Help and support	26

Overview of the functions



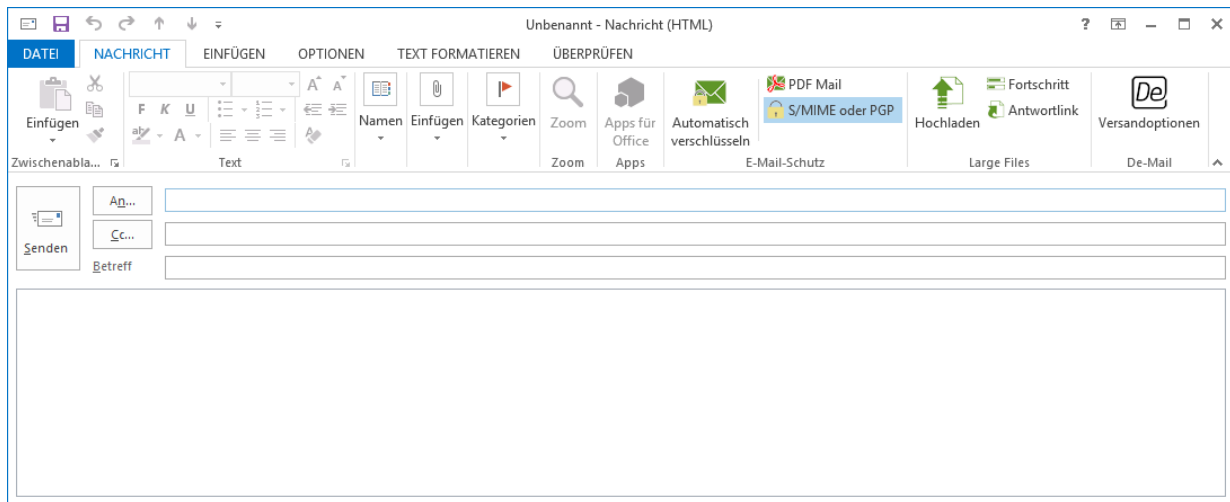
NOTE: If you install the Outlook Add-in via MSI file, this file must be located on a local hard disk. Installation via a UNC path is not possible.

I Functions of the Outlook Add-In when composing emails

- **Automatic Encryption**| Enables the delivery of encrypted emails to recipients who do not have cryptographic keys in their possession. NoSpamProxy Encryption automatically selects the appropriate delivery method and delivers the email securely.
- **PDF Mail**| Converts the email content with all attachments into a PDF document and secures this document with a password. This allows you to securely deliver emails with all attachments even to recipients without cryptographic keys.
- **S/MIME or PGP**| Allows the signature and encryption of emails using cryptographic keys such as PGP key pairs or S/MIME certificates.
- **Large Files**| Transfers large files via the NoSpamProxy Web Portal. Instead of the file, a link is attached to the email, with the help of which the recipient(s) of the email can download the files secured by SSL. The link can be protected

by a password.

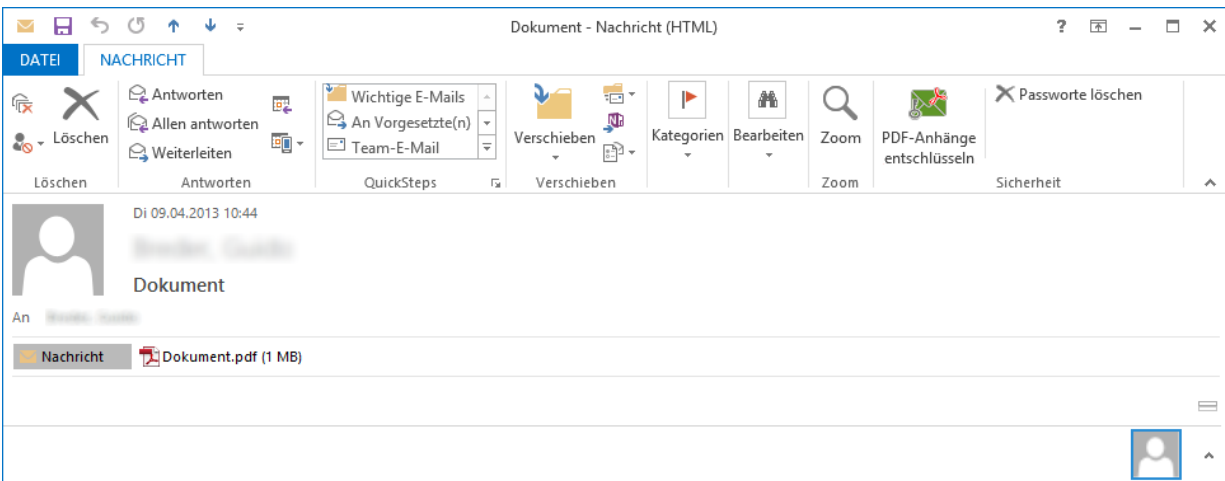
- **De-Mail**| Displays all the delivery options available to you for De-Mail delivery.



NOTE: You will find the above-mentioned functions in the menu ribbon of a new message in the three areas **Email protection**, **De-Mail** and **Large Files**.

Functions of the Outlook Add-In when reading emails

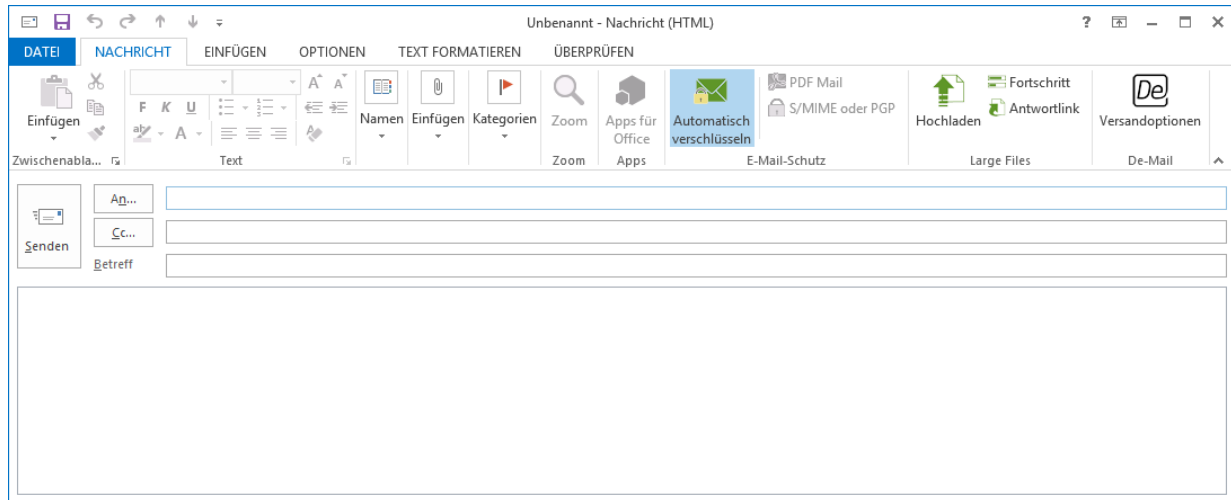
- **Decrypting PDF attachments**| Decrypts password-protected PDF attachments and removes passwords.
- **Deleting passwords**| Deletes previously saved PDF decryption passwords.



NOTE: The PDF decryption functions become active when you select or open an e-mail with one or more PDF attachments.

Encrypt automatically

The Automatic Encryption function is the easiest way to transmit an email securely



- If you select Automatic Encryption, an email signature and encryption by cryptographic keys is requested for this email.
- If encryption via certificates or PGP keys is not possible, the email is secured by PDF Mail. For PDF Mail a password is automatically generated and delivered to the sender of the email. The entire email content and all attachments are embedded in a protected PDF document. This means that an email can be delivered safely and securely without your communication partner having to have cryptographic keys.

PDF Mail


To open the PDF Mail dialog, proceed as follows:

1. Click **New email** in the Microsoft Outlook ribbon.
2. Go to **Message > Email protection**.
3. Click **PDF Mail**.

Action

- **Disable PDF Mail**| PDF Mail is not used for the current message.
- **Convert email to PDF and protect with password**| Converts the email with all attachments to a PDF.
- **Protect attached PDF file with a password**| Protects attached PDF files with a password.

PDF Mail

 PDF Mail


Aktion

- ☒ PDF Mail abschalten
- ☐ E-Mail zu PDF konvertieren und mit Passwort schützen
- ☐ Angehängte PDF-Dateien mit Passwort schützen

Passwort

- ☒ Den Server das Passwort bestimmen lassen
- ☐ Passwort von Hand setzen

Benachrichtigung

- ☐ Passwort versenden an Empfänger auswählen 

Nummer

- ☐ Ich möchte darüber informiert werden, wie die E-Mail verschlüsselt wurde.

Speichern und schließen

Abbrechen und schließen

Password

- **Let the server define the password**| NoSpamProxy Encryption automatically generates a password.
- **Set password manually**| Lets you create a password yourself.



NOTE: The password is sent to the sender or recipient depending on the settings under Notification.



NOTE:

For a password to be valid, it must have at least two of the following properties:

- It consists of at least eight characters.
- It contains a lowercase letter.
- It contains an uppercase letter.
- It contains a number.
- It contains a special character.

Notification

- **Send password to**| The password is sent to the recipient via text message. To do this, enter the number of the recipient into the input field.



NOTE: If recipients were already entered in the "To" field of the email when the dialog was opened, the contact details of the first recipient are entered automatically. After selecting a text message recipient, check the phone number or alternatively enter the phone number for text message reception directly into the selection list.

- **I want to get an information on how the email was encrypted** | A text message with the password will be sent to the sender.

The following combinations are possible:

Send password to	Inform about encryption	Behaviour of NoSpamProxy
No	No	A message with the password is sent to the sender so that the sender can process an automatically created password.
No	Yes	A message with the password is sent to the sender.
Yes	No	An SMS with the password is sent to the recipient.
Yes	Yes	An SMS with the password is sent to the recipient and a message with the password is sent to the sender.

**NOTE:**

Use the following examples for the phone number formatting so that the text message phone number can be processed correctly:

+49 (area code without 0) Number

e.g.: +49 (1234) 567890

e.g.: +49 1234 567890

0049 (area code without 0) Number

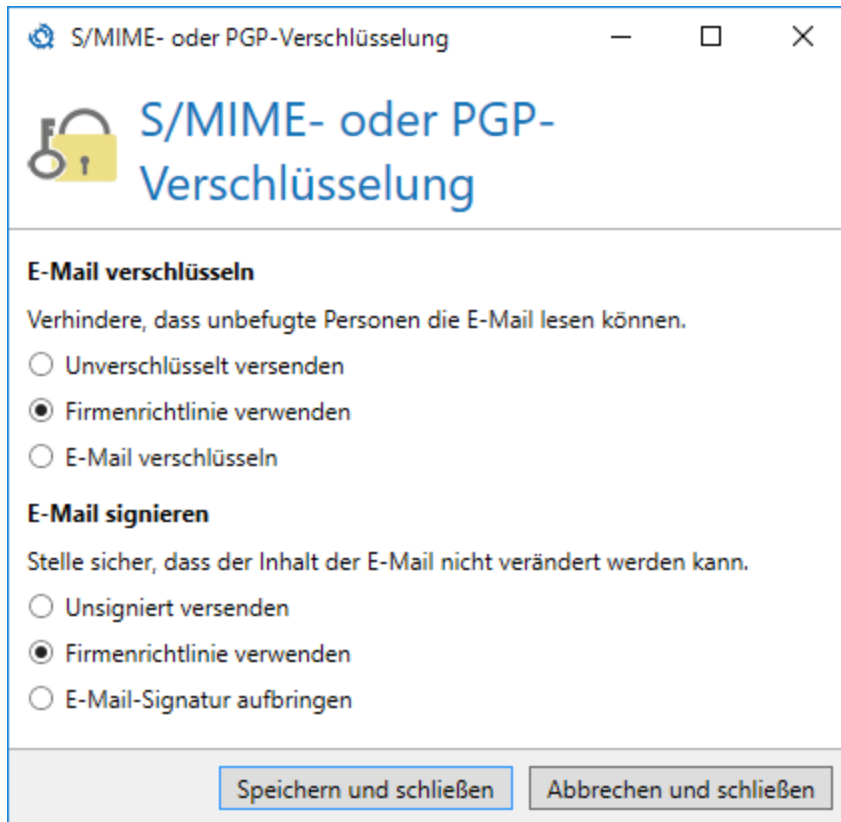
e.g.: 0049 (1234) 567890

e.g.: 0049 1234 567890

Area code with 0 number

e.g.: 01234 567890

S/MIME or PGP



I Encrypting emails

Send unencrypted | The current email is not encrypted.

Use company policy | The company policy is applied to the current email.

Encrypt email | The current email is encrypted.

Signing emails

Send unsigned| The current email is not signed.

Use company policy| The company policy is applied to the current email.

Apply signature| The current email is signed.



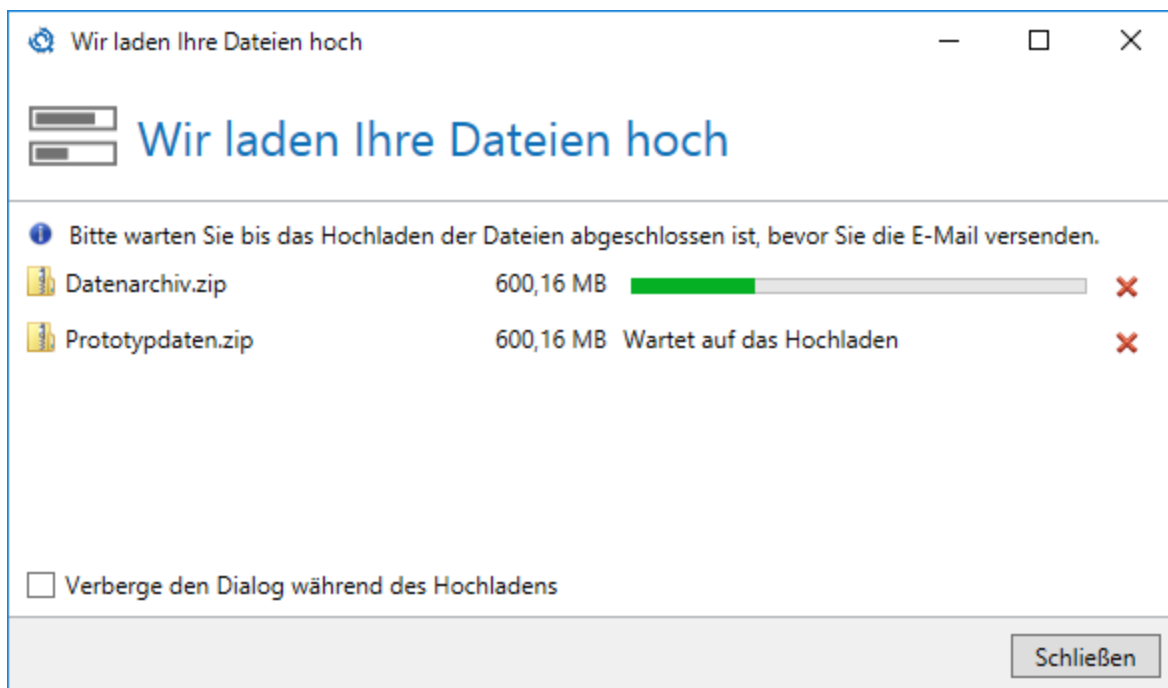
NOTE: If a behaviour is set in this dialog that is not permitted in the configuration of NoSpamProxy Encryption, the email will not be delivered.

Large Files

Sending large files

1. Click **New email** in the Microsoft Outlook ribbon.
2. Go to **Message > Large Files**.
3. Click **Upload**.
4. Select the files you want to upload.
5. Send the email.

Once the transfer is complete, a link is attached to the email for each selected file. With this link the recipient can download the file to his computer.





NOTE: To check the progress of the upload, click **Progress**. Here you will also see any problems that may occur when uploading files. Via the red **X** you can cancel the upload of a file or remove files that have not yet been uploaded.



NOTE: The Outlook Add-in automatically supports the user based on the sender email address whether and how the file is transmitted. This is done through content filters specified by the administrator. This allows the add-in to immediately inform the user about, for example, locked file types or files that are too large. The content filter enables the add-in to comply with the company's specifications for permitted files when using the Outlook function Attach File and to automatically carry out the transfer through large files.

I Differences between **Attach file** and the Large Files **Upload** function

You can also attach files as usual via **Attach file** or drag and drop to the email. Depending on the settings that you can change via **Options**, the file is either attached directly to the email or transferred via the Web Portal.

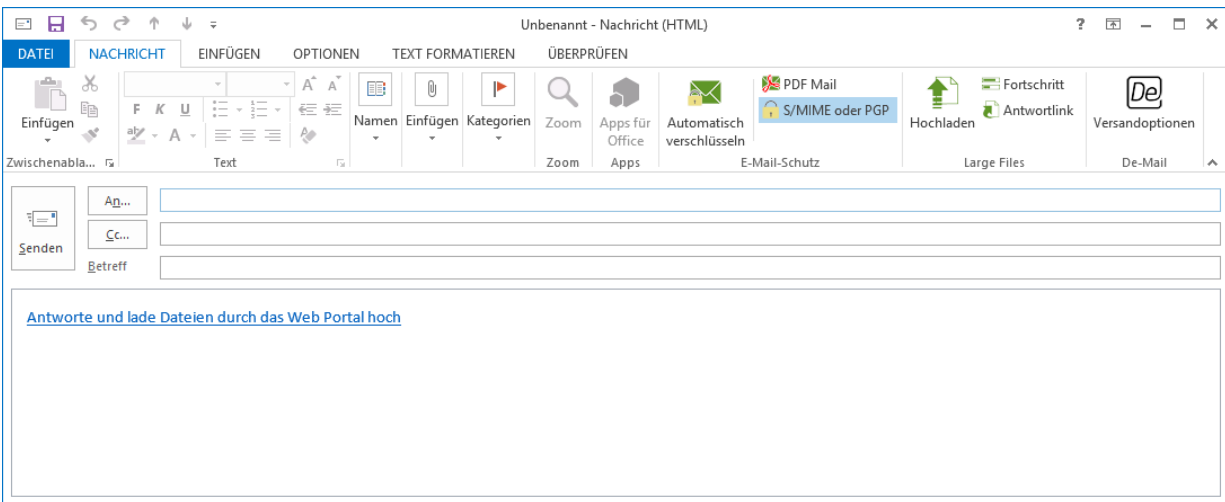
Depending on the settings for your email server, you can attach files up to a maximum of 20MB to the email using **Attach file**. In the default settings of Large Files, an HTML file that refers to the Web Portal is attached instead of the original file if the file size exceeds 2MB. The email recipient can use this HTML file to download the original file from Web Portal.

By **uploading** to Large Files, files are never attached directly to the email, but the Web Portal is always used. The **Upload** option is not limited to a fixed size but is specified by the administrator of NoSpamProxy. This allows - if allowed by the administrator - the upload of files with sizes up to several gigabytes.

Inserting a response link

- Click **Response link** to include a link for the recipient in the email.

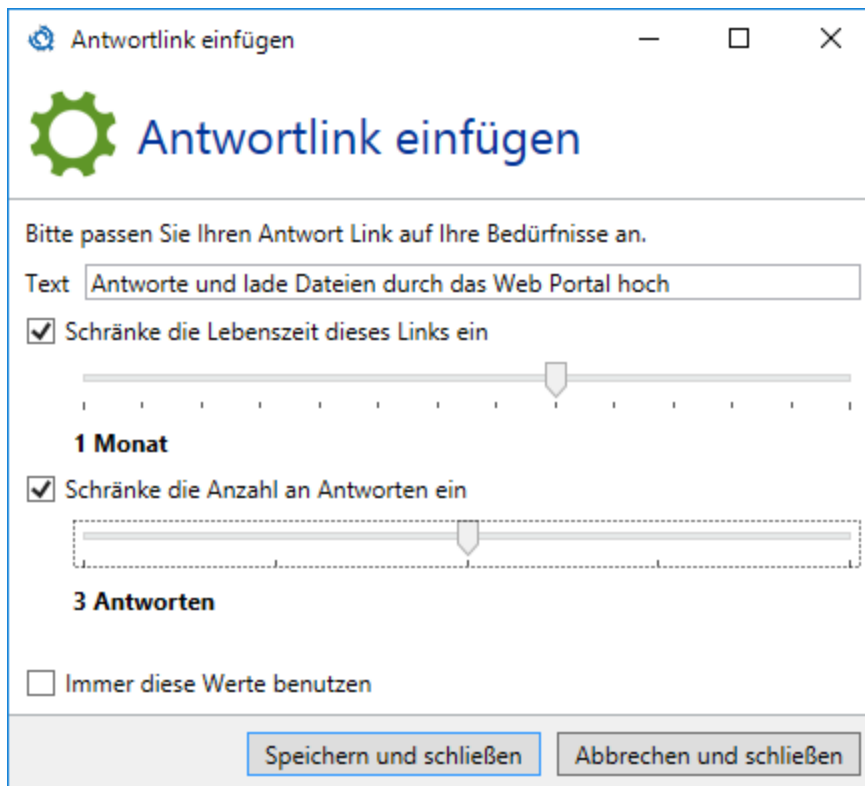
Using this link, the recipient(s) can reply to you via the Web Portal and transfer large files to you.



Specify the following information:

- Text for the link
- Lifetime of the link.
- Number of possible responses

With the button Always use these settings you can specify whether the currently set values are also used for future links by default in this dialog.



The screenshot shows a Windows-style dialog box titled "Antwortlink einfügen" (Insert Answer Link). It features a green gear icon and the title in blue text. Below the title, it says "Bitte passen Sie Ihren Antwort Link auf Ihre Bedürfnisse an." (Please adapt your answer link to your needs). There are three main settings:

- Text:** A text box containing "Antworte und lade Dateien durch das Web Portal hoch".
- Lifetime:** A checked checkbox "Schränke die Lebenszeit dieses Links ein" (Limit the lifetime of this link). Below it is a slider set to "1 Monat" (1 month).
- Number of responses:** A checked checkbox "Schränke die Anzahl an Antworten ein" (Limit the number of answers). Below it is a slider set to "3 Antworten" (3 answers).

At the bottom, there is an unchecked checkbox "Immer diese Werte benutzen" (Always use these values). Two buttons are at the bottom right: "Speichern und schließen" (Save and close) and "Abbrechen und schließen" (Cancel and close).

I Protecting Large Files links with a password

You can password-protect large file links by configuring password protection either by using a corresponding content filtering action in NoSpamProxy or by manually enabling it during composing. The password requested for downloading is always the password stored in the individual user entries for partners.

Default settings in NoSpamProxy

To enable password protection of Large Files links, you must make the following settings via the NoSpamProxy Command Center:

- Under Configuration > Rules in an outbound email rule, make sure that you have selected Enabled on the General tab under Content filtering. Please refer to the Rules chapter in the NoSpamProxy user manual.
- Under Configuration/Content filter/Actions of the content filter, on the Attachments tab, decide whether you want to require password protection for all emails to be sent or let the respective user decide. Please refer to the chapter Actions of the content filter in the NoSpamProxy user manual.
- Make sure that you have created a content filter entry under Configuration/Content filter/Content filter for a content filter that triggers the desired action for untrusted or outgoing emails. Please refer to the Content Filter chapter in the NoSpamProxy user manual.
- Make sure that the appropriate outbound policy (content filter) is configured for business users. You can set this as a default setting, at user level or for

individual email addresses. Please refer to the Corporate Users chapter in the NoSpamProxy User Guide.

- Make sure that the appropriate outbound policy (content filter) is configured for partners. You can make this setting as a default, at domain level or at user level. Please refer to the Partner chapter in the NoSpamProxy user manual.

Enabling password protection

1. Click **New email** in the Microsoft Outlook ribbon.
2. Go to **Message > Large Files**.
3. Click **Protect all files**.



The password protection for large file links is then activated for the respective email. The password requested is the password stored in a partner for the respective user. See **Partner**.

4. Send the email.



NOTE: If **Protect all files** is not selectable, the password protection has already been set by your administrator in the action of the content filter.

De-Mail

Click **Dispatch options** to configure the dispatch options and confirmations for De-Mail.

De-Mail Optionen

Bestätigung

- ☐ **Versandbestätigung (Einschreiben)**
Bei Wahl dieser Option wird eine Versandbestätigung vom Versanddienst des Absenders erzeugt und dem Absender zugestellt.
- ☐ **Eingangsbestätigung (Einschreiben Einwurf)**
Bei Wahl dieser Option wird eine Zugangsbestätigung vom Postfachdienst des Empfängers erzeugt und dem Absender sowie dem Empfänger der ursprünglichen Nachricht zugestellt.
- ☐ **Abholbestätigung**
Bei Wahl dieser Option erstellt der Postfachdienst des Empfängers einen Nachweis darüber, wann sich der Empfänger nach dem Eingang der Nachricht mit Authentisierungsniveau 'hoch' an seinem Konto angemeldet hat. Diese Abholbestätigung wird sowohl dem Absender wie auch dem Empfänger zugestellt.

Versandart

- ☐ **Absenderbestätigt**
Der Postfachdienst des Absenders bestätigt nach Entgegennahme der Nachricht, dass er die Nachricht tatsächlich von dem Absender entgegengenommen hat und dieser sich mindestens mit dem Authentisierungsniveau 'hoch' angemeldet hat.
- ☐ **Persönlich (Einschreiben Eigenhändig)**
Die Wahl dieser Option bedeutet, dass das erforderliche Anmeldeniveau des Empfängers mindestens 'hoch' sein muss, um die Nachricht lesen zu können. Um diese Option wählen zu können, muss auch das Anmeldeniveau des Absenders 'hoch' sein.

Save and close **Cancel and close**

- **Confirmation**| Specify whether you receive notifications about the sending, receipt and collection of the message.
- **Dispatch type**| Specify how the De-Mail message is to be transmitted.

Decrypting PDF attachments

When archiving password-protected PDF documents, it is necessary to archive the password as well. Otherwise, these documents cannot be opened later. Losing your passwords means that you will not be able to access the PDF documents afterwards. This is where the Outlook Add-in helps you by removing the now no longer needed password protection from PDF documents. The function becomes active for an email with PDF attachments.

Proceed as follows:

1. Go to **Start > Security**.
2. Click **Decrypt PDF attachments**.



NOTE: The Outlook Add-in first checks whether you need a password to open the PDF attachments. Then it tries to decrypt the password-protected attachments with the already saved passwords. For attachments that cannot be decrypted with the stored passwords, you will be asked for the password. If you do not know the password, you can skip the decryption for this attachment with **Do not decrypt this PDF**.

3. Enter the password.
4. (Optional) Click **Save password for later use** to add the entered password to the list of saved passwords if decryption is successful
5. Click **Try this password**.

Documents for which decryption failed are displayed along with their file name and the reason for the failed decryption. PDF files that are not password protected - and therefore do not need to be decrypted - are not included in this list.

A report is attached to the email for successfully decrypted documents. The file name used is **PDF decryption report.txt**.

EXAMPLE: The following attachments were decoded on 15.06.2016
13:48:46: Invoice.pdf Contract.pdf

Hideable areas

Some areas of the Outlook Add-in are configurable. If add-in functions are not available in your company, the corresponding areas can be hidden. This allows the functional scope of the Add-In to be optimally adapted to your company's needs.

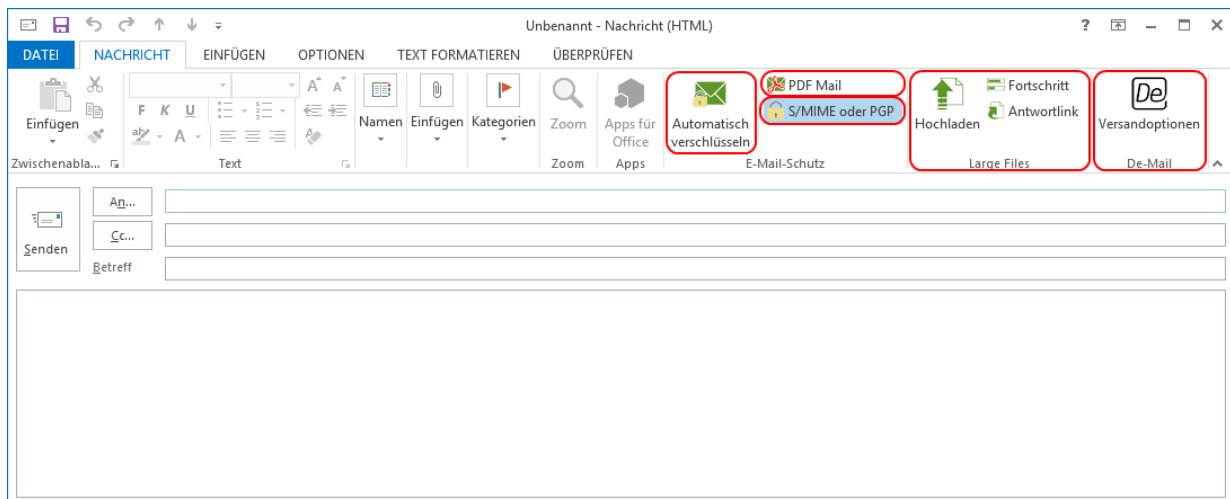


TIP: Details on how to show and hide areas can be found under .

The configurable ranges are listed below.

Writing emails

All functions in the menu ribbon can be shown and hidden.



- The function for **De-Mail** is hidden by default.
- The **Large Files** area is only displayed if a URL has been configured for the connection to the Web Portal.
- The **Options** button is hidden if the options have already been set by an administrator using Group Policy.
- In the PDF Mail dialog the **automatic assignment of passwords** and the **dispatch of text messages** can be hidden.

PDF Mail

Aktion

- ☒ PDF Mail abschalten
- ☐ E-Mail zu PDF konvertieren und mit Passwort schützen
- ☐ Angehängte PDF-Dateien mit Passwort schützen

Passwort

- ☒ Den Server das Passwort bestimmen lassen
- ☐ Passwort von Hand setzen

Benachrichtigung

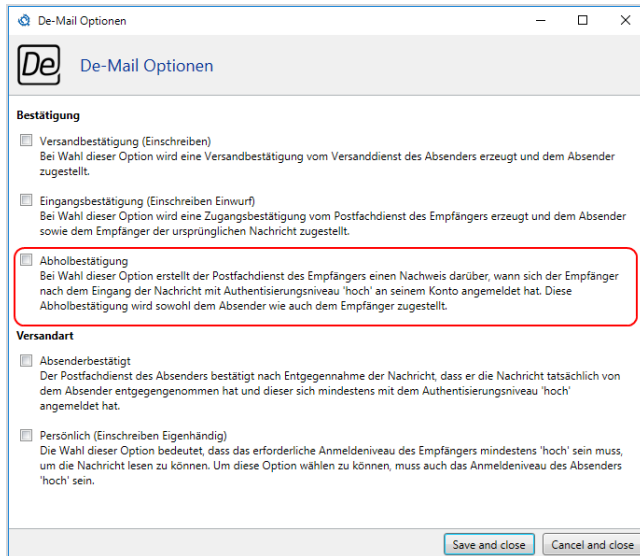
- ☐ Passwort versenden an Empfänger auswählen

Nummer

☐ Ich möchte darüber informiert werden, wie die E-Mail verschlüsselt wurde.

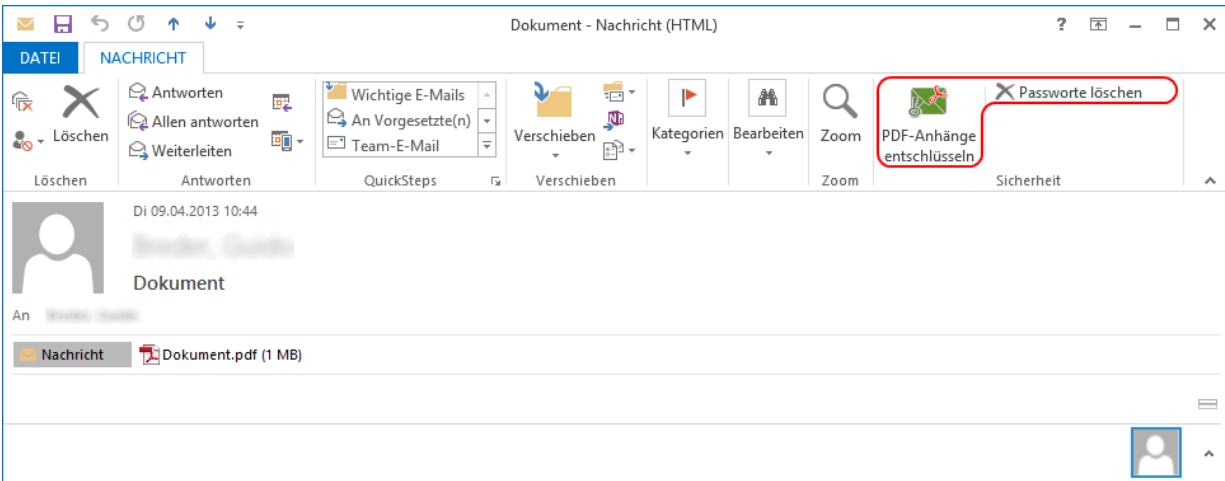
Speichern und schließen Abbrechen und schließen

- The option **Confirmation of retrieve in the De-Mail dialog** is not available to most users of the De-Mail portal. It is hidden by default.



I Reading emails

The area for decrypting PDF attachments and deleting the passwords stored by them as well as generating a password reset email can be shown and hidden in the menu ribbon.



Help and support

Knowledge Base

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

Website

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

NoSpamProxy Forum

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

Blog

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

YouTube

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

NoSpamProxy Support

You can reach our support team

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

