



Outlook Add-in

Installation und Gruppenrichtlinien

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

Installing the Outlook Add-in	1
Manageable options in the Outlook Add-In	2
Composing emails	2
Reading emails	6
Subject flags when sending emails	6
Distributing settings via group policy	8
Help and support	14

Installing the Outlook Add-in

There are two ways to install the add-in:

- **Setup file**| The setup automatically installs all required components. This includes the required Microsoft .NET Framework 4.8, the Microsoft Visual Studio 2010 Tools for Office Runtime, and the actual add-in, and Setup guides you through all the necessary steps and ensures that all prerequisites for a successful installation are met.
- **MSI file**| The MSI file is required when using automatic software distribution. First the Microsoft .NET Framework 4.8, then the Microsoft Visual Studio 2010 Tools for Office Runtime and finally the MSI file with the actual add-in must be installed. The actual installation depends on the software distribution used.



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



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

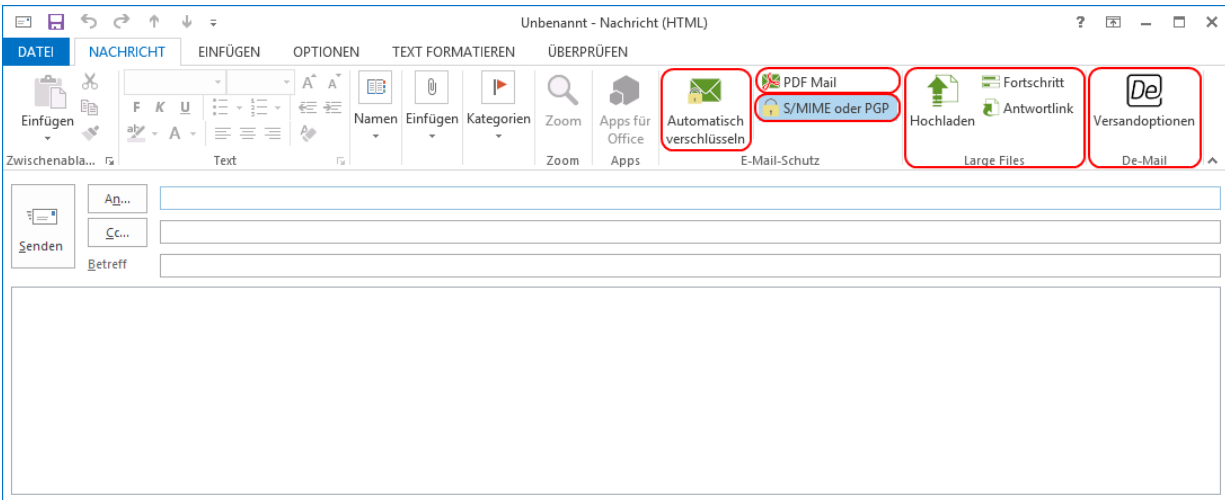
Manageable options in the Outlook Add-In

The availability of the individual functions is controlled via entries in group policies. This allows the add-in to be controlled in such a way that only those functions are available that should actually be available to the end user group.

I Composing emails

These functions can be displayed in the menu bar for a new email after installation. The following options can be individually shown and hidden when composing emails.

- Automatic encryption
- PDF Mail
- S/MIME or PGP
- Large Files
- De-Mail




NOTE: In addition to the hideable areas in the menu ribbon, the text of the response link can also be adjusted.

Manageable options in PDF Mail

- **Automatic password creation**| In the PDF Mail dialog you can hide the option for automatic password creation. In this case the manual input of the password is still available.
- **Text message notification**| This area can be hidden if this option is not available and the password is to be sent to the recipient via another route.

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

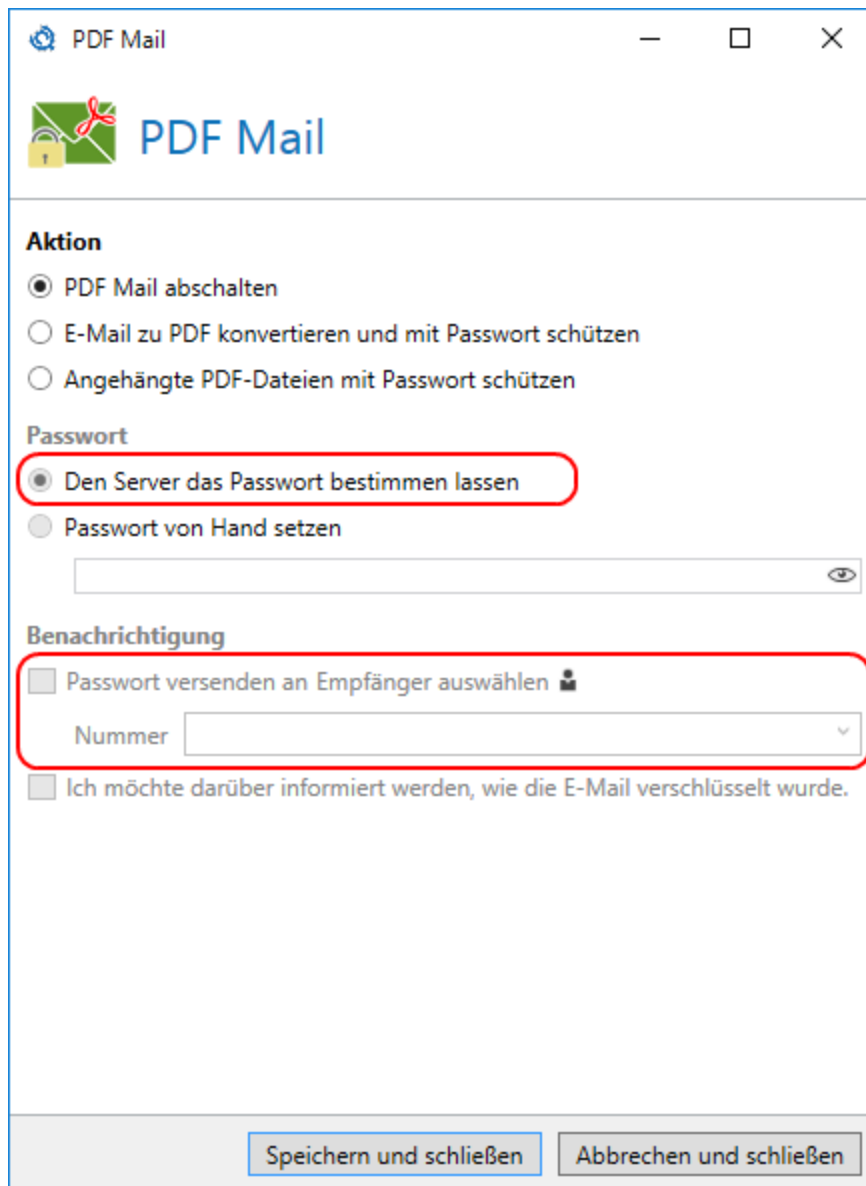
Abbrechen und schließen

Manageable options in Large Files

The entire Large Files area is only displayed if the Web Portal URL policy is configured with a valid URL.

Manageable options in De-Mail

- **Collection confirmation** | This option is only available in De-Mail for certain participants. Offices can use it, it is not intended for private individuals.



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

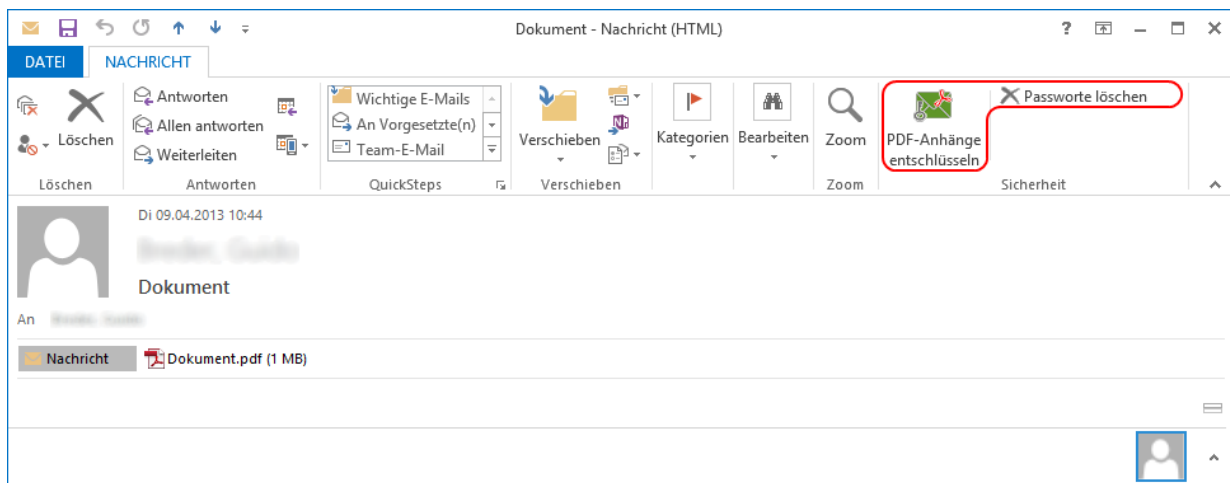
Benachrichtigung

- ☐ Passwort versenden an Empfänger auswählen 
- Nummer
- ☐ Ich möchte darüber informiert werden, wie die E-Mail verschlüsselt wurde.

Reading emails

These functions are displayed in the read view menu of an email after installation.

- Decrypting PDF attachments
- Deleting passwords



Subject flags when sending emails

You can configure the add-in to add the corresponding subject line labels in addition to the email headers when the email is sent, **Betreffkennzeichnungen**. This function is switched off by default. It is used to control NoSpamProxy Encryption via the Outlook Add-in, even if all header information is deleted from the email on the way to NoSpamProxy.



NOTE: To use this function, the subject line flags must match the default values specified in NoSpamProxy. If you have changed subject flags in NoSpamProxy, you must reset them to the default value.

Distributing settings via group policy

The functions of the Outlook Add-in are controlled by group policies. You can distribute group policy across your domain or set it locally in small installations and for testing purposes.

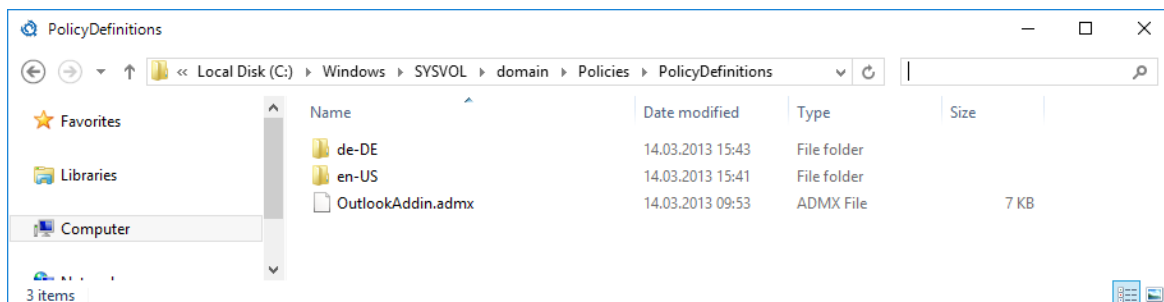
Step 1: Deploying ADMX file and voice files on the server

1. Go to the [download area of the NoSpamProxy website](#) .
2. Download the [Outlook Add-In - Package for Group Policies \(GPOs\)](#).
3. Unzip the downloaded file.
4. Copy the unzipped files to the
%windir%\SYSVOL\domain\Policies\PolicyDefinitions folder on the domain controller.



NOTE: If the directory does not exist, you must create it.

5. Copy the language files as ADML files into the respective folders with the corresponding language designation, for example de-DE for German or en-US for English.





NOTE: For a local installation of group policy without a domain, you must place the files in the `%windir%\PolicyDefinitions` directory.

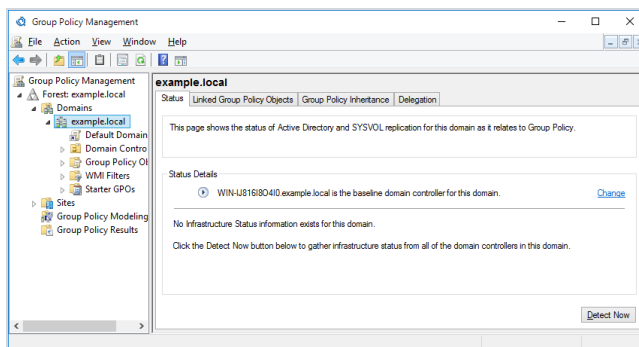
Step 2: Creating a new group policy in the Group Policy Manager



NOTE: If you are performing an on-premises installation of group policy without a domain, skip this step.

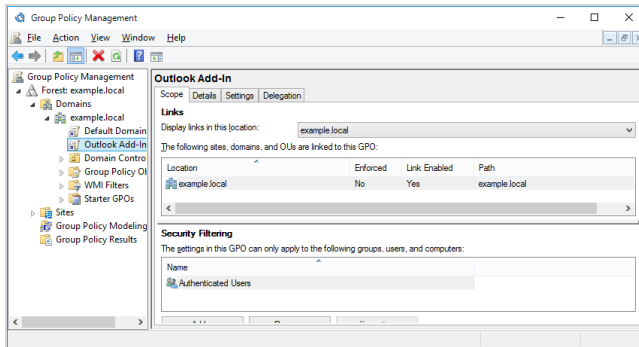
1. Open the Group Policy Management Console.
2. Right-click the corresponding domain and in the context menu, click **Create a GPO in this domain and link it here.**

The new object appears below the domain.



3. Adjust the security filtering.

4. Specify the organisational unit or users for whom the Outlook Add-in is to be installed.



Step 3: Editing group policies

1. Right-click the group policy object and click **Edit.../Edit...** in the context menu.

The Group Policy Object Editor appears.

2. Go to **User Configuration > Policies > Administrative Templates > Net at Work NoSpamProxy > Outlook Add-In**.



NOTE: For a local installation of group policies without a domain, start the local group policy object editor with the command `gpedit.msc`. Go to **User Configuration > Administrative Templates > Net at Work > NoSpamProxy > Outlook Add-In**.

Configurable settings of the Outlook Add-In

Policy name	Description	Not configured
Show 'Decrypt PDF attachments'	Displays the 'Decrypt PDF attachments' button on the menu ribbon if enabled. Hides the button when it is disabled.	The button is displayed if the policy is not configured.
Show 'Automatic Encryption'	Displays the 'Automatically encrypt' button in the menu ribbon of a new email when the policy is enabled. Hides the button when it is disabled.	The button is displayed if the policy is not configured.
Show 'PDF Mail'	Displays the 'PDF Mail' button in the menu ribbon of a new email when the policy is enabled. Hides the button when it is disabled.	The button is displayed if the policy is not configured.
Show PDF Password Generator option	Displays the PDF Password Generator option in the 'PDF Mail' dialog if the policy is enabled. Hides the option when it is disabled.	This option is displayed if the policy is not configured.
Show Text message for PDF password option	Displays the Text message for PDF password option in the 'PDF Mail' dialog if the policy is enabled. Hides the option when it is disabled.	The option appears if the policy is not configured
Show 'Email encryption'	Displays the 'Email encryption' button in the menu ribbon of a new email if the policy is enabled. Hides the button when it is disabled.	The button is displayed if the policy is not configured.

Policy name	Description	Not configured
Show 'De-Mail'	Displays the 'De-Mail' button in the menu ribbon of a new email when the policy is enabled. Hides the button when it is disabled.	The button is hidden if the policy is not configured.
Show 'Confirmation of retrieval'	Displays the 'Confirmation of retrieval' option in the De-Mail dialog if the policy is enabled. Hides the option when it is disabled.	The option is hidden if the policy is not configured.
Web Portal URL	Defines the Web Portal URL, for example: 'https:// portal.example.com/enqsig'. The 'Large Files' section in the menu ribbon of a new email is displayed if this policy is enabled and configured with a valid URL.	The area is hidden if the policy is not configured or if the URL is in an invalid format.
Large Files reply limit	Defines a limit for the maximum number of replies to this message. Values from 1 to 10 and the value "unlimited" are available.	If the policy is not configured, these settings can be set by the user.
Expiration of Large Files replies	If the policy is configured, the administrator defines an expiration date for Large File response links. You can choose between different time periods and the value "never".	If the policy is not configured, these settings can be set by the user.

Policy name	Description	Not configured
Write subject flags	Subject flags are written in addition to email headers if enabled. Email headers are written without subject flags if it is disabled.	Email headers are written without subject labels if the policy is not configured.
response link Text	Defines an alternative text for the Large Files response link.	If the alternative text has not been entered, the default text is displayed.
Shared Web Portal password	Defines a password shared between Web Portal and NoSpamProxy Outlook Add-Ins. This must be entered in the NoSpamProxy Command Center in the settings of the Web Portal and Outlook Add-In of NoSpamProxy to ensure that the Large Files can upload files.	The Large Files area is hidden if no password is configured.
Show 'Protect all files	Displays the 'Protect all files' button in the menu ribbon if enabled. Hides the button when it is disabled.	The button is displayed if the policy is not configured.

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**.

