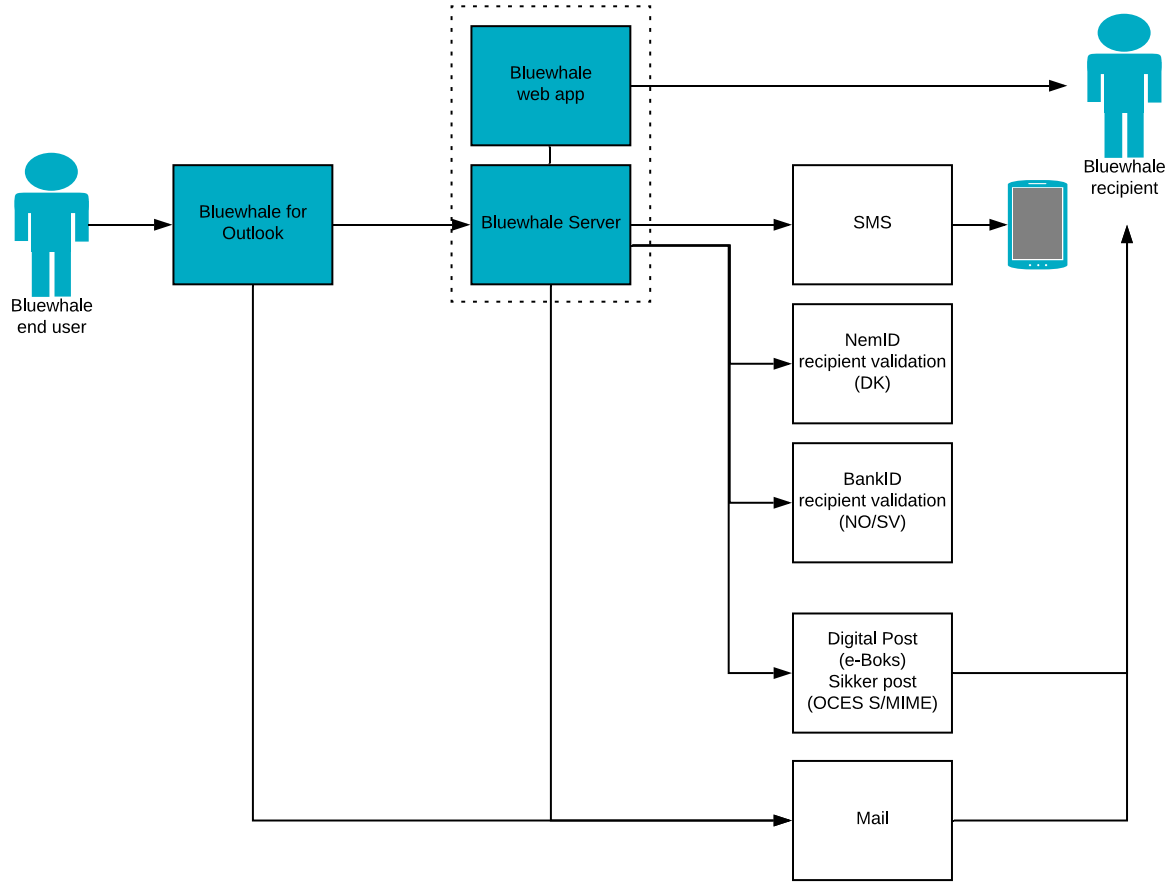
Bluewhale for Outlook 2.2.x User guide

Last updated 2020-06-22

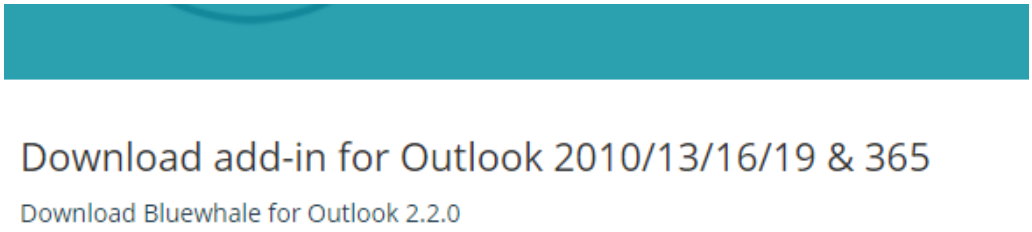
Introduction to Bluewhale for Outlook

Bluewhale makes it easy to exchange confidential messages and large files using e-mail with two factor authentication and file encryption.
With the Bluewhale for Outlook add-in most of Bluewhale's functionality is available directly from Microsoft Outlook 2010 and newer.
Bluewhale for Outlook is shipped as an MSI package and requires .Net 4.5 which is preinstalled with Windows 8 and newer.

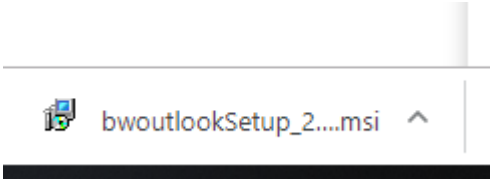


Download and installation

Visit the following address in your browser: https://bluewhale.dk/en/support-faq/download/ and click “Download Bluewhale for Outlook 2.x.x here” to start the download.

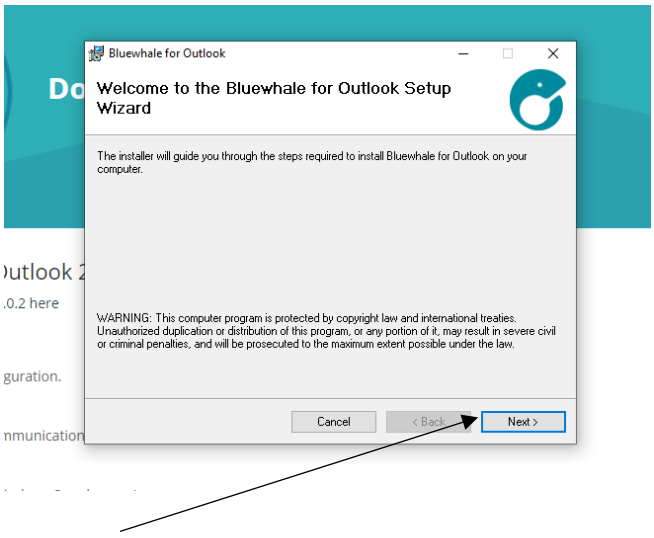


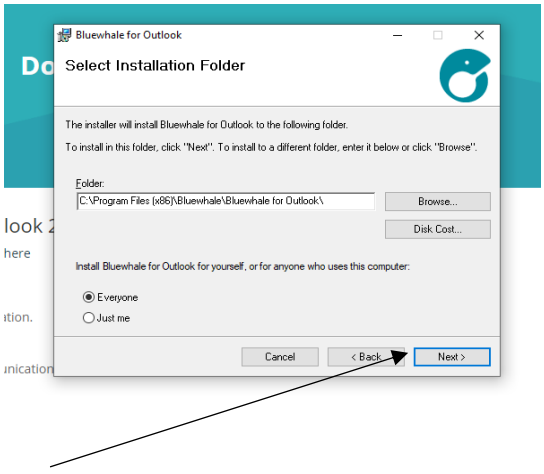
When the download is complete, you should see the installation file in the bottom left corner of the browser window.

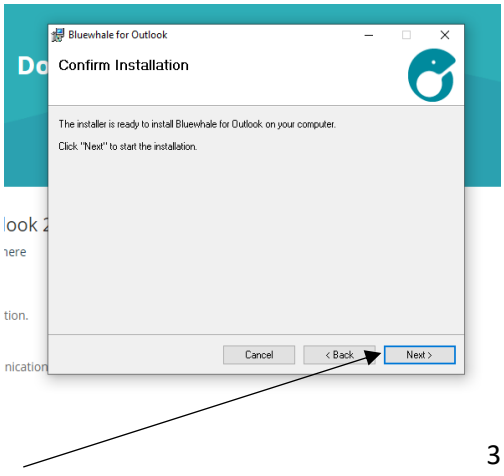


Your previous version of Bluewhale for Outlook will be replaced once installation of the latest version is complete, so it is not necessary to uninstall as this is done automatically.

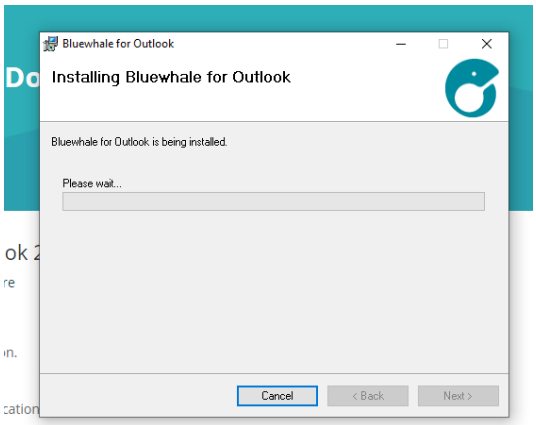
If Outlook is running, please close it and then click on the installation file to start the installation.

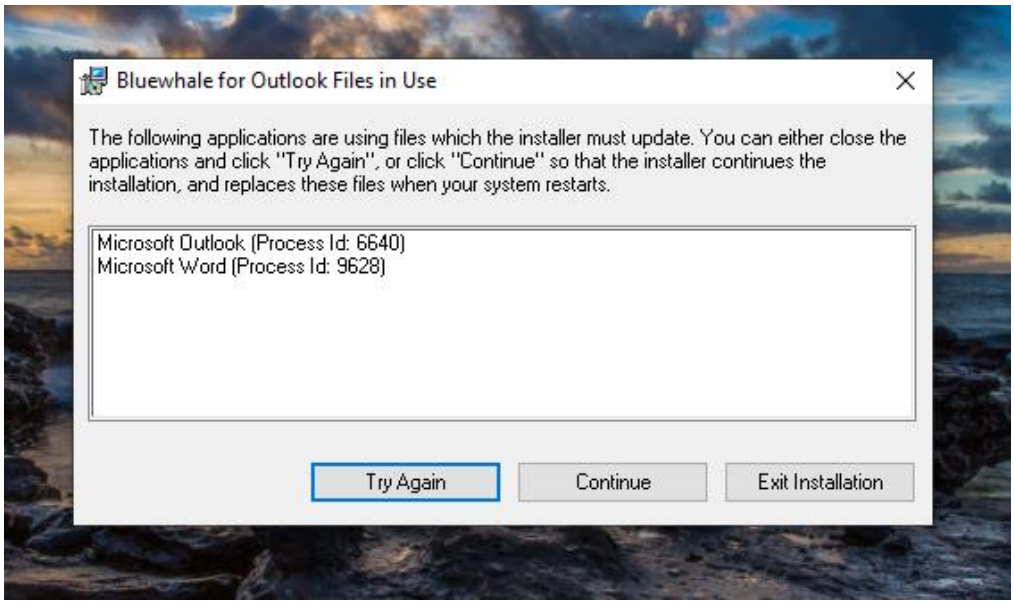






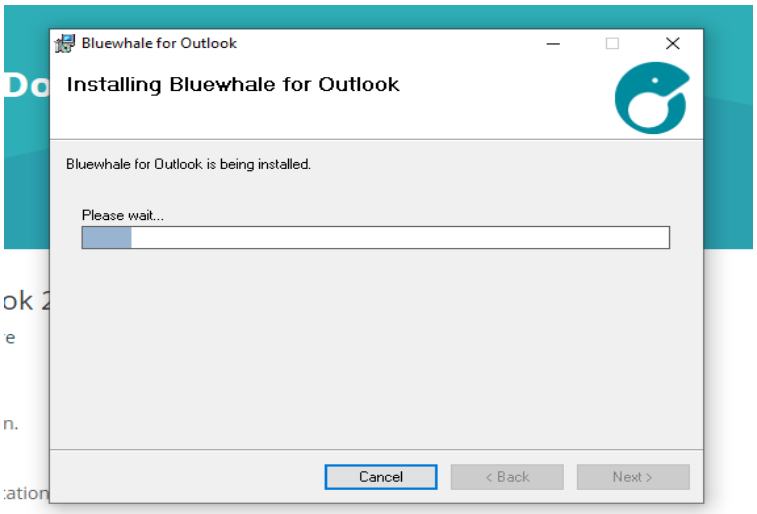
If Outlook is still running you will see the message below:



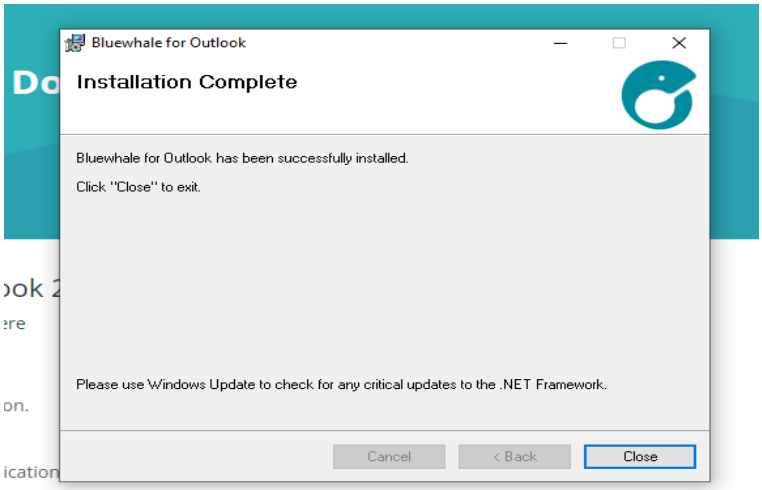


You can either close Outlook and click “Try Again” or click “Continue” and restart later.

Installation begins…

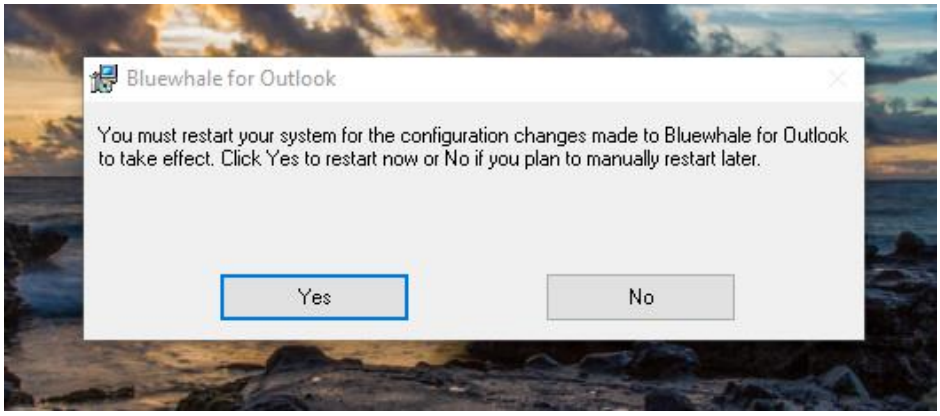


Installation is done. Click “close” to Complete.



If you did not close Outlook before installing, you need to restart to finish the installation.

Otherwise you can just start Outlook again.

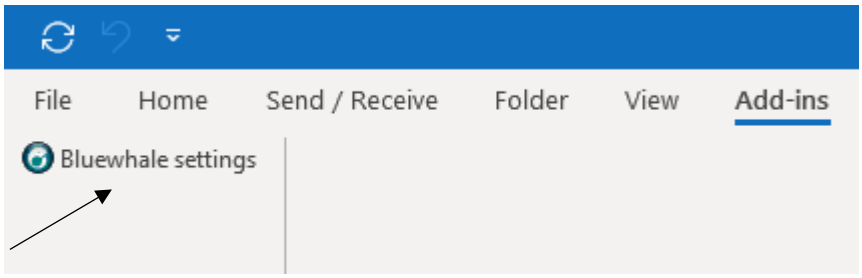


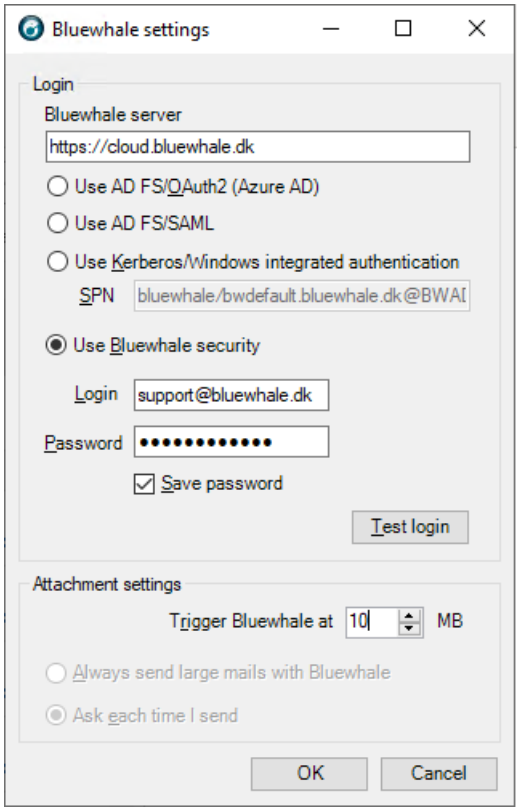
Settings

Before using Bluewhale you must enter the address of your Bluewhale-server and select authentication method.
If you're Bluewhale Cloud customer use following Bluewhale server: https://cloud.bluewhale.dk
Wolters Kluwer customers should use: https://wolterskluwer.bluewhale.dk
In both cases choose "Bluewhale Security" and enter your login and password in the provided fields.

If you're a Bluewhale Enterprise customer, please ask your IT-department for appropriate settings.

Click the **"Test login"**-button to verify your login settings.



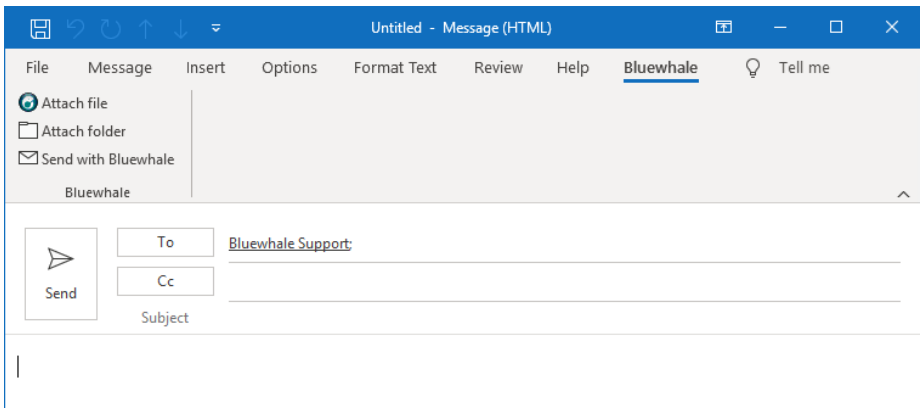


Upgrading from Bluewhale for Outlook 1.x

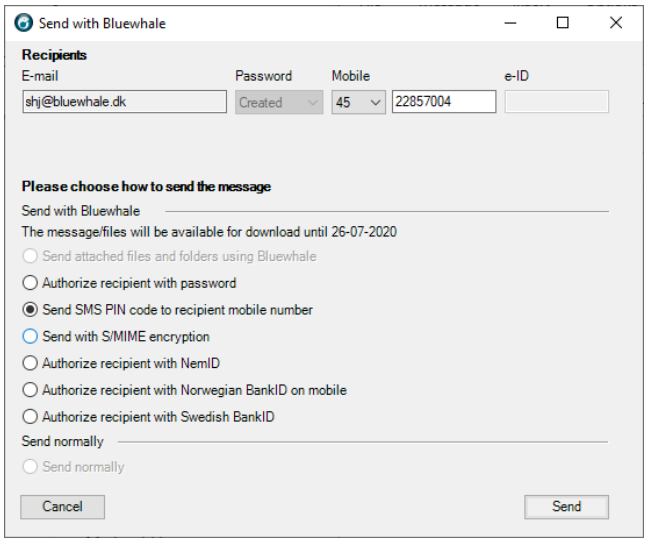
Personal settings from Bluewhale for Outlook 1.x are automatically detected and applied.

Usage

When Bluewhale for Outlook is installed, a “Bluewhale” tab is added to mail windows:



“Attach file” can be used to attach files, bypassing Outlook’s normal limitations on file sizes and types.
“Attach folder” can be used to attach a complete folder, including any subfolders, preserving the folder structure.
Bluewhale is activated by clicking the **“Send with Bluewhale”**-button:



You can now choose how to authorize the recipient. The choices are either password, SMS PIN code, S/MIME or your recipient’s e-ID (e.g. NemID for Denmark and BankID for Norway and Sweden).

- SMS PIN code and Norwegian BankID require that you enter the recipient’s mobile number.
- S/MIME requires a valid certificate for your recipient in the public certificate database (DK).
- NemID requires the recipient’s CPR- or CVR-number.
- Swedish BankID requires the recipient’s personal identity number (Swedish: personnummer).

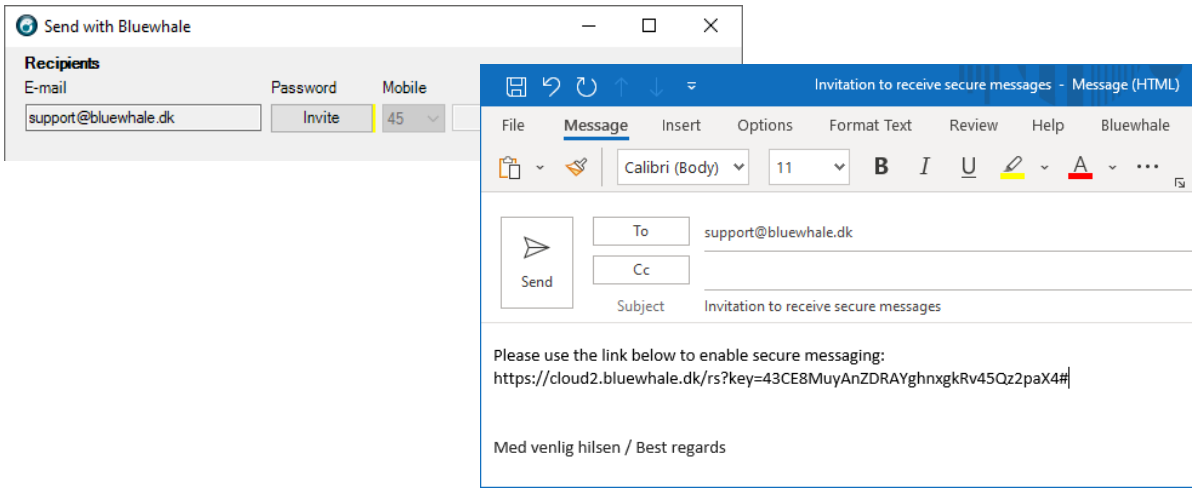
Click **“Send”** to send the message. The secure message is stored in your “Sent items”-folder in Outlook. The original message can be viewed in the “Sent with Bluewhale”-folder.

Password authorization

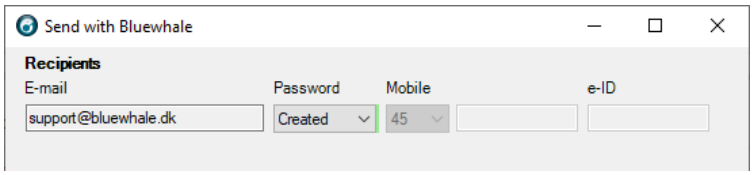
If SMS or e-ID authorization is not possible for a recipient, you can use password authorization.

For security reasons, messages carrying sensitive content must be sent after the recipient has created a password. This means that you need to mail new recipients twice: First to prompt them to create a password, second you can mail the actual sensitive content.

Click the **"Invite"**-button next to the new recipient to generate a password invitation mail. When you have sent the invitation mail, the recipient is guided to create a password.



You will receive a mail when the password is created and the password status for the recipient is updated from "Invite" (yellow) to "Created" (green).



The recipient can use the password to open **future** password validated messages.

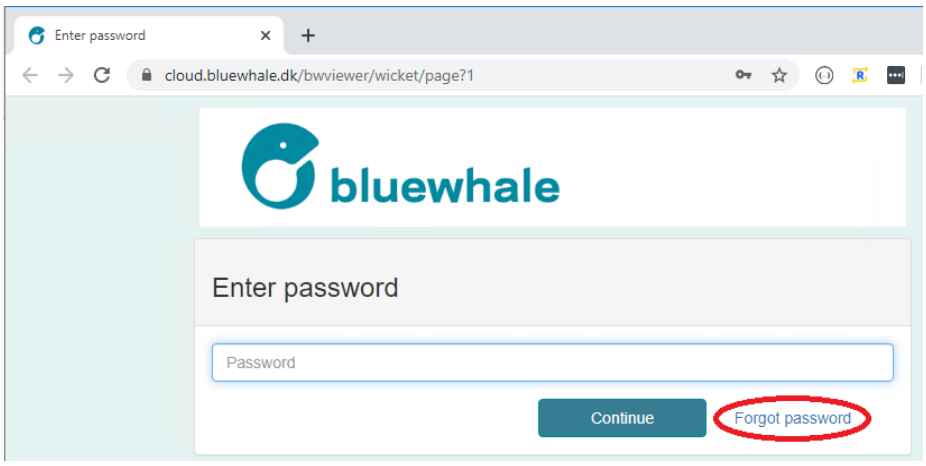
The recipients' password statuses are shared within your organization, so if a co-worker has already communicated with a recipient, you can send the sensitive content right away. This is indicated by the recipient's password status being "Created" or "Verified" (see below).

Verifying password recipients

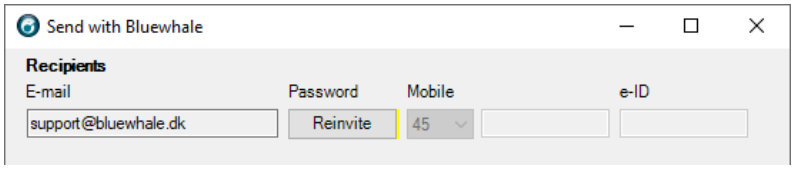
You can optionally add an extra layer of security by verifying the recipient. This is done by contacting the recipient (e.g. calling the recipient by phone) and verifying that the password indeed was created by the intended recipient. Register this by toggling the recipient's password status to "Verified".

Forgotten recipient password

If a recipient forgets her password, the recipient can request a password reset by clicking the **"Forgot password"**:



This will trigger a mail notification to you and cause the recipient's password status to change to "Reinvite":

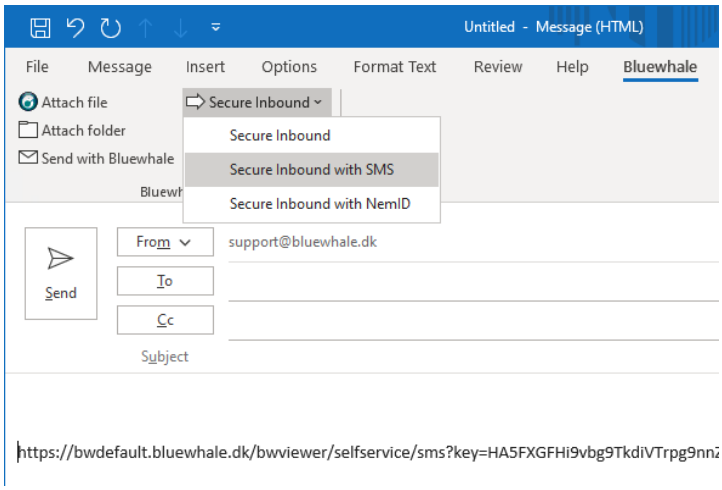


To allow the recipient to create a new password, simply click the **"Reinvite"**-button to generate a new invitation mail.

This mail is equivalent with the initial invitation mail and will allow the recipient to create a new password. When this happens, the recipient's status is updated to "Created".

Secure Inbound

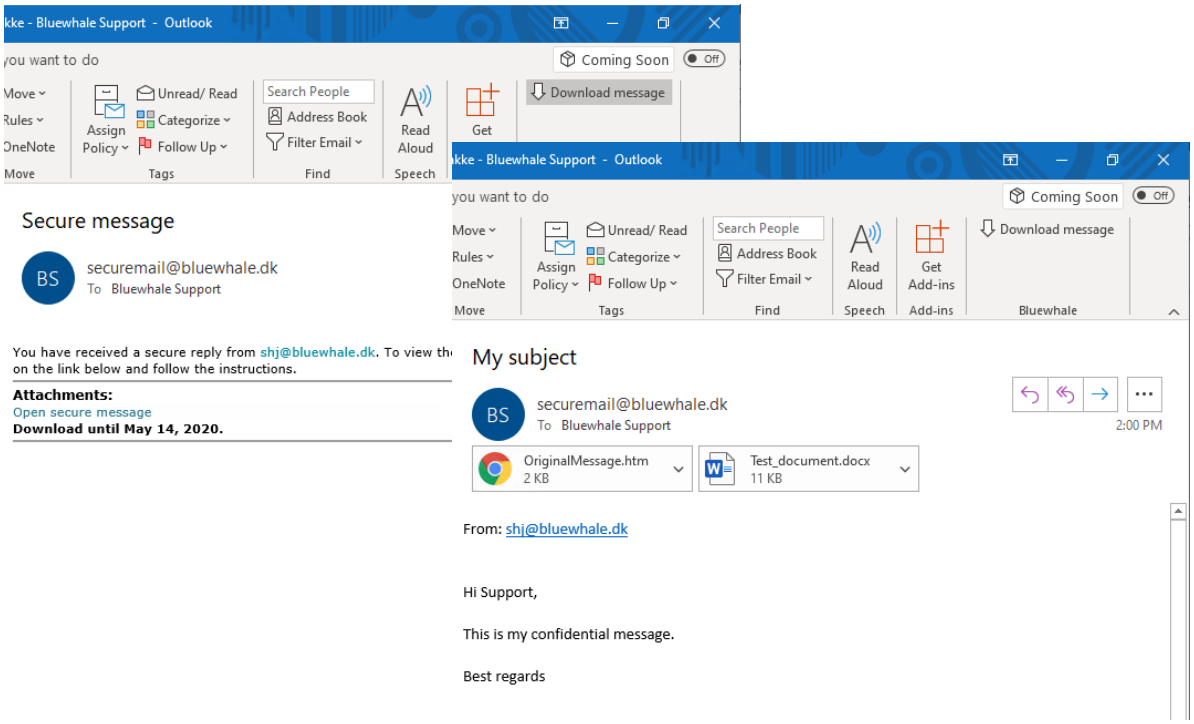
When a communication is initiated by you, recipients can use the reply-button to return a secure reply. However, to enable secure inbound communication initiated by an external party, you must first share a “Secure Inbound” link e.g. on your website.
If you are a Bluewhale Enterprise customer, you can generate a “Secure Inbound” link in Outlook. Click on the **“Secure Inbound”**-button on the Bluewhale-tab and select the required validation.



Bluewhale Cloud customers who wish to use “Secure Inbound” can add the module “Secure Inbound” by ordering a link, please contact sales@bluewhale.dk.

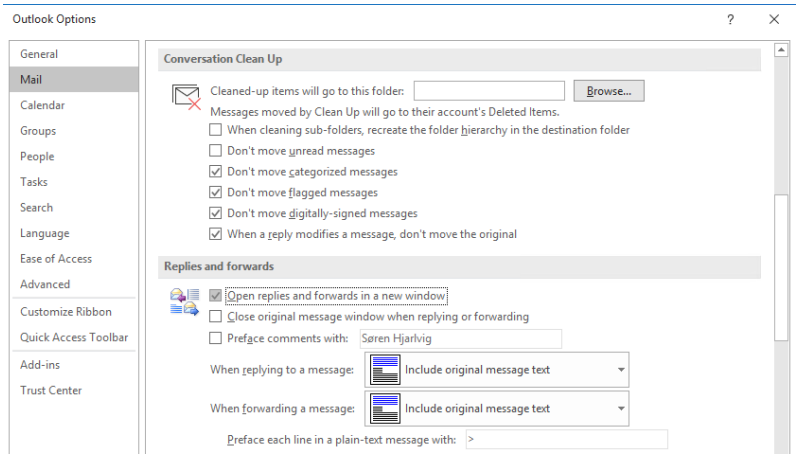
Downloading secure messages

When you receive a secure reply (e.g. a recipient has replied to a message sent with Bluewhale or someone has used your “Secure Inbound” link), you can always access it by clicking the provided link. However, it is also possible to import the message in Outlook.
This enables you to handle the secure message like any other email.
Just click **“Download message”** in order to download:



Open replies and forwards in a new window

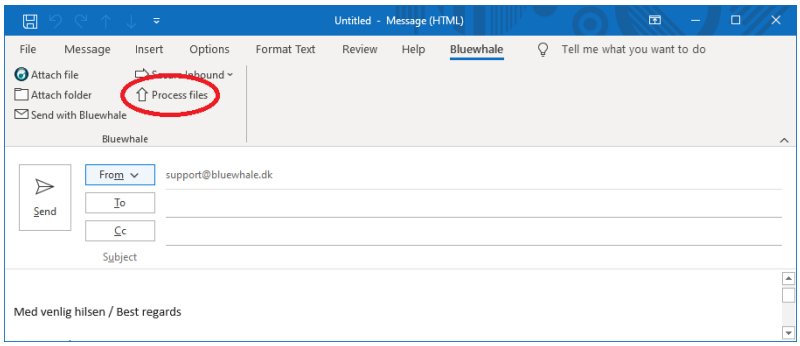
To enable Bluewhale functionality when replying or forwarding mail, you must check the “Open replies and forwards in a new window” option in Outlook mail settings.



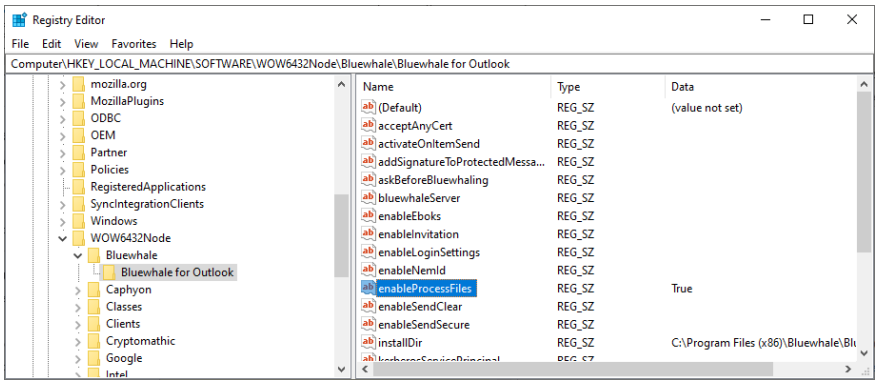
Enabling “Process files”

Sometimes it can be useful to combine the capabilities of Bluewhale with other secure mail solutions. Perhaps you wish to sign or encrypt the message using S/MIME or send the message using another secure mail add-in.

“Process files” prepares the message for delivery without sending the message. When the message is prepared, you can manually choose how to send the message.



To enable “Process files” set the Registry key HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bluewhale\Bluewhale for Outlook\enableProcessFiles to “True”.



Deployment

The Bluewhale for Outlook MSI supports various properties.
When Bluewhale for Outlook is installed the settings provided to the installer are stored in the registry:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bluewhale\Bluewhale for Outlook

This will be the default settings for all users on the machine. Personal settings are stored here:

HKEY_CURRENT_USER\Software\Bluewhale\Bluewhale for Outlook

When installing on many computers, it is recommended to create an install script or transformation file with the desired settings. It is also possible to push the settings using a group policy.

Example installation parameters

This example configures Bluewhale for Outlook for Kerberos single sign-on and a lower limit of 30 Mb. If there are attached more than 30 Mb of files to a mail, the user is automatically prompted to use Bluewhale (default is 20 Mb).

```
msiexec.exe /i bwoutlookSetup.msi /qn
   BLUEWHALE_SERVER="https://bluewhale.your.domain"
   SERVICE_PRINCIPAL="bwservice/bluewhale.your.domain@COMPANY.DOMAIN"
   USE_SSPI="True"
   LOWER_LIMIT="30"
   /l* bwinstall.log
```

Example installation parameters - Bluewhale Server 5.2+

With Bluewhale Server 5.2+ it is no longer needed to specify a login method. If single sign-on is configured on the server, Bluewhale for Outlook will automatically query the server and use the appropriate login method (Oauth2/SAML/Kerberos).

```
msiexec.exe /i bwoutlookSetup.msi /qn
   BLUEWHALE_SERVER="https://bluewhale.your.domain"
   LOWER_LIMIT="30"
   /l* bwinstall.log
```

Multi-user environments

By default Bluewhale for Outlook is available for all users on the system.
If you wish to limit the add-in to specific users, you can delete the HKLM registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\bwoutlook.AddinModule

And only re-add the key to HKEY_CURRENT_USER where needed using a group policy:

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Outlook\Addins\bwoutlook.AddinModule]
"FriendlyName"="Bluewhale for Outlook"
"Description"="Bluewhale for Outlook allows you to send and receive large files using e-mail."
"CommandLineSafe"=dword:00000000
"LoadBehavior"=dword:00000003
```

Registry settings

Property: BLUEWHALE_SERVER
Registry key: bluewhaleServer
Example value: https://bluewhale.company.com
User override: Yes
Description: URL to your Bluewhale Server.

Property: ASK_BEFORE_BLUEWHALING
Registry key: askBeforeBluewhaling
Default value: False
User override: Yes
Description: Prompt the user if the e-mail should be sent by Bluewhale.

Property: SAVE_PASSWORD
Registry key: savePassword
Default value: True
User override: Yes
Description: Bluewhale for Outlook can store Bluewhale login information in an encrypted form. Only used if Kerberos or AD FS single sign-on is not used.

Property: LOWER_LIMIT
Registry key: lowerLimit
Default value: 20
User override: Yes
Description: The default Bluewhale attachment size trigger in Mb. Mails with attachments larger than this limit, will be intercepted by Bluewhale.

Property: HIDE_BW_INFO_MESSAGE
Registry key: hideBwInfoMessage
Default value: False
User override: Yes
Description: This options toggles if the “Bluewhale is installed and ready to use”-message should be shown to the user, the first time Bluewhale is installed.

Property: ACCEPT_ANY_CERT
Registry key: acceptAnyCert
Default value: False
Description: If enabled Bluewhale will accept any SSL certificate, including self-signed certificates. **Not recommended for production systems.**

Authentication

Property: SERVICE_PRINCIPAL
Registry key: kerberosServicePrincipal
Example value: bwservice/bluewhale.your.domain@COMPANY.DOMAIN
User override: Yes
Description: Kerberos service principal. Required for Kerberos single-sign-on.

Property: USE_SSPI
Registry key: useSSPI
Default value: False
User override: Yes

Description: Login using Kerberos single sign-on.

Property: USE_ADFS
Registry key: useADSF
Default value: False
User override: Yes
Description: Login using AD FS.

Property: USE_ADAL
Registry key: useADAL
Default value: False
User override: Yes
Description: Login using ADAL/OAuth2.

Sending methods

Property: ENABLE_SEND_SECURE
Registry key: enableSendSecure
Default value: True
Description: Enables the extended "Send with Bluewhale"-dialog.

Property: USE_PIN_CODE_BY_DEFAULT
Registry key: usePinCodeByDefault
Default value: True
Description: Controls if "Send SMS PIN code" should be selected by default in Bluewhale dialog. If set to True the ASK_BEFORE_BLUEWHALING property is ignored since the Bluewhale dialog must always be shown. Can also be controlled server side.

Property: ENABLE_EBOKS
Registry key: enableEboks
Default value: False
Description: Enables Digital Post/e-Boks features. Can also be controlled server side.

Property: ENABLE_NEMID
Registry key: enableNemId
Default value: False
Description: Enables NemId features. Can also be controlled server side.

Property: ENABLE_Send_Clear
Registry key: enableSendClear
Default value: True
Description: Enables the ability to send large files and folder but with no extra recipient validation. Can also be controlled server side.

Additional features

Property: ENABLE_PROCESS_FILES
Registry key: enableProcessFiles
Default value: False
Description: Enables the Process Files button on the Bluewhale tab. This allows Bluewhale to be used in combination with other secure mail systems (e.g. Bluewhale handles the large files and the other system protects the message).

Property: ENABLE_INVITATION
Registry key: enableInvitation
Default value: False
Description: Enables the Insert Invitation button on the Bluewhale tab.

Property: ADD_SIGNATURE_TO_PROTECTED_MESSAGES
Registry key: addSignatureToProtectedMessages
Default value: True
Description: If enabled the user's standard signature is appended to secure messages.

Property: ACTIVATE_ON_ITEM_SEND
Registry key: activateOnItemSend
Default value: True
Description: If this property is true, Bluewhale will intercept Outlook send events and scan for Bluewhale attachments and large files.

Property: ENABLE_LOGIN_SETTINGS
Registry key: enableLoginSettings
Default value: True
Description: If this property is true, the user is allowed to adjust the Bluewhale settings.