BAYOOSOFT
MANAGEMENT SOFTWARE

Administrator Manual

GPG4O- Version 8.5

Manual for Administrators

Content

1 Introduction

This document describes the installation and configuration of gpg4o for usage on multiple systems in a network environment for system operators. Private users are advised to read the „Gpg4o User Manual“, which describes the general installation and usage of gpg4o.

From version 3.3 onwards, gpg4o has been optimized with its numerous improvements for application in companies. In particular, the configuration of gpg4o was extended such that it may be administrated via group policies now. With these group policies you can process the behavior or the settings of gpg4o, respectively, according to your demands.

2 Installation

Gpg4o is installed for all users of a computer which is why the installation or an update, respectively, may only be made by users with administrative privileges. For utilizing gpg4o you do not require administrative privileges.

2.1 Unattended Installation

Reasons for an unattended installation:

- Remote installation on a client-PC in your company
- Installation on different client-PCs in your company
- Updating gpg4o on different client-PCs in your company

For an installation of gpg4o without user interaction it is sufficient to indicate the parameter /quiet when calling the setup. gpg4o will then be installed on the computer without further feedback to the user.

```
gpg4o_setup.exe /quiet
```

If you utilize the downloaded „gpg4o_setup.exe“ for installation it is not necessary to perform any further preliminary work. The installation program checks whether all components required by gpg4o are available and installs them automatically, if necessary. Please mind that gpg4o downloads the required packages via the Internet.

For an offline installation of gpg4o please regard the hints and prerequisites stated in the following chapter 3.1.

Hint: The required OpenPGP implementation is not deployed when installing gpg4o unattended. Instead, you have to install GnuPG before the installation of gpg4o.

3 Distribution of gpg4o in the Company

3.1 Integration in automatic Software Distribution Systems

A distribution of gpg4o within a network is possible with customary tools. You can unpack the MSI using this command: `gpg4o_setup.exe /extract`

3.2 Offline Installation

In case you want to install gpg4o without or a slow internet connection you have to put the installation packages mentioned above into the same directory as the „gpg4o_setup.exe“.

You can find these packages in the download area on our website in the section „Software requirements“ https://www.bayoosoft.com/en/email-encryption/.

3.3 About operating on Terminal Servers

Please keep in mind that gpg4o temporarily generates a data file required for operations in the temp-directory of the user. This directory is not persistent on terminal servers which will cause problems when starting Outlook. This error can be prevented by activating a group policy (see chapter 3.3.2) (only gpg4o v6 or older).

3.3.1 Installation of gpg4o

After having installed gpg4o on the target computer every user of gpg4o necessitates a license file. This license file can be made available to the user via a copy procedure into the gpg4o user directory (see chapter 8). After having restarted Outlook gpg4o will recognize and utilize this license file. Alternative you can change the path to the license file by using the group policy (see chapter 3.4).

For the utilization of gpg4o with a computer with multiple users there may be cases where some of the users shall not obtain any license at all. If gpg4o is not disabled, these users will fall into the trial mode which will be available for 45 days from the time of the first installation onwards. Afterwards, gpg4o cannot be utilized any longer and dialogs will appear requesting to purchase.

As this disturbs the user during his work, we have designed a special license file for this („Cloak-License“) which causes an almost entire deactivation of gpg4o. Only importing a license from within an attachment of an email will remain available. This „Cloak-License“ can be requested from the support free of charge.

Distribution of this special license file takes place like any other license file and is described in chapter 3.4.

The other possibility to disable gpg4o is with the help of the group policies „Functional limitations\Licensing\Disable the use of gpg4o“. This has the same effect as the distribution of the cloak license, however, in most cases the effort is smaller.

3.3.2 Datafile in Roaming Directory

After successfully installing gpg4o on a terminal server, please activate the group policy „Functional restrictions\General Settings\Outlook data file for decryption into roaming directory “. This policy ensures that the data file required by gpg4o will be saved in the roaming directory (only gpg4o v6 or older).

3.4 License File Distribution

In case you want to administrate licenses from a central point then you are able to roll out these at any time. For example, this is the case when you have renewed your license subscription.

You can achieve this by using a startup script or you set path to the new license file by using the group policy „Functional restrictions\Licensing\Determine path to license file“. This policy can point to a folder in your network for example.

If you don’t want to set the path to the license file manually you have to copy it into the following directory:

%AppData%\BAYOOSOFT\gpg4o\LicenseInformation.lic

3.5 Activate gpg4o permanetly

To make sure gpg4o is permanently active, the following DWORD registry values have to be created or changed. These can be distributed via group policies.

Make sure that „LoadBehavior“ has the value 3. You can find it at:

HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Addins\gpg4o

Also make sure that „gpg4o“ has the Value 1. It can be found at:

HKEY_CURRENT_USER\Software\Microsoft\Office\x.0\Outlook\Resiliency\DoNotDisableAddinList

Please note that „x“ represents the version number of your current Outlook version. Possible values are „14“ for Outlook 2010, „15“ for Outlook 2013 and „16“ for Outlook 2016 as well as for Outlook 2019.

4 Set up additional encryption recipients

Sometimes it makes sense for all encrypted messages to be encrypted to an additional key in addition to the addressees and the sender named in the e-mail, e.g., for archiving the e-mail. Note, however, that the entry of an additional key will also be seen by every other recipient of the message and could possibly be misinterpreted there. For example, it could be interpreted as a sign of surveillance. You should therefore deal with this circumstance as openly as possible.

In order to set up an additional key (here archive key) for the encryption of all data, you need access to the "gpg.conf" file in the user directories of your users. This is usually located in the "%AppData%\gnupg\" folder, unless you have changed the path to the GnuPG data, e.g., via group policy. The "gpg.conf" is located in the corresponding directory, or you may have to create it again. In this case, you only need an empty text file. You also need the complete key ID of the archive key that is to be used. Open the file with any text editor and add the following line: *encrypt-to <long key-id>* where you replace *<long key-id>* accordingly. Finally, save the file.

You can test the result by sending a test mail in gpg4o (see Settings -> Account settings) and double-clicking on the green bar above the message in the *read* view while holding down the Ctrl key. You will now see some debug information where you can find the recipient keys. Note that these are the key IDs of the subkeys. You can find the key IDs of your subkey in the key details of the archive key. Alternatively, open the encrypted message on another computer where only the secret key of the archive key is located. You should now be able to decrypt the message there as well.

5 Group Policies

Since version 3.3, administrators can limit the utilization of program functions and program settings of gpg4o via group policies. The configuration of gpg4o was extended such that it can be set via group policies. For this purpose, the template-formats ADM as well as ADMX are available which you can request from the support free of charge. All newer Windows versions support template-format ADMX.

You can find the policies in the group policy administration editor under user configurations\BAYOOSOFT - gpg4o. All policies contain an explanation, stating how the program will behave with the user if the policy is enabled or disabled, respectively and what the standard behavior is like. A general rule for all settings is that when activating or deactivating, respectively, the setting is given, which means that the user cannot modify it later.

Example of Group Policies:

A keypair is placed at the disposal of the users. The users shall not be able to delete keypairs or to generate new keys.

The following group policies have to be activated for that purpose:

- Users must not delete keypairs
- Users must not generate keypairs

With these settings you have made sure that the user will not be able to generate his own keys and will not be able to unintentionally delete keys that have been placed at his disposal. With these settings the users must obtain their keypair from an administrative authority.

In the following you will find a list of the policies and their additional explanations for gpg4o. The presettings of gpg4o are indicated. (The initial installation of gpg4o utilizes these presettings.)

5.1 Functional Restrictions

- Users must not save emails permanently decrypted
  - If you enable the policy the users will not be able to save emails permanently decrypted any longer. By default, the users will be able to save emails permanently decrypted via the corresponding button.
- Users must not save passphrases permanently decrypted (gpg4o v6)
  - If you enable the policy the users will not be able to permanently save passphrases any longer. By default, the users will be able to permanently save passphrases within the gpg4o account settings (only gpg4o v6 or older).

5.1.1 Backup

- Users must not export any backups
  - If you enable the policy the users will no longer be able to export any backups in the settings. By default the users can export backups.
- Users must not import any backups
  - If you enable the policy users will not be able any longer to import backups in the settings or the configuration wizard, respectively. By default, the users can import backups, however, depending on the status of the policy "Users must not import any licenses", importing of the license will be skipped.

5.1.2 Licensing

- Disable the use of gpg4o
  - If you enable the policy gpg4o will be disabled with the users to the greatest extent. Only the import of license files from an email will remain active as far as this has not also been disabled by means of a policy. By default, gpg4o will be loaded and is normally usable within the scope of the license.
- Users must not import any licenses (gpg4o v6)
  - If you enable this policy the users will no longer be able to import any license files, neither from an email nor from the file system. Additionally, the license will be ignored when importing a backup. By default, users can import license files. In addition, when importing a backup, the import of the license will not be skipped (only gpg4o v6 or older).
- Determine path to license file
  - If you enable this policy, the license file of the user will not be loaded from the default location anymore but from the path you selected. You can also use a UNC path. Should the path be not available, the last successfully loaded license is loaded from the local cache. By default, the license will be loaded from the default path in the user's roaming directory.

5.1.3 Key Management

- Users must not apply any revocation certificates
  - If you enable this policy the users will not be able to apply any revocation certificates to their keypairs. This will then have to be done by an administrative authority. Said administrative authority must then redistribute the revoked key. By default, the users will be able to apply revocation certificates to their keypairs.
- Users must not modify the passphrase of their keypairs
  - If you enable this policy the users will not be able to modify the passphrase of keypairs in their keyring. By default, the users will be able to modify the passphrase of keypairs in their keyring. This does not modify the key itself. Thus, copies of the key will remain unaffected and functional.
- Users must not generate any keys
  - If you enable this policy the users will not be able to generate any keys. An administrative authority must be available which generates and manages the keys, and which issues them to the users. By default, the users will be able to generate their own keys.
- Users must not generate any revocation certificates
  - If you enable this policy the users will not be able to generate any revocation certificates for their keypairs. These revocation certificates will then have to be generated by an administrative authority having a copy of the keypair. By default, the users will be able to generate revocation certificates for their keypairs.
- Users must not delete any keypairs
  - If you enable this policy the users will not be able to delete keypairs from their keyring. By default, the users will be able to delete keypairs from their keyring.
- Users must not delete any public keys
  - If you enable this policy the users will not be able to delete any public keys from their keyring. However, this policy does not have any influence when deleting keypairs. By default, the users will be able to delete public keys from their keyring.
- Users must not enable or disable any keys
  - If you enable this policy the users will not be able to enable or disable any keys in their keyring. By default, the users will be able to enable or disable keys in their keyring.
- Users must not export any keypairs
  - If you enable this policy the users will not be able to export any keypairs as a file. By default, this policy the users will be able to export keypairs.
- Users must not export any public keys
  - If you enable this policy the users will not be able to export any public keys or to send them by email. This excludes exporting public keys to key servers. By default, the users will be able to export public keys and to send them by email.

- Users must not import any keypairs
  - If you enable this policy the users will not be able to import any keypairs from files, attachments or from the clipboard. By default, the users will be able to import keypairs from the mentioned media.
- Users must not import any public keys
  - If you enable this policy the users will not be able to import any public keys from files, attachments or from the clipboard. This excludes importing public keys from key servers. By default, the users will be able to import public keys from the mentioned media.
- Users must not download any keys from key servers
  - If you enable this policy the users will not be able to import any public keys from key servers. This does not apply to the server for the automatic downloading of keys. By default, the users will be able to import public keys from key servers.
- Users must not upload any keys to key servers
  - If you enable this policy the users will not be able to upload any public keys to key servers. This also applies to the public part of the own keypairs. By default, the users will be able to upload public keys to key servers.
- Users must not set/modify the owner trust of keys
  - If you enable this policy the users will not be able any longer to set or modify the owner trust of keys in their keyring. By default, the users will be able to set or modify the owner trust of keys in their keyring.
- Users must not sign keys
  - If you enable this policy the users will not be able to sign any keys. The keys will have to be signed by an administrative authority. By default, the users will be able to sign keys. This policy only refers to the exportable signature and not to local signatures.
- Users must not locally sign keys
  - If you enable this policy the users will not be able to locally sign keys. By default, the users will be able to locally sign keys. This policy only refers to the not exportable „**local**“ signature.
- Users must not extend keys
  - If you enable this policy the users will not be able to extend the expire date of any keypair. By default, the users will be able to extend keypairs.

5.1.4 Sending Rules

- Users must not generate any sending rules
  - If you enable the policy the users will not be able to generate any sending rules. By default, the users will be able to generate sending rules.
- Users must not delete any sending rules
  - If you enable the policy the users will not be able to delete any sending rules. By default, the users will be able to delete sending rules.
- Users must not modify any sending rules
  - If you enable the policy the users will not be able to edit existing sending rules. By default, the users will be able to edit existing sending rules.

5.2 Default Settings

5.2.1 Update Settings

- Determine update behaviour of gpg4o
  - If you enable this policy gpg4o will search for updates according to your selection. Mind, however, that even with automatic search for updates this installation will still have to be confirmed by the users before they will be installed. By default, the users will be able to influence the settings with regard to updates by themselves.

5.2.2 General Settings

- Always clone mails instead of copying them (gpg4o v6)
  - If you enable this policy gpg4o will clone emails for decryption. By default, emails will not be cloned, and the outlook internal copy routine will be used if possible (only gpg4o v6 or older).
- Users must not decrypt insecure mails with missing MDC protection
  - If you enable this policy the users will not be able to decrypt mails with missing MDC protection.
    If you disable this policy the user will be able to decrypt mails with missing MDC protection.
- Decrypting of emails in public folders (gpg4o v6)
  - By default, gpg4o tries to decrypt emails in public folders and verify their signature. (The corresponding private key is required for decryption.) If you disable this policy gpg4o will not process any emails in public folders (only gpg4o v6 or older).
- Find OpenPGP keys in attachments
  - By default, gpg4o searches for OpenPGP keys among the attachments of an email that shall be displayed and offers the user to import them. If you disable this policy gpg4o will not search for OpenPGP keys among attachments. The import of public keys or keypairs has to be allowed.

- Find gpg4o licenses in attachments (gpg4o v6)
  - By default, gpg4o searches for its license files among the attachments of an email that shall be displayed and offers the user to import them. If you disable this policy gpg4o will not search for its license files. The import of license files has to be allowed (only gpg4o v6 or older).
- Use advanced signature check
  - If you enable this policy PGP/MIME signatures without encryption will also be checked. This can fail depending on the mail server and its configuration. By default, gpg4o will not check signatures in PGP/MIME signed but not encrypted emails.
- Redirect sales requests to an own email address
  - If you enable this policy, you can enter an email address, that will be used for sales-inquiries. The default email address is: sales@gpg4o.de
- Redirect support requests to an own email address
  - If you enable this policy, you can enter an email address, that will be used for technical inquiries. The default email address is: support@gpg4o.de
- Hide filename
  - By default, the original filenames of email attachments will be hidden when they are going to be encrypted. Thus, encrypted filenames such as attachment1.pgp will appear instead of the actual filename with attached file extension. However, this manner of encrypting files is not supported by all OpenPGP-implementations. If you disable this policy the filenames will not be hidden. For example, the filename Invoice.xlsx.pgp will appear then. Indeed, this variant allows conclusions to be drawn with regard to the contents of the files, but it is better compatible with other OpenPGP-implementations.
- Hint for expiring keypairs
  - By default, users get a hint if an account key will be expired until the next 30 days. With this hint the users also get the possibility to extend their keys for one more year. If you disable this policy the users do not get a hint for expiring keypairs.
- Utilize domain based key search (gpg4o v6)
  - If you activate this policy, when encrypting messages to recipients for whom no suitable key can be found, an alternative key is searched for in the locally available keys. By default, gpg4o will not determine a missing key based on the domain of the recipient (only gpg4o v6 or older).
- Use the file extension .gpg for encrypted attachments
  - By default, the file extension .gpg will always be used for encrypted attachments. If you disable this policy the file extension .pgp will always be used for encrypted attachments.

- Use the gpg4o-internal packet parser
  - By default, gpg4o will analyze the data of OpenPGP packets largely independent to save computing time. This can cause problems with some attachments. In this case gpg4o will use GnuPG for analysis. If you disable this policy gpg4o will always use GnuPG to analyze the OpenPGP data.
- Perform decryption in a separate outlook data file (gpg4o v6)
  - Before decrypting emails are always copied/cloned to a place from where they will not be synchronized with the server. By default, the datafile gpg4oTemo.pst will be used for this. If you disable this policy a folder called Temp below your inbox will be used instead and its synchronization with the server will be prevented. Because this prevention cannot be guaranteed in all cases you should disable this policy only if having problems using the datafile (only gpg4o v6 or older).
- Detect keypairs with outdated MD5 signature algorithm
  - By default, gpg4o will search for keypairs with the outdated MD5 signature algorithm. If any keypairs are found the user gets the opportunity to update these keypairs to a modern signature algorithm. This search will not be performed when disabling this policy.
- Put Outlook data file for decryption into roaming directory (gpg4o v6)
  - By default, gpg4o stores the data file used for decryption in the %Temp% directory of the user. In terminal server environment this can lead to problems when starting the program, which can be prevented by activating this policy. gpg4o stores the data file in the roaming directory in this case (only gpg4o v6 or older).

5.2.3 Key server Settings

- Allow automatic import for verification
  - If you enable this policy the users can use the automatic import for signature verification. A server must be available for automatic import. By default, users cannot use this function.
- Determine key server list
  - If you enable this policy the users can only use the given key servers. You need to enter the key server's URI and their privileges. The privileges are separated into download and export and can have the values 0 (Not allowed), 1 (Only manually allowed), 2 (Only automatically allowed) and 3 (Both allowed). The value needs to be formatted by entering the numeric value of the download privileges followed by a semicolon and the upload privileges. Entering „hkp://keys.company.com 3;1 " results in a single key server available to the users, which can be used for downloading and uploading keys manually and also automatically import missing keys while writing emails from this server. By default, users will be able to determine their key servers by themselves.

- Update locally existing keys
  - If you enable this policy keys will be imported into the user's keyring even when they exist there already. So, the keyring of the user is kept up to date. Prerequisite is that you have configured at least one key server in the list of key servers as a source for automatic download of keys.
  - By default, the keyring will not be updated automatically.

5.2.4 View Settings

- Show encryption status in inspectors (gpg4o v6)
  - If you enable this policy gpg4o will insert the encryption status at the beginning of the message when opening a message in an own window (Inspector). By default, gpg4o will not insert any encryption status in the message (only gpg4o v6 or older).
- Link encryption status in permanently decrypted messages (gpg4o v6)
  - By default, gpg4o will insert the encryption status at the beginning of the message during permanent decryption. If you disable this policy gpg4o will not insert any encryption status in the message (only gpg4o v6 or older).
- Show encryption status in the gpg4o reading pane (gpg4o v6)
  - By default, gpg4o will insert the encryption status at the beginning of the message when reading a message in the gpg4o reading pane. If you disable this policy gpg4o will not insert any encryption status but only display the message itself (only gpg4o v6 or older).
- Show encryption status with printed emails (gpg4o v6)
  - By default, gpg4o will insert the encryption status at the beginning of the message when printing a message via the button Print in the gpg4o reading pane. If you disable this policy gpg4o will not insert any encryption status (only gpg4o v6 or older).
- Show encryption status in answers (gpg4o v6)
  - By default, gpg4o will insert the encryption status at the beginning of the original message when answering or forwarding a message. If you disable this policy gpg4o will not insert any decrypting information into the original message (only gpg4o v6 or older).
- Language selection
  - If you enable this policy gpg4o will be started with the language selected by you when the users start Outlook, the next time. By default, the users will be able to set their preferred language by themselves.
- Hide send options with inactive gpg4o-accounts
  - If you enable this policy the users will see the gpg4o send options only when generating emails from an active email account. By default, the send options will be displayed for all new emails.

5.2.5 GnuPG Settings

- Online update GnuPG version information every time Outlook starts
  - By default, the list of GnuPG versions will be updated from the internet every time outlook is started. If you disable this policy the list will not be updated.
- Don't show notification about other installable GnuPG versions
  - If you enable this policy gpg4o will not notify about other installable GnuPG versions.
  - By default, gpg4o will notify about other installable versions.
- Don't show notification about unknown GnuPG versions
  - If you enable this policy gpg4o will not notify about GnuPG versions that it doesn't know.
  - By default, gpg4o will notify about unknown versions.
- Caching time of a passphrase when utilizing the GnuPG agent (GnuPG 2.0.x)
  - This policy only applies to those users who utilize GnuPG 2.0.x with the GnuPG agent. If you enable this policy the GnuPG agent will cache passphrases entered for the period of time indicated by you. The duration is counted separately for every private key. If a private key is not used for more than the indicated period of time the user will be demanded the passphrase again during the next utilization. By default, the users will be able to determine the duration by themselves.
  - The passphrases will be cached for 5 minutes if no duration was set by the user.
- Caching time of a passphrase when utilizing GnuPG 1.4.x (gpg4o v6)
  - This policy only applies to users who utilize GnuPG 1.4.x. If you enable this policy gpg4o will cache the last entered passphrase for the period of time indicated by you. If another key is used than that used last and if the passphrases differ the user will have to enter the passphrase of the other key. If you disable this policy the users will be able to determine the duration by themselves.
  - The policy is disabled. The passphrases will be cached until quitting Outlook (only gpg4o v6 or older).
- Determine GnuPG home directory
  - If you enable this policy gpg4o will load the keyrings from the directory indicated by you. That is why the path should use a user-specific system variable in order to exclude the situation that all users access the same keyrings. By default, the users will be able to set the directory by themselves.
  - The default directory will be taken: %AppData%\gnupg
  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.

- Determine path to GnuPG
  - If you enable this policy gpg4o will utilize the GnuPG-installation under the path indicated by you. You can also use system variables under the path. If you disable this policy the users will be able to determine the path to the GnuPG installation by themselves.
  - The path will be identified automatically. By default, GnuPG will be searched via the registry or alternatively under %ProgramFiles(x86)%\GNU\. GnuPG will be searched with the filenames gpg.exe or gpg2.exe, respectively.
  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.
- Determine timeout of GnuPG processes
  - If you enable this policy, you determine the duration of how long gpg4o will wait for the GnuPG processes to end normally before it will inform the user about a potential error. The user can then give the process more time to end or terminate the process. If you disable this policy the default value of 15 seconds will be used. This value cannot be configured by the users in the configuration of gpg4o. If you encounter problems with long running GnuPG processes on some computers, you should enable this policy to give them more time.
  - The default setting of 15 seconds (value: 15000 ms) will be used if not configured otherwise.
- Always trust keys
  - If you enable this policy the users will be able to send encrypted messages to all key owners and to check all signatures of the key owners - irrespective of the web of trust. Even though this is easier for the users you should not activate this policy as it permits the use of untrustworthy keys. If you disable this policy keys will have to be validated by the web of trust first before they can be used.
  - By default, all keys will be trusted.
- Disable GnuPG-headers
  - If you enable this policy the insertion of the GnuPG version information as well as the annotation with the gpg4o version will be disabled. This may be reasonable for security reasons. By default, the above-mentioned lines will always be inserted. In case of a bug this facilitates debugging with the recipient.
- Quit GnuPG agent as well when quitting Outlook
  - By default, the GnuPG agent will be terminated when quitting Outlook. Thus, all saved passphrases will be forgotten and will have to be entered again, if necessary, when rebooting Outlook. If you disable this policy the GnuPG agent will not be terminated when quitting Outlook. Passphrases will be available as well after rebooting Outlook as far as the period of caching is not exceeded.

5.2.6 Log Settings

- Determine the verbosity of logging
  - If you enable this policy, you can set the logging behavior for gpg4o. By default, gpg4o logs all activities except for the time measurements and stack traces.
  - The policy is configured. The default setting is Log Level 6.
- Limit the maximum amount of log files (gpg4o v6)
  - If you enable this policy, you can set the maximum amount of log files.
  - The default amount is 30 log files (only gpg4o v6 or older).
- Logging in case of extended signature checking (gpg4o v6)
  - By default, the external library gpg4oH will be able to write log outputs. If you disable this policy gpg4oH will not write any log outputs. This policy is should only be changed in case of issues (only gpg4o v6 or older).

5.2.7 Homedir Backup Settings

- (De)Activate automatic GnuPG homedir backups
  - If you enable this policy a daily backup of the GnuPG home directory will be created as a zip archive.
  - If activated, the user won't be able to modify the destination directory and the number of backups to keep.
  - This feature is only available for users with professional license.
- Maximum count of homedir backups to keep
  - Declare the maximum count of kept backups of the GnuPG home directory.
  - Default: 60 backups are kept.
- Path to destination directory for homedir backups
  - Set the directory for the GnuPG home directory backups.
  - The path cannot contain a backslash at the end.
  - Default: %AppData%\BAYOOSOFT\gpg4o\Backup
  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.
- Interval of backups
  - Set the frequency of the GnuPG home directory backup.
  - Default: Data is backed up every 1440 minutes (24 hours).

6 Distribution of Sending Rules

Please create the sending rules on a computer with gpg4o. Then copy the file „Rulelist.xml“ to the desired computers. The file resides in the user directory of gpg4o. (see chapter 9)

To prevent users from modifying the sending rules you can activate group policies. (See chapter 5.1.4)

7 Automated Generation of Keypairs

Gpg4o offers you the possibility of generating several keypairs in one flow. This is reasonable for example if during initial operation of gpg4o in a company you have to equip many employees with keypairs.

For this you only need a functionally set gpg4o with empty keyrings and a CSV-file with the data of the keypairs to be generated.

7.1 Preparation

The setting of gpg4o must be functional and the GnuPG keyrings should be empty. This can be achieved by renaming the directory for the keyrings with closed Outlook.

You can find the storage locations of the gpg4o and GnuPG files referenced in the present paragraph in the chapter 9.

Attention: The keyrings contain your private key which you need for decrypting emails. That is why you should not delete the keyrings or overwrite a backup!

The data of the keypairs to be generated must be available in a CSV-file (Comma Separated Values).

The CSV-file comprises the data separated from another by semicolon per line „;“ for every individual keypair and consists of three columns for name and first name, the email address and the passphrase:

Mrs. Smith, Erika;Erika.Smith@work.com;passphrase
Karl-Heinz Smith;Karl-Heinz.Smith@work.com;passphrase
John Doe;JohnDoe@work.com;passphrase

Please mind that the file does not contain a header with column identifiers.

Attention: The CSV-File should be stored in a secure place!

7.2 Generation of the Keypairs

You can then call the dialog (New Key) in Outlook via the key management in order to generate a new keypair. Here, the algorithm to be utilized for the keys, the length of the primary and subkey and the expire date can be selected as well.

If you enter the text „[csv]“ in the field „Name“ in this dialog and if you click the button „OK“ a file dialog will be opened. There you can choose your saved CSV-file. The keys will be generated once you open the file.

The thus generated keys will afterwards be available via the gpg4o key management. Already existing keys will be identified by means of the email address and will not be generated/overwritten so that there will not be the risk of duplicates.

7.3 Backup of the Keypairs

Hint: You should always use a safe passphrase for the generation of the keypairs.

Hint: After having generated the keypairs you should make a backup of those keypairs. For that purpose, you simply have to save the two files „secring.gpg“ and „pubring.gpg“ which can be found in the GnuPG directory see chapter 9 The associated passphrases shall be saved as well.

7.4 Distribution of the Keys

The generated public keys can be exported individually into the file system via the gpg4o key management or can be uploaded to a key server so that the users will be able to import them on their keyring.

Tip: With the key management it is also possible to highlight several keys at the same time.

If it is a question of an initial installation in your company and all the users shall receive the public keys generated in the previous paragraph you can copy the file „pubring.gpg“ in the GnuPG directory (see chapter 9) to the target computers.

Now you export the private key to a data storage medium (USB-stick, CD/DVD, ...) or to a specially secured network drive and send it to the individual user so that he or she may import the keypair with the gpg4o key management.

Attention: You should only let the users receive their keypairs via a secured path as otherwise there will be the risk that unauthorized persons might decrypt emails or sign them under the name of another person.

Hint: After having imported the private key into the user’s computer the passphrase will have to be changed by the user!

8 gpg4o Update via a Proxy Server

For connection establishment with the update server via a proxy server gpg4o uses the network settings which are directly configured in your system. In order to establish connection via a proxy server you have to enter said proxy server into your Internet options.

You can find these Internet options under the „Control panel“ of Windows under the „Internet options“.

Open the tab „Connections“ in the following window and click on the button „LAN settings“ in the lower section.

In the following window you can now enter the address of the desired proxy server or an automatic configuration script in order to permit gpg4o to build up a connection with the update server (or similar).

9 Paths to Files of gpg4o und GnuPG

9.1 User Directory

%AppData%\BAYOOSOFT\gpg4o\

9.2 License File

%AppData%\ BAYOOSOFT \gpg4o\LicenseInformation.lic

9.3 Folder for Log Files

%AppData%\ BAYOOSOFT \gpg4o\LogFiles\

9.4 GnuPG Directory

%AppData%\gnupg\

9.5 Sending Rules

%AppData%\ BAYOOSOFT \gpg4o\Rulelist.xml

10 Company and Support Contact Information

10.1 Support

Please use the following e-mail address to request support related to gpg4o from **BAYOOSOFT GmbH**:
support@gpg4o.de

10.2 Contact:

BAYOOSOFT GmbH

Machtlfinger Straße 11

81379 München

Deutschland

Internet: https://www.bayoosoft.com/en/email-encryption/