Guard

User Guide

Guard: User Guide

Publication date Tuesday, 12. July 2016 Version 2.4.2

Table of Contents

1 About This Documentation

The following information will help you make better use of the documentation.

Who is the Target Group for this Documentation?

This documentation is addressed to users who want to use encryption to protect their E-Mail communication and files against unauthorised access.

Which Contents are Included in the Documentation?

This documentation includes the following information:

- In *What is Guard for?* you will find a short description of Guard.
- In *Using Guard* you will find instructions for using Guard.

This documentation describes working with a typical groupware installation and configuration. The installed version and the configuration of your groupware might differ from what is described here.

Additional Help

A comprehensive groupware documentation can be found in the Groupware User Guide.

2 What is Guard for?

Guard is a groupware security component that allows to encrypt E-Mail messages and files.

- Encrypt your E-Mail communication with other users or external partners.
- Encrypt single files. Share the encrypted data with other users.
- Use the security options to define the encryption level.
- The encrypted data is password-protected. Use the password reset function to protect against the consequences of a lost password.

3 Using Guard

Learn how to work with the *Guard* application.

- apply basic settings
- encrypt E-Mail communications
- encrypt files
- apply security settings

3.1 Setting up *Guard*

Prior to being able to use *Guard*, you have to apply some basic settings.

- First of all you have to enter a Guard security password that is used to encrypt data and to access encrypted data.
- Enter a secondary E-Mail address that is used if you forget your Guard security password. In this case, use the function for resetting the Guard security password. A new password will then be sent to you. For security reasons, it is highly recommended that you enter a secondary e-mail address for this purpose. Otherwise the new password is sent to your primary e-mail account.

There are two options for entering the basic settings:

- Define the basic settings while initially using an encryption function.
- Define the basic settings in the groupware settings page before using the encryption function.

How to define the basic settings when initially using an encryption function:

1. Enable the encryption function when composing an E-Mail, encrypting a file or uploading a new file by clicking on the **Encrypt** icon next to the folder name in the folder tree.
2. You consecutively will be asked to enter a Guard security password and a secondary e-mail address. Enter the data.

How to define the basic settings before initially using an encryption:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Click on **Guard Security** in the side bar.
   When initially opening the Guard security settings, the *Guard Create Security Keys* window opens.
3. In the **Password** field, enter the password that you want to use for encrypting your data.
   Confirm the password in the **Verify** field by entering it again.
4. In the **Enter new secondary e-mail** field, enter the e-mail address that is used for receiving a temporary password for resetting your Guard security password.
5. Click on **OK**.

3.2 Encrypting E-Mail Conversations

The following options are available:

- Reading encrypted E-Mail Messages
- Sending encrypted E-Mail Messages
- How can external recipients read an encrypted E-Mail?

3.2.1 Reading encrypted E-Mail Messages

To be able to read an encrypted e-mail, the Guard security password is required at least. The sender of an encrypted e-mail can protect the E-Mail with an additional password.

How to read an encrypted E-Mail:

1. Select an E-Mail with the *Encrypted* icon . In the detail view, the notification *Secure E-Mail, enter your Guard security password.* is displayed.

   Note: If, when having used Guard the last time, you set that Guard should remember the security password, the e-mail is displayed immediately, depending on the setting.
2. Enter the Guard security password.

   You can define how long the security password should be remembered by Guard. To do so, enable Keep me logged into **Guard** . Select a value from the list.
3. Click on **OK**. The content is shown in plain text.

   If the E-Mail includes attachments, functions for using the attachments' decrypted or encrypted versions are displayed.

Note: You can only reply to this E-Mail or forward it when using an encrypted E-Mail.

3.2.2 Sending encrypted E-Mail Messages

The following options are available:

- Sending an encrypted E-Mail. Only you and the recipients can read the e-mail content.

  Warning: When sending an encrypted E-Mail draft, the draft will be deleted when being sent from the *Drafts* folder.
- Sending an E-Mail with a signature. The signature ensures that the recipient is able to recognise whether the E-Mail content has been changed on the transport.
- Sending an encrypted E-Mail with a signature.

How to send an encrypted E-Mail:

1. Compose an E-Mail in the *E-Mail* app as usual.

   In the *Compose* page, click the **Encrypt** icon on the upper right side.

   You can also click on **Security** below the subject. Enable **Encrypt**.

   Icons next to the recipients indicate whether the message can be encrypted for this recipient. If hovering over an icon, a description will be displayed.

2. In order to show additional options, click on **Security**. You can activate the following options.

   In order to additionally sign the E-Mail, enable **Sign**.

   In case the recipient's E-Mail client does not support PGP, the message should be readable though, enable **PGP Inline**. If you use this setting, you can not send E-Mail messages in HTML format.

   To enable the e-mail recipient to send an encrypted reply, the recipient needs to have your public key. You can send your public key as an attachment. To do so, enable **Attach my key**.

3. Click on **Send encrypted**.

   When sending to external recipients, a window is displayed that allowssending notes for opening the encrypted E-Mail [12] to the external recipients.

   When initially sending an encrypted E-Mail to an external recipient, the latter receives an E-Mail attachment with your public key.

3.2.3 How can external recipients read an encrypted E-Mail?

You can also send encrypted E-Mail messages to external recipients who are not groupware users. When adding an external recipient, Guard checks whether a public key is available for this recipient. Depending on the result, Guard uses different procedures for sending the encrypted E-Mail.

- If there is a public key for the recipient:
  - The message is encrypted and sent with this key. The recipient can read the message with his/her private key.
  - To enable the recipient to send an encrypted reply, your public key is sent as an attachment. The attachment is called public.asc. The recipient can import this key to his/her E-Mail client.
- If there is no public key for the recipient:
  - If the external user already has a guest account, he/she receives an E-Mail with the link to the login page of his/her guest account. When having logged in, he/she can read the encrypted E-Mail on the guest page. He/she can send an encrypted reply from this page.
  - If there is no guest account, a guest account will be created. The external recipient receives an E-Mail with some guidelines and an automatically created password. He/she receives an additional E-Mail with the link to the guest page. On the guest page, he/she logs in with the automatically created password. Then he/she can create a password.
  - Depending on the groupware configuration, guest account E-Mail messages are deleted after a specific number of days. To still make those E-Mail messages available, the E-Mail with the link to the guest page contains an attachment with the encrypted E-Mail. The attachment is called encrypted.asc. This attachment can be uploaded and read on the guest page.

3.3 Encrypting files

The following options are available:

- Encrypting files
- Creating new encrypted files
- Opening encrypted files
- Downloading encrypted files
- Decrypting files

3.3.1 Encrypting files

When encrypting a file, only the latest version of the file will be encrypted. All other versions will be deleted.

How to encrypt a file:

Warning: When encrypting a file, all versions of the file will be deleted, except for the current version. If you need to keep an older version, save it before encrypting the file.

1. Select one or several files in the *Drive* app. Click the **Actions** icon in the tool bar. Click on **Encrypt** in the menu.

   You can also use the **Actions** icon on the right side of the categories bar. Click on **Encrypt** in the menu.

2. If the file contains multiple versions, the *Encrypt Files* window is displayed. Confirm that you want to encrypt the file and delete all previous versions by clicking on **OK**.

   If the file contains one version only, the file is encrypted without additional requests.

3.3.2 Creating new encrypted files

You can create a new encrypted file by uploading a local file with encryption.

How to create a new encrypted file:

1. In the *Drive* app, select a folder in the folder tree.

   Note: Open a folder for which you have the appropriate permissions to create objects.

2. Click on **New** in the tool bar. Click on **Add and encrypt local file**.

3. Select one or several files in the *Upload file* window.

   Click on **Open**. The display area shows the current progress status.

   In order to cancel the process, click on **File Details** at the bottom right side of the display area. Click on **Cancel** next to a file name in the *Upload progress* window.

Tip: You can also create a new encrypted file by dragging a file from your operating system's desktop to the *Drive* app window and dropping it in the upper part.

3.3.3 Opening encrypted files

You can open and read an encrypted file. The file remains encrypted on the server.

How to open an encrypted file:

1. In the *Drive* app, select an encrypted file in the display area. Click the **View** icon in the tool bar.
2. The *Enter Guard security password* window opens. Enter the Guard security password.
   You can define how long the security password should be remembered by Guard. To do so, enable **Remember Password**. Select a value from the list.
   Click on **OK**.

3.3.4 Downloading encrypted files

You can download an encrypted file to locally read or edit it. The file remains encrypted on the server.

How to download an encrypted file:

1. In the *Drive* app, select an encrypted file in the display area. Click the **View** icon in the tool bar.
   Note: If you click on **Download** in the pop-up instead, the downloaded file remains encrypted.
2. The *Enter Guard security password* window opens. Enter the Guard security password.
   You can define how long the security password should be remembered by Guard. To do so, enable **Remember Password**. Select a value from the list.
   Click on **OK**.
3. Click the **Actions** icon in the viewer. Click on **Download Decrypted**.

3.3.5 Decrypting files

You can remove a file's encryption by decrypting the file.

How to decrypt a file:

1. In the *Drive* app, select an encrypted file in the display area. Click the **Actions** icon in the tool bar. Click on **Remove Encryption** in the menu.
2. The *Enter Guard security password* window opens. Enter the Guard security password.
   You can define how long the Guard security password should be valid. To do so, enable **Remember Password**. Select a value from the list.
   Click on **OK**.

3.4 Sign out Guard

You can sign out from Guard without closing the groupware. To open an encrypted e-mail, file or folder afterwards, you again have to enter the Guard security password.
Note: This function is only available if you enable **Remember Password** when opening an encrypted e-mail or file.

How to sign out from Guard:

1. Click the **System menu** icon on the right side of the menu bar.
2. Click on **Sign out Guard** in the menu.

3.5 Guard Settings

There are the following options:

- In order to manage your Guard security password, use the Guard security settings.
- To change the default settings for sending secure e-mail messages, use the PGP encryption settings.
- You can adminster your PGP keys.

3.5.1 Guard security settings

There are the following options:

- change the Guard security password
- When Guard you have lost the security password, you can request a temporary Guard security password by resetting the Guard security password.
- change the secondary E-Mail address

How to change the Guard security password

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. In the side bar, click on **Guard** Security.
3. In the **Enter current Guard security password** field below *Password*, enter the password that you have used so far for encrypting your data.

   In the **Enter new Guard security password** field, enter the password that you want to use for encrypting your data from now on.

   Confirm the password in the **Verify new Guard security password** field by entering it again.
4. Click on **Change Guard security password**.

How to reset the Guard security password:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. In the side bar, click on **Guard** Security.
3. Click on **Reset Guard security password**. A new password will be sent to your secondary e-mail address.

   If not having entered a secondary E-Mail address, the new password will be sent to your primary E-Mail address.
4. This new password is now your current Guard security password. You should immediately change this password.

How to change your secondary E-Mail address for resetting the encryption password:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. In the side bar, click on **Guard** Security.
3. Enter the password for encrypting your data in the **Enter current Guard security password** field below *Secondary E-Mail*.

   In the **Enter new secondary e-mail** field, enter the e-mail address that is used for receiving a temporary password for resetting your Guard security password.

   Click on **Change e-mail**.

3.5.2 PGP encryption settings

The PGP encryption settings define the preset settings that are available when composing e-mail messages. When composing a new e-mail, the default settings can be adjusted before sending the e-mail.

How to change the PGP encryption settings:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Select the entry **Guard** Security in the side bar. Click on **Advanced settings**.
3. Change a setting below *PGP Encryption Settings*.

The following settings are available.

Default to send encrypted when composing e-mail

Defines whether a new E-Mail is encrypted with PGP by default.

Default adding signature to outgoing e-mail messages

Defines whether a new E-Mail is encrypted with PGP by default.

Enable advanced PGP features

Defines whether PGP features, like key management are displayed.

Default to using PGP inline for new e-mail messages

To show this setting, enable the checkbox **Enable Advanced PGP Features**.
Defines whether the PGP encryption is done inline. Only use those settings if the e-mail client of a recipient does not support PGP, the message should be readable though. If you use this setting, you cannot send e-mail messages in HTML format.

3.5.3 Administering keys

In order to send or receive encrypted messages, the functions for administering keys are typically not required. Those functions can be used for the following requirements though:

- You want to use your Guard PGP keys in other e-mail clients, e.g.: in local e-mail clients.
- You have PGP keys from other PGP applications. You want to use those keys in Guard.
- You have an external partner's public key. In order to read encrypted messages from this external partner without having to access a key server, you want to import the partner's public key into Guard.
- You want to provide your public key to a recipient in order to give the latter read access to your encrypted messages without the need to access a key server.

How to open the page for administering your keys:

1. Click the **System menu** icon on the right side of the menu bar. Click the **Settings** menu item.
2. Select the entry **GuardSecurity** in the side bar. Click on **Advanced Settings**.
   Enable **Enable Advanced PGP Features**.

The page contains the following elements.

- Options for adjusting the Guard default settings
- *Your Keys* section. Contains functions for administering your private and public PGP keys.
  Your existing keys will be displayed below *Your Key List*. The key list contains two keys:
  - A master key. Among other things, this key is used for signing your E-Mail messages.
  - A subkey. This key is used for encrypting and decrypting E-Mail messages and files.

  The differentiation between master key and subkey is one of the features of the PGP encryption technology. Each master key and each subkey contains a public and a private key. Depending on the requirements, Guard automatically uses the respective key.
- *Public Keys* section. Displays the pubic keys shared by you or other users. If a user's public key is shown in this list, you can assume that this user can decrypt the encrypted e-mail messages that you send to this user.

The following functions are available:

- download your public key
- send your public key by E-Mail
- add new keys to your existing ones by uploading local keys or creating new Guard keys
- turn a key into the current key
- show details for a key
- delete a key
- download your private key
- add an additional E-Mail account to a key
- upload an external partner's public key

How to download your public key:

1. In the settings, open the page for administering the keys.
2. Click on **Download PGP Public Key** below *Your Keys*.

How to send your public key by E-Mail:

1. In the settings, open the page for administering the keys.
2. Click on **E-mail your PGP Public Key** below *Your Keys*.

How to add a new key to your keys:

1. In the settings, open the page for administering the keys.
2. Click the **Add** icon + next to *Your Key List* below *Your Keys*. The *Adding Keys* window opens.
3. You have the following options:
   - To add a private key, click on **Upload Private Key**. Select a file containing a private key. The *Upload Private Keys* window opens.

     To upload the new key, enter your Guard security password. Enter a new password for the new key.
   - To add a public key, click on **Upload Public Key Only**. Select a file containing a public key.
   - To create a new key pair, click on **Create New Keys**. The *Create Guard Security Keys* window opens.

     Enter a password for the new key. Confirm the password.

     The new key consists of a master key and a corresponding subkey.

   The new key will be entered on top of your key list. The new key becomes the current key.

How to make a key the current one:

You can use this function if your key list contains more than one master key and subkey. From now on, the current key will be used for encryption.

1. In the settings, open the page for administering the keys.
2. Below *Your Key List*, click the checkbox next to a key below **Current**. When turning a master key into the current key, the corresponding subkey will be marked as current too, and vice versa.

How to show a key's details:

You can get details for the keys. A key's details are especially useful for users with PGP knowledge.

1. In the settings, open the page for administering the keys.
2. Click the **Details** icon on the right side of the categories bar. The *Key Details* window opens. To view the key's signatures, click on **Signatures**.

How to delete a key:

1. In the settings, open the page for administering the keys.
2. Click the **Delete** icon on the right side of the categories bar. The *Delete Private Key* window opens.
3. The following options are available:
   - To revoke a private key, click on **Revoke**.

     Enter the password for the private key. If required, select a reason for revoking the key.

     Click on **Revoke**.
   - In order to delete a private key, click on **Delete**.

     Enter the password for the private key.

     Click the **Delete** button.

   When deleting a master key, the corresponding subkey will be deleted too.

How to download your private key:

Caution: Downloading a private key to your local machine can be a security risk. Make sure that no other person can get access to your private key.

1. In the settings, open the page for administering the keys.
2. Click the **Download** icon on the right side of the categories bar.

How to add an additional E-Mail account to a key:

When adding additional user IDs to a key, you can use the key for multiple E-Mail accounts.

1. In the settings, open the page for administering the keys.
2. Click the **Edit** icon on the right side of the categories bar. The *Add User ID* window opens.
3. Enter a name for the user ID. Enter the E-Mail address that you want to use for this key.
   Enter your password for this key.
   Click on **OK**.

How to upload an external partner's public key:

1. In the settings, open the page for administering the keys.
2. Click the **Add** icon on the right side of the categories bar. Select a file containing a public key.

Index