Guard
User Guide

Guard: User Guide

Publication date Wednesday, 23. March 2016 Version 2.2.0
Copyright © 2016-2016 OX Software GmbH , This document is the intellectual property of OX Software GmbH

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?
- Which Contents are Included in the Documentation?
- Further Help

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 unauthorized 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.

Further 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-Mails 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 are 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 be 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 to 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 making 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 sidebar.
   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 email** 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 exist:

- Reading encrypted E-Mails
- Sending encrypted E-Mails
- Access for external recipients

3.2.1   Reading encrypted E-Mails

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-Mails

The following options exist:

- Sending an encrypted E-Mail. Only you and the recipient 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 recognize 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 new E-Mail* page, click the **Encrypt** icon 🔓 on the upper right side.

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

2. In order to show further 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-Mails in html format.

3. Click on **Send secure**.

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

3.2.3   Access for external recipients

You can also send encrypted E-Mails to external recipients who are no groupware users. When initially sending an encrypted E-Mail to an external recipient, the following happens:

- A special account will automatically set up for the external recipient.
- You define whether the external recipient receives an automatically created notification about the encrypted E-Mail or a customized notification.
- The external recipient receives an E-Mail with the notification and an automatically created password.

  Depending on the groupware configuration, you can transfer a 4 digit pin to the recipient to secure the automatically created password.
- The external recipient receives an E-Mail with a link to the login page for the special account.
- The external recipient enters the automatically created password on the login page.

  Then, the recipient has to change the automatically created password. In order to be able to reset the account in case of a password loss, a security question and the proper answer has to be defined.

  The encrypted E-Mail is displayed.
- The external recipient can send an encrypted reply to the E-Mail.

When sending the next encrypted E-Mail to this external recipient, the following happens:

- The external recipient receives an E-Mail with a link to the login page for the special account.
- On the login page, the recipient enters the password set up when initially having received an encrypted E-Mail.

  If the recipient no longer remembers the password, a new password can be requested. To do so, the security question has to be properly answered.

3.3   Encrypting files

The following options exist:

- 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 last version of this files will be encrypted. All other versions will be deleted.

How to encrypt a file:

> **Warning:** When encrypting a file, all versions of this 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 menu bar. Click on **Encrypt** in the menu.

  You can also use the **Actions** icon ≣ in the *Viewer*. 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 further request.

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 toolbar. 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 drop 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 toolbar.

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 toolbar.
    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 toolbar.
    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-Mails, use the Guard default 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 having 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 sidebar, 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 sidebar, 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 sidebar, 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 email** field, enter the E-Mail address that is used for receiving a temporary password for resetting your Guard security password.

   Click on **Change email**.

3.5.2   Guard default settings

The default settings define the preset settings that are available when composing E-Mails. When composing a new E-Mail, the default settings can be adjusted before sending the E-Mail.

How to change the default 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 sidebar. Click on **Guard PGP Settings**.
3. Change a setting below *PGP Encryption Settings*.

The following settings are available.

Default to send encrypted when composing email

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

Default adding signature to outgoing mails

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

PGP default to using PGP inline for compatibility

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 can not send E-Mails 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 **Guard** Security in the sidebar. Click on **Guard PGP Settings**.

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.
- *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 E-Mails that you send encrypted to this user.

The following functions are available:

- download your public key
- send your public key per E-Mail
- add new keys to your existing ones by uploading local keys or creating new Guard keys
- download your private 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 per E-Mail:

1. In the settings, open the page for administering the keys.

2. Click on **Email 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✚ below *Your Keys* next to *Your Key List*. 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 will be entered below *Your Key List*.

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 upper right side.

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 upper right side. Select a file containing a public key.

Index

C
Change the password, 16
Create new encrypted files, 13

D
Decrypt files, 14
Documentation, 5
Download encrypted files, 14

E
Encrypt
   create new encrypted files, 13
   E-Mail conversation, 11
   Files, 13
Encrypt E-Mail conversations, 11
Encrypted E-Mails
   access for external recipients, 12
   block, 11
   read, 11
   send, 11
Encrypted files
   decrypt, 14
   download, 14
   Open, 13
Encrypting files, 13

G
Guard, 7, 9
   administer keys, 18
   default settings, 16
   security settings, 16
   set up, 10
   Settings, 16
   sign out, 15
Guard Guard PGP Settings
   Default adding signature to outgoing mails, 17
   Default to send encrypted when composing email, 17
   PGP default to using PGP inline for compatibility, 17
GuardSettings
   Change password, 16
   Reset the password, 16

O
Open encrypted files, 13

R
Reset the password, 16

S
Sign out
   Change password, 15