Guard

User Guide

Guard: User Guide

Publication date Monday, 08. December 2014 Version 1.2.0

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 the 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 OX App Suite 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 or external partners.
- Use the security options to define the encryption level.
- Define an expiry date or time for the encrypted data.
- The encrypted data are password-protected. Use the password reset function to protect against the consequences of a lost password.

3 Using the Guard

Learn how to work with the *Guard* application.

- apply basic settings
- encrypt E-Mail communications
- encrypt files and folders
- 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.
- To protect against the consequences of a lost password, you should set up the function for resetting the Guard security password by entering a secondary E-Mail address.

  Note: It is highly recommended to set up this function. If you do not set up this function and lose your Guard security password, you no longer have access to your encrypted data.

Instructions for changing or resetting the Guard security password can be found in Guard Security Settings.

How to initially set up the Guard security password for encryption:

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 Settings**.

   When initially selecting the Guard security settings, the *Create Guard 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. Click on **OK**.

How to define a 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 Settings**.
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**.

3.2 Encrypting E-Mail Communications

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.
2. Enter the Guard security password.

   You can set how long the encrypted E-Mail should be displayed as plain text. To do so, enable **Keep me logged into Guard**. Select a value from the list.

   The sender might have protected the E-Mail with an additional password. In this case, an additional input field will be displayed. Enter the additional password in this input field.
3. Click on **OK**.

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:

- send an encrypted E-Mail

  Warning: When sending an encrypted E-Mail draft, the draft will be deleted when being sent from the *Drafts* folder.
- to increase the security level, you can use further functions
- retract a sent encrypted E-Mail by blocking it.

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 top right side.

   You can also click on **Security options** on the left. Activate **Enable Guard**.
2. To further increase the security level, you can use further functions: set an expiry date or time, use an additional password
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.

How to use additional encryption functions when sending E-Mails:

Prerequisite: The *Compose new email* page is selected.

1. In the *Compose new E-Mail* page, click on **Security options** on the left side.
2. To further protect the E-Mail encryption with an additional password, enable **Require Additional Password**. The *Extra Password* window opens.

   Enter the additional password in the fields **Password** and **Confirm**. Click on **OK**.
3. To set an expiry date for the visibility of a encrypted E-Mail, select an entry from **Retract in**.

How to block an encrypted E-Mail:

1. Open the **Sent objects** folder. Select an E-Mail that you sent encrypted.
2. Click the **More** icon ≡▾ in the detail view. Click the **Retract** menu item. The E-Mail can no longer be read by the recipients.

3.2.3 Access for external recipients

You can also send encrypted E-Mails to external recipients who are no groupware users. In this case 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.
- External recipients then have to enter their E-Mail address and the automatically created password.
- When initially logging in to this account, the external recipient is asked to change the automatically created password. The encrypted E-Mail is displayed.
- The external recipient can send an encrypted reply to the E-Mail.

3.3 Encrypting files

The following options exist:

- Encrypting 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. In the *Drive* app, click on a file in the detail view. In the pop-up, click the **More** icon ≡▾ . Click on **Encrypt** in the menu.

   You can also select a file. Click the **More** icon≡▾ in the toolbar. Click on **Encrypt** in the menu.
2. The *Encrypt Files* window will be displayed. Confirm that you want to encrypt the file and delete all previous versions by clicking on **OK**.

3.3.2 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, click on a file in the detail view. In the pop-up, click on **Decrypt and Open**.
2. In the *Enter Guard Security Password* window, enter the Guard security password.

   You can set how long the encrypted file should be displayed unencrypted. To do so, enable **Remember Password**. Select a value from the list.

   Click on **OK**.

3.3.3 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, click on a file in the detail view. In the pop-up, click the **More** icon≡▾ . Click on **Download Decrypted**.

   Note: If you click on **Download** in the pop-up instead, the downloaded file remains encrypted.
2. In the *Enter Guard Security Password* window, enter the Guard security password.

   Click on **OK**.

3.3.4 Decrypting files

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

How to decrypt a file:

1. In the *Drive* app, click on an encrypted file in the detail view. In the pop-up, click the **More** icon≡▾ Click on **Remove Encryption** in the menu.

   You can also select a file. Click the **More** icon≡▾ in the toolbar. Click on **Remove Encryption** in the menu.

2. In the *Enter Guard Security Password* window, enter the Guard security password.

   You can define how long the Guard security password should be valid. To do so, enable **Remember Passwort**. Select a value from the list.

   Click on **OK**.

3.4 Signing out from 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 Security Settings

There are the following options:

- customize the Guard default settings
- change the Guard security password
- If you forgot your Guard security password, you can request a temporary password to be sent to your secondary E-Mail address by reset your Guard security password.
- change the secondary E-Mail address

How to change the Guard default settings:

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 Settings**.
3. Change a setting below *Defaults*.

The following settings are available.

Use Guard when composing a new email

Defines whether a new E-Mail is encrypted per default. Regardless of this preset option, you can define for each E-Mail whether it should be sent encrypted or decrypted.

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 Settings**.
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:

Note: Prior to being able to use this function, you need to have set up a secondary E-Mail address by using your 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 Settings**.
3. Click on **Reset Guard security password**. A new password will be sent to your secondary E-Mail address.
4. This new password is now your current Guard security password. You should immediately change this password.

Index