



Open-Xchange Guard Major Release v2.0.0

Feature Overview

V1.4

© 2015 Copyright Open-Xchange Inc.

This document is the intellectual property of Open-Xchange Inc.

The document may be copied in whole or in part, provided that each copy contains this copyright notice.

The information contained in this document was compiled with the utmost care. Nevertheless, erroneous statements cannot be excluded altogether. Open-Xchange Inc., the authors and the translators are not liable for possible errors and their consequences.

The names of software and hardware used in this document may be registered trademarks; they are used without warranty of free usability. Open-Xchange Inc. generally follows the spelling conventions of the manufacturers.

The reproduction of brand names, trade names, logos, etc. in this document (even without special marking) does not justify the assumption that such names can be considered free (for the purposes of trademark and brand name regulations).

Table of Contents

1	Objective of this Document	4
2	OX Guard PGP Mail Support – In General	5
2.1	In General	5
2.2	Advantages / Disadvantages of the current system.....	5
3	OX Guard PGP Mail Support – Function.....	7
3.1	General Function Overview of new PGP Support.....	7
4	OX Guard PGP Mail Support – Usability.....	9
4.1	General Handling	9
4.2	Sending encrypted Emails	9
4.3	Reading encrypted emails.....	10
4.4	Access for external recipients	10
4.5	PGP Encryption Settings.....	11
4.5.1	General Settings.....	13
4.5.2	Administering Keys.....	13
5	OX Guard Drive Support – Usability	14

1 Objective of this Document

This document provides an overview of the major new features that will be available in the OX Guard v2.0.0 release.

The objective of this document is to help Open-Xchange customers and partners understand the logic behind these features and changes, especially the reason for enhancements in usability.

2 OX Guard PGP Mail Support – In General

2.1 In General

OX Guard is a fully integrated security add-on to OX App Suite that provides end users with a flexible email and file encryption solution. OX Guard is a highly scalable, multi server, feature rich solution that is so simple-to-use that end users will actually use it. With a single click a user can take control of their security and send secure emails and share encrypted files. This can be done from any device for both OX App Suite and non-OX App Suite users. The browser-based reader for non-OX App Suite users is also perfect for advertising and viral user acquisition.

Based on customer feedback we have now implemented a solution using standard PGP encryption. With the release of OX Guard v2.0.0, Open-Xchange uses PGP for the encryption email and files.

2.2 Advantages / Disadvantages of the current system

Why was a proprietary solution used in the first versions of OX Guard?

- Open-Xchange held the content key (the AES key) separately enabling:
 - Retraction of files/emails
 - Expiration dates
 - Positive verification of when/if items are decoded
- Open-Xchange created the Public/Private Keys
 - This meant identity was essentially guaranteed, as it was associated with the OX account
- Simplification
 - Keys were centralized in Guard. There were no extra public repositories. This means:
 - Corrupt/expired/invalid/or malicious public keys in the public repositories are possible
 - Guard had a key, or it created one.
- Guest users were taken to our user interface creating upsell opportunities

The main disadvantage with using a proprietary solution was that it meant that email and files could not be opened by any system other than Guard. In addition, due to the

nature of how Guard managed the keys (for example for expiration and retraction), offline use was not possible.

3 OX Guard PGP Mail Support – Function

3.1 General Function Overview of new PGP Support

PGP has been around for a long time, yet really hasn't caught on with the masses. This is generally blamed on the barriers caused by the confusion and complications of managing the keys, understanding trust, PGP format types, and lack of trusted central key repositories. Guard simplifies all of this, making PGP encryption an easy one-click process, with no keys to keep track of; yet the options of advanced PGP management for advanced users that understand how to do this.

Guard minimizes these barriers to use by implementing the following:

- Very large, trusted PGP Public key store with Guard
 - All OX users with Guard installed will have automatic keys created
 - All Public keys are created from the account, so identity is certain
 - All public keys that are created by Guard will be shared with all users, through a standard PGP API
 - Public keys uploaded by a user (unverified) are shared within the context only
 - Guard servers query each other through DNS record and the HKP protocol.
- Hides most of the PGP Public key complexity for most users. If Guard has a PGP Public key for the recipients, it will just use it. If it does not have the key it will mark the recipient and create a "Guard Guest" account for the user just as it does now.
 - Guest users will get an email with the password and link as before.
 - The Guest user, once logged in, will be able to download his/her public/private key that was created for them, or upload their preferred public key for future emails. Users who don't know about PGP will just use the Guest account as before to read / reply.
 - Guest users, with PGP knowledge, can have the email sent directly to them in PGP format rather than as a Guest link
- Users can download their PGP keys to use with their offline email clients (Thunderbird, GPG Mac Mail, etc.)
- Advanced users, after being verified through their OX App Suite login, can upload their own PGP Public key to be used for encryption, keeping their PGP Private key locally for their personal use. For example:

- Private keys used with Thunderbird or Mac mail
 - Drive clients, if applicable, could access Private Keys on the local machine
- Keys held either in centralized location, or possibly associated with address book

4 OX Guard PGP Mail Support – Usability

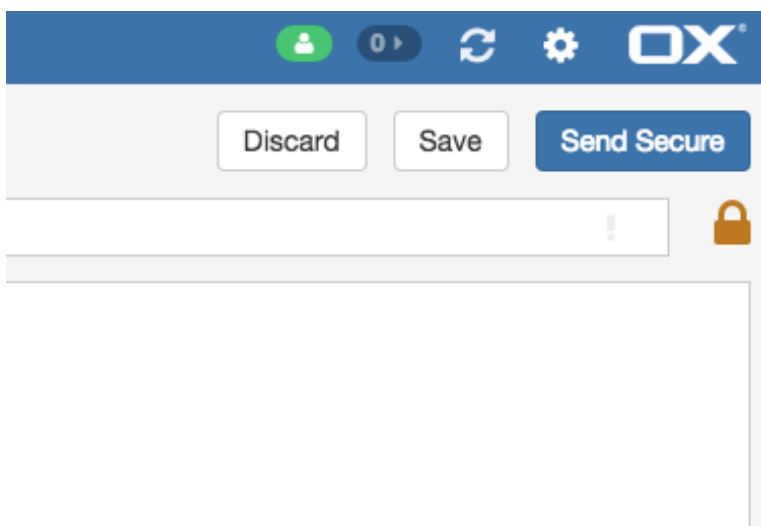
4.1 General Handling

By creating a solution as outlined above, Open-Xchange hopes to create a PGP experience be very similar to current OX Guard experience. As before the user sends an encrypted email by just pressing the lock symbol. Advanced users can manage the keys directly, but for the general user, everything will just be managed in the background. OX Guard thus makes PGP accessible to the masses, while allowing advanced users the ability to manage their keys and even withhold their private keys from OX Guard.

4.2 Sending encrypted Emails

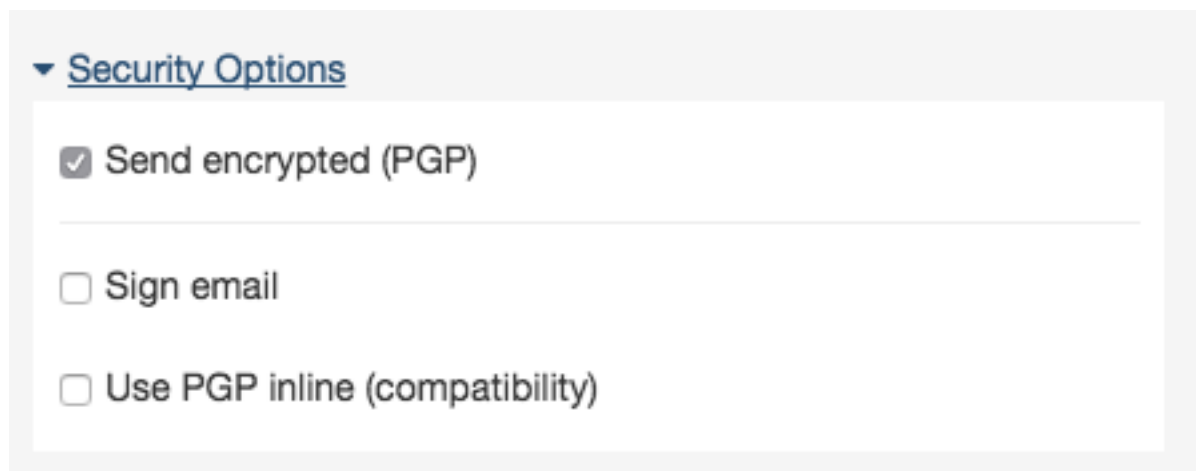
OX Guard v2.0.0 provides a completely new sending concept based on PGP. The following options exist:

- Sending an encrypted email. Only you and the recipient can read the email content.
- Sending an Email along with a signature. The signature ensures that the recipient is able to recognize whether the email content has been changed during transport.
- Sending an encrypted email with a signature.



From the compose new email page the user has to click on the encrypt icon in the top right corner. It is also possible to click on security options on the left of the window. In this area, the user can also enable Guard. In order to sign the email the user simply has to enable the "Sign email" checkbox.

By default, Guard sends emails using PGP Mime, which is the most robust and standardized way to send PGP emails. For compatibility with some older systems, Guard can also send PGP emails using PGP Inline.



When sending email to external recipients, a dialog within OX App Suite is displayed, that allows the creation of an additional message for those recipients when they receive an encrypted email.

4.3 Reading encrypted emails

In order to read an encrypted email the Guard security password is required.

When the user selects an encrypted email, indicated by with encrypted icon, it is necessary to enter the Guard security password in the detail view.

The user can define how long the security password remain active. **Please Note:** Replies to encrypted emails have PGP encryption automatically enabled.

4.4 Access for external recipients

Users can send encrypted mails to external recipients (like Gmail, Yahoo etc.) who are not OX App Suite users. When sending an encrypted mail to an external recipient, the following happens:

- A special account will automatically be set up for the external recipient.
- The sender defines whether the external recipient receives an automatically created notification about the encrypted mail or a customized notification.

- The external recipient receives an email with the notification and a system generated password (secure and random).
- Depending on the OX App Suite and Guard configuration the sender can also send a 4-digit pin to the recipient to provide additional security to the system-generated password.
- The external recipient receives an email with a link to a login page (Guard Guest Mode) for the special external account.
- The external recipient enters the system-generated password on the login page.
- After this the recipient has to change the system generated password. In order to be able to reset the account in case of a password loss, a security question and the correct answer has to be specified.
- The encrypted mail is then displayed.
- The external recipient can then send an encrypted reply to the mail.

4.5 PGP Encryption Settings

OX Guard v2.0.0 now has a new settings page in the user settings. From this page the user can change the following general options:

- Administer the Guard security password from the Guard security settings.
- Change the default settings for sending secure emails from the Guard default settings.
- The user can administer the PGP keys.

PGP Encryption Settings





- Default to send encrypted when composing email
- Default adding signature to outgoing mails
- PGP default to using PGP inline for compatibility

Your Keys

[Download PGP Public Key](#)

[Email your PGP Public Key](#)

Your Key List

Key ID	Private Key	Current	Details	Delete	Download
4d3c030	✓	✓			
↔ 730ecbe2	✓	✓			

Public Keys

PGP Public Key List

No Keys Found

[Guard PGP Settings](#)

4.5.1 General Settings

The first settings on the page are as follows:

- Default to Guard PGP when composing email
 - Defines whether all new emails get encrypted with PGP by default.
- Default signing of outgoing PGP mails
 - Defines whether all new email is signed with PGP by default.
- Use PGP inline (compatibility)
 - Defines whether encryption is done via the "PGP inline" implementation. Users should only use those settings if the mail client of the recipient does not support PGP MIME. For example "mailvelope" users will require the email in PGP inline format.

Note: Due to limitations in the "PGP Inline" specification the user cannot send emails in html format.

4.5.2 Administering Keys

In order to send or receive encrypted messages the administration of keys is typically not required. However the following functionality is supported by OX Guard v2.0.0. if required:

- If the user wants to use their private Guard PGP keys in other mail clients, e.g. in local mail clients, it is possible to download the private PGP key.
- If the user has PGP keys from other PGP applications, these keys can be uploaded
- The user has an external partner's public key. In order to send encrypted messages to this external partner without having to access a key server, he can import the partner's public key into Guard.
- The user wants to provide his public key to a recipient to receive encrypted emails; public keys can be downloaded or attached to emails here.

5 OX Guard Drive Support – Usability

OX Guard v2.0.0 will support "one person only" encryption. This means that a file can be encrypted by an OX App Suite user, but only for his own usage. For example, an ID document could be uploaded to OX Drive and then encrypted. But only the OX App Suite user himself can decrypt it.

It is not possible to encrypt the file with multiple public keys (for example for other users like in email). If the user would like to share an encrypted file for multiple public keys he should send it via encrypted email to the corresponding contacts.