



OX Guard
Release Notes for Release 2.0.0

July 1, 2015

Copyright notice

©2015 by Open-Xchange AG. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of Open-Xchange AG. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

1 Shipped Product and Version

Open-Xchange Guard 2.0.0-rev6

Find more information about product versions and releases at http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering

2 General information

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 to 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.

PGP has been around for a long time, yet has not really caught on with the masses. This is generally blamed on 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 as easy as a one click process, with no keys to keep track of, yet the options of advanced PGP management for those that know how.

A more detailed overview of all the new features and improvements to OX Guard v2.0.0 can be found here:

http://software.open-xchange.com/products/guard/doc/OX_Guard_Product_Guide_2_0_0.pdf

3 Bugs fixed with this Release

This document provides a summary of bugfixes and changes that have been applied subsequently to shipping Release 1.2.0. Some of the announced bugfixes may have already been fixed at the existing code-base via Patch Releases.

38014 Issues with decrypting mail

While decrypting mail, their ID has been internally mapped to Integer values. If that ID value exceeds 2.147.483.648, the corresponding mail could not be decrypted. This has been solved by handling IDs as strings, which do not have those limitations.

36923 Guest welcome messages are not translated

When configuring users to a non-english language, Guard welcome mails for guests have still been sent in english. The users language settings were not taken into account correctly. This has been solved by accessing the correct configuration parameter when generating welcome mails.

38265 Resetting user passwords via command line triggers errors

When trying to reset a users password via Guard command line tools, an error was thrown. This was caused by assuming that the user has a secondary mail address configured, but the user had not. The reset process now checks if that address is set and if it can be used to deliver the new credentials.

38564 Printing encrypted mail prints placeholder text

The print functionality triggered the OX backend to print the encrypted version of the E-Mail, which obviously led to undesirable results. Now the print content will contain the decoded content of the E-mail.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #2600 Introduction of new Guard capabilities

The following capabilities have been added and are optional:

- `com.openexchange.guard.externalReaderURL` (Configure the url for the external reader links)
- `com.openexchange.guard-norecovery` (Disables password recovery)
- `com.openexchange.guard-nodeleterecover` (Disabled the users ability to delete their recovery)
- `com.openexchange.guard-nodeleteprivate` (Disables the users ability to delete their private PGP key. Can retract only!)

Change #2603 Introduction of new configuration options in the `guard.properties` file

Additional config options are required for PGP support in Guard 2.0.

Change #2604 Support for HKP in Guard 2.0

If Guard 2.0 needs to act as a PGP public key server, then additional proxy options will need to be added to Apache `mod_proxy` or other load balancer. The URL of `domain/pks` should be directed to the `guardserver/pgp`.

Change #2605 Introduction of DNS based PGP keyserver lookups

The proprietary Guard DNS lookup in the TXT record is no longer supported, as the proprietary Guard 1.x format is being phased out. PGP standards are supported, with a SRV record for `_hkp._tcp.domain` to enable other Guard and PGP services to look up the Public keys from the Guard server.

4.2 Changes of Database Schema

Change #2606 Introduction of DB tables

The requirements for Guard 2.0 are less than 1.2, as each encrypted item does not take up a database entry. Storage requirements are essentially just the keys. New tables created for uploaded PGP keys. New table for PGP Public key lookup created in the main Guard database. This is used to locate public keys based on their fingerprint. In order to add the additional database tables and update the lookup table, an upgrade process is required. Instructions here http://oxpedia.org/wiki/index.php?title=AppSuite:OX_Guard#Update_1.2_to_2.0

4.3 Changes of Behaviour

Change #2597 PGP Support

All encryption will be now done with PGP. Decrypting the Guard 1.0/1.2 proprietary methods is still supported. Encryption with Guard 1.0/1.2 proprietary methods is no longer supported. With the change to PGP, email expiration date, status or read/unread emails, and retracting is no longer supported. Sharing files within the context by adding multiple keys is no longer supported. PGP encrypted files are specific to the user only PGP. PGP Mime and PGP Inline is now fully supported. Guard is now able to act as a hkp compliant PGP Public key server.

Change #2598 Introduction of new support API

New support API enabled that allows support teams to reset passwords, delete accounts, and recovery deleted accounts. Detailed documentation available on <http://www.oxpedia.org/>.

Change #2607 Enhancements for handling Drive files + eMail MIME data

Guard 2.0 now handles Drive files entirely in stream. Emails, however, are fully loaded in memory

to create proper MIME bodies. Therefore, memory requirements are based on the (number of simultaneous emails x (max Email size) x 3) + base footprint. This is an improvement over Guard 1.2 which also required space for full file processing.

4.4 Changes of Packaging

Change #2599 Introduction of an additional backend package / bundle

The package `open-xchange-guard-backend` is now required for the OX backend. This package must be installed on all OX backend servers that are Guard enabled.

Change #2601 Requirement for JAVA JCE package

Guard 2.0 now requires the Java Cryptography Extension unlimited strength installed. This is default with many Linux installations, but may be an additional install. Guard 2.0 and its PGP encryption will otherwise fail, if not installed.

5 Tests

The Open-Xchange QA team has successfully verified all bug fixes that could be reproduced within a lab environment.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup for system and integration testing.

All changes have been checked for potential side-effects and effect on behavior. Unless explicitly stated within this document, we do not expect any side-effects.

6 Fixed Bugs

38014, 36923, 38265, 38564,