OX Guard
Release Notes for Release 2.4.2

July 13, 2016

Copyright notice

1 Shipped Product and Version

Open-Xchange Guard 2.4.2-rev4

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 now supports the concept of ”Basic” and ”Advanced” users. It is recognized that most people are not encryption experts, and some of the features and terminology in Guard that were designed for advanced encryption users were confusing to normal users. This is why OX Guard now offers easy-to-use functions for basic users and advanced options for professional users. In addition, OX Guard adapts its terminology to the target audience with different terminology for basic or advanced encryption users. A more detailed overview of OX Guard v2.4.2 can be found at: http://software.open-xchange.com/products/guard/doc/OX_Guard_Product_Guide_2_4.2.pdf

Announcements
Open-Xchange encourages administrators to regularly update to the latest available release. In order to ensure a stable and up to date environment please note the different supported versions.An overview of the latest supported Major, Minor and Public Patch Releases can be found in the Knowledgebase at: http://oxpedia.org/wiki/index.php?title=AppSuite:Version_Support_Committment

3 Bugs fixed with this Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Release 2.4.1. Some of the announced bugfixes may have already been fixed at the existing code-base via Patch Releases.

43939 Unclear description of PGP inline
In case a user has selected HTML E-Mail composing and enables PGP-inline, a warning is shown since compatibility is not guaranteed. Using specific workflows enabled the user to use both configurations without warnings. This has been solved by catching those cases and display warnings as well.

45245 Wrong signature used when replying to a encrypted mail
App Suite allows to define separate signatures for new mails and replies/forwards. This concept has now also been implemented with Guard to make sure users are getting consistent behaviour regardless of plain or encrypted communication.

46280 Google fonts service used by external Guard reader
The external reader of OX Guard contained references to the fonts.googleapis.com service. To avoid external dependencies and privacy issues, we’ve changed this to load the required font from the external reader itself.

44910 French translation does not fit password box
When changing a OX Guard password, the description within the password field did not fit the input box. This has been solved by using a dynamic width and height.

46286 Typos at british english translation
The dialog to create a OX Guard keyspair was lacking dots at the end of sentences. This was solved by providing proper translation.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3307 Add a configuration for user to default to advanced or basic
As we are now introducing a new Guard setting for the user to see Advanced options or not, the default for this value should be configurable. The property `com.openexchange.guard.defaultAdvanced` (Default: `true`, but not enabled) has been added to `guard-core.properties`.

Change #3313 Add seperate trusted and untrusted Public PGP Key Server configuration
There are scenarios, such as with Grouped Guard servers, where trusted key servers are known, compared to the public PGP key servers that are unverified. How these are handled should be different. Trusted keys can be used to verify signatures, where the untrusted public keys should only be trusted after user verification. Configuration at `guard-core.properties` has been changed and `com.openexchange.guard.publicPGPDirectory` got superseeded by `com.openexchange.guard.trustedPGPDirectory` (Default: empty) and `com.openexchange.guard.untrustedPGPDirectory` (Default: MIT public HKP servers).

Change #3318 New basic authentication configuration properties for mail resolver
OX Guard uses the REST API credentials for accessing the default mail resolver. It was not possible to define separat credentials if a customer implemented an own mail resolver. New properties got introduced to `guard-core.properties`, `com.openexchange.guard.mailResolverUrl.basicAuthUsername` (Default: empty) and `com.openexchange.guard.mailResolverUrl.basicAuthPassword` (Default: empty).

4.2 Changes of Behaviour

Change #3357 New background task for deleting expired authentication tokens
OX Guard 2.4.2 allows attaching an authentication token to a middleware session. In order to prevent that authentication tokens become orphaned in the Guard DB (for example due to a restart of a middleware node), a maximum lifetime of an auth-token is required. OX Guard now schedules a background task on a daily basis which deletes expired authentication tokens. A new configuration property has been introduced to `guard-core.properties` which defines the maximum lifetime of an authentication token: `com.openexchange.guard.authLifeTime` (Default: `1W`).

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

43939, 45245, 46280, 44910, 46286,