



**OX Guard**  
**Release Notes for Release 2.10.2**  
2019-05-15

## Copyright notice

---

©2019 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. 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 General Information

### OX Guard v2.10.2 for OX App Suite v7.10.2

- With this new release, Open-Xchange integrates OX Guard even more closely with OX App Suite, particularly when composing and reading emails.

### What's New in General and Feature Overviews

- Open-Xchange now provides more detailed overviews and Feature Overview documents relating to new product releases. These can be found at <https://www.open-xchange.com/portfolio/whats-new/>

### General Information – Please Note

- Open-Xchange encourages administrators to regularly update to the latest available release. To ensure a stable and up to date environment please note the different versions supported. 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](http://oxpedia.org/wiki/index.php?title=AppSuite:Version_Support_Committment).

## 2 Shipped Product and Version

Open-Xchange AppSuite guard 2.10.2-rev3

Find more information about product versions and releases at [http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning\\_and\\_Numbering](http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering) and <http://documentation.open-xchange.com/>.

## 3 Vulnerabilities fixed with this Release

This section provides a summary of security related bug fixes that have been applied subsequently to shipping Release 2.10.1. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

**64992 CVE-2019-11521**  
CVSS: 5.3

## 4 Bugs fixed with this Release

This section provides a summary of bug fixes and changes that have been applied .

### **61893 Guard Guest Accounts gives Timeout or Mails are not shown**

This was caused by a timeout because guest sessions were not synced between servers. Now guest sessions are synced between hazelcast server.

### **62076 Replies to Guard emails broken**

When replying to an encrypted email, the compose dialog shows the ENCRYPTED mail rather than the proper decrypted content. This also breaks the Guest replies. This is limited to Customer that have the feature setting `io.ox/mail/features/fixContentType=true`.

Now it is possible to reply to Guard emails also `io.ox/mail/features/fixContentType` is "true".

### **62258 ics file can't be impoted from attachment if mail was encrypted**

Added support for importing encrypted ical files.

**62575 Second and Consecutive Messages to External User not Localized**

During the login process, Guard checking if the language selection in the Guard key table was different from the language selection of the UI, and if different, then updating. This allows Guests, to change their language and have it updated for new Guest emails. But null wasn't being handled. This has been fixed by also handling NULL and invalid values for languages.

**63175 NPE at com.openexchange.guard.auth.LoginHandler.login**

Fixed handling of null or invalid locale string in Guard keys.

## 5 Changes relevant for Operators

### 5.1 Changes of Configuration Files

**Change #SCR-333 Autocrypt service configuration**

The following is added to the guard-core.properties file:

- `com.openexchange.guard.autoCryptEnabled=true`
- `com.openexchange.guard.autoCryptMutual=true`
- `com.openexchange.guard.keySources.trustLevelAutoCrypt=2`
- `com.openexchange.guard.keySources.trustLevelAutoCryptUserVerified=5`

**Change #SCR-360 Add lean configuration for sessionSyncDelay**

Guard servers verify that a session is valid before allowing most actions. Guard queries a middleware server with the session information to confirm the user is logged in a valid. If, due to load balancing, etc, the Guard server queries a middleware server not currently handling the user session, there may be a race condition between the hazelcast sync and when Guard queries the middleware. New lean configuration added (`com.openexchange.guard.sessionSyncDelay`, default:3000). If the middleware is unaware of the session, Guard will wait this period of time before trying again.

**Change #SCR-443 Additional configuration for webkey lookup service**

With 2.10.2, Guard will additionally search for keys using the webkey/webdirectory standard. This looks up keys for the user by searching for keys in a published directory. A hash of the users email (before domain) is used. The keys are searched in `domain/.well-known/openpgpkey/hu/HASH`. Trust level for this needs to be declared for Guard:

- `com.openexchange.guard.keySources.trustLevelWKSServer=3`
- `com.openexchange.guard.keySources.trustLevelWKSSRVDNSSECServer=4`

### 5.2 Changes of Database Schema

**Change #SCR-104 Added table to store guest email meta data**

A new table `GuestEmailMetaData` is created for storing non-confidential meta data of guest emails. For example folder-id, subject, size, dates, content-type, message-flags, color-flags, etc. OX Guard will only store non-confidential data parsed from the headers of the encrypted mail. The data is used for querying a guests user's mail folder based on certain criteria.

**Change #SCR-332 New database table required for PGP public keys found in Autocrypt headers**

Autocrypt headers contain the public keys of the sender. These keys need to be treated differently

from other public keys, as they are more limited (only single userId, no trust signatures), and are not as fundamentally trusted as imported keys. Therefore, a new database table is created to store these keys for users

**Change #SCR-346 New datatype for og\_KeyTable.lastmod**

The type of og\_KeyTable.lastmod is now "datetime" to store additional time information.

## 6 Tests

Not all defects that got resolved could be reproduced within the lab. Therefore, we advise guided and close monitoring of the reported defect when deploying to a staging or production environment. Defects which have not been fully verified, are marked as such.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server set-up 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.

## 7 Fixed Bugs

61893, 62076, 62258, 62575, 63175, 64992,