OX Guard

Release Notes for Release 2.10.0

2018-07-04

Copyright notice

Contents

1 General Information

OX Guard v2.10.0 for OX App Suite v7.10.0

With this new release, Open-Xchange integrates OX Guard even more closely with OX App Suite, particularly when composing and reading emails. Enhancements to the OX Guard platform in this release include:

- Updated web interface for external users (now uses regular OX App Suite Mail Frontend)
- Share encrypted files

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/.

2 Shipped Product and Version

Open-Xchange Guard 2.10.0-rev7

Find more information about product versions and releases at 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 2.8.0. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

58258 CVE-2018-10986
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N), Credits to Secator

4 Bugs fixed with this Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Release 2.8.0. Some of the announced bug fixes may have already been fixed at the existing code-base via Patch Releases.

58503 Originating IP header missing for Guard Mails
When sending mail with OX Guard, the `X-Originating-IP` mail header was missing, even though configured to be added. This has been solved by considering the appropriate configuration option.

58431 Timeout when sending mails with huge attachments
In case a encrypted mail contains a huge attachment, timeouts could strike on slow mail systems. To work around this, we're introducing the option `com.openexchange.guard.endpointTimeout` (Default: `15000`). See SCR-171 for more details.

58230 Guest users with PIN are not recognized
In case a guest user logs in using a PIN the first thing that showed up was a request to change the password - which the user did not have. We're now considering ”password-less” users.

58157 Confusing error messages when using a PIN

In case of entering a wrong PIN, the German error message is misleading. We've updated the translation to a more useful wording.

57636 Encrypted files in Drive with uppercase file type name

An encrypted file in Drive with uppercase file type name couldn't be previewed. We now handle file extension for encrypted files case insensitive to solve this issue.

57436 Guard not uploading public key

The public key upload dialogs was not working properly with Microsoft Edge. This has been fixed by changing order of dialog handling.

56796 Incorrect sender address used for password reset

When resetting a users password, that users primary mail address was used as sender. Now the values defined at `com.openexchange.guard.passwordFromAddress` and `com.openexchange.guard.passwordFromName` are used instead.

56640 Signature key related errors when decrypting mail

If the decryption was successful, but Guard did not understand the signature algorithm, the signature was ignored. This has been fixed by allowing decryption with unknown signature types.

56376 Incompatibilities with client-side encryption

Client-side encryption solutions were not working anymore due to a regression. We solved this to regain compatibility even though such solutions are not officially supported.

55961 Added one-to-one mapping for HKP

To support additional scenarios, we added a one-to-one mapping for public keys and mail addresses.

55843 Unencrypted reply on encrypted email is not possible

When setting `com.openexchange.guard.secureReply=false` a ”reply” to an encrypted email would result in a encrypted reply. Now the reply to an encrypted mail is no longer enforced to be encrypted too when setting this option.

55553 Unable to open encrypted mail in ”Sent”

In case users have the capability to use OX Guard for Mail but not for Drive, a error was raised if users tried to decrypt their own sent mail. This has been solved by considering users to be eligible to use OX Guard if either one of those capabilities are set.

55019 Passwords with leading spaces are not recognized

If users chose to set a password with leading whitespace, that password was not recognized during the authentication process. We now make sure to strip whitespace before evaluating a password.

54728 Glitches when dealing with re-created users

When deleting a former OX Guard users and sending internal mail after re-creating that user, no new keys were being created for the ”new” user. This has been fixed.

54727 Missing support for secure HKP servers

We now query for HKPS (secure HKP) servers using DNS service records. This allows to retrieve PGP public keys over a secure channel.

52637 Unable to print encrypted mails

Encrypted mails could not be printed after decrypting. This has been solved.

5 Changes relevant for Operators

5.1 Changes of Configuration Files

Change #4488 Change in configuration for Guest cleanup

New configuration setting `com.openexchange.guard.guestCleanedAfterDaysOfInactivity` (Default: `365`) is added to the guard-core.properties file. The old configuration `com.openexchange.guard.cacheDays` is no longer used.

Change #SCR-171 Configuration option for connection timeouts to OX App Suite

We've added a property to `guard-api.properties` to specify a HTTP timeout for connections from OX Guard to OX App Suite in milliseconds: `com.openexchange.guard.endpointTimeout` (Default: `15000`).

Change #SCR-116 New configuration in `proxy_http.conf` required for "webkey" service

The webkey service is a method for mail clients to look up public PGP keys. When looking up an email like joe.doe@example.org, the client will assemble a URL consisting of `https://` plus the domain `example.org`, followed by `/.well-known/openpgpkey/hu/`, followed by a Z-Base32 hash of the username "joe.doe". This URL then provides access to the users PGP public key and requires a new entry at `proxy_http.conf` to map it to a OX Guard endpoint:

```
ProxyPass /.well-known/openpgpkey/hu balancer://oxguard/hu
```

Change #SCR-101 Enabled setting to delete password recovery by default

`noDeleteRecovery` is a setting for OX Guard which disables a users ability to delete their password recovery. While we think users should be able to delete their recovery for extra security, there are some clients that may require this to be disabled. The default behavior has been changed in a way that password recovery removal is enabled by default and can be disabled if required.

Change #SCR-83 Add configuration to Guard S3 to set signature version

Additional configuration setting required to allow specification of signature version for S3 access. Settings for signer override already existed at OX App Suite middleware, but was missing for OX Guard. The following option has been added to the `guard-s3.properties` file: `com.openexchange.guard.storage.s3.signerOverride` (Default: `empty`). and can be used to specify a custom S3 signer type.

Change #SCR-80 Configurable trust levels of public key sources

OX Guard does now provide a configurable trust-level for each "key source" from where a recipient's public key can be retrieved from. A configurable threshold value defines if a "key source" is considered to be "trusted" or "untrusted". Information about the recipients key trustworthiness are now shown in the email compose dialog: The fingerprint of the key, the creation date of the key, the source of the key, and whether or not the key is considered to come from a "trusted" source. The following new configuration properties were introduced to `guard-core.properties`:

- `com.openexchange.guard.keySources.trustLevelGuard`
- `com.openexchange.guard.keySources.trustLevelGuardUserUploaded`
- `com.openexchange.guard.keySources.trustLevelGuardUserShared`
- `com.openexchange.guard.keySources.trustLevelHKPPublicServer`
- `com.openexchange.guard.keySources.trustLevelHKPTrustedServer`
- `com.openexchange.guard.keySources.trustLevelHKPSRVServer`
- `com.openexchange.guard.keySources.trustLevelHKPSRVDNSSECServer`

Change #SCR-30 Add configuration setting for mail `FROM` at SMTP Envelope

The mail `FROM` header was set to the guest's email address when sending through the guest SMTP relay server. This caused issues if the SMTP server requires a known user, and potentially causes issues with SPF checks at the recipient side. The following Configuration Setting has been added to specify a custom `FROM` address, if necessary: `com.openexchange.guard.guestSMTPMailFrom` (Default: `empty`).

5.2 Changes of Database Schema

Change #SCR-115 New column for webkey hash storage
The webkey service requires an additional column at the `oxguard.og_email` table to store pre-computed user hashes for remote lookup. A database update-task will create this column and a separate thread runs in the background to populate this column.

5.3 Changes of Behavior

Change #SCR-117 OX Guard guests now use OX App Suite guest mode
Previously recipients of encrypted emails which did not publish a public PGP key had to use a separate user interface for mail communication. This behavior has been changed fundamentally by using OX App Suite ”guest mode”. Guest users will receive a E-Mail with invitation, similar to a notification about shared files, that allows them to log into OX App Suite. They will then have a temporary mailbox provided by OX Guard, listing encrypted emails they have received so far. While appearance is similar to a regular OX App Suite account, its limited to reading mail and replying.

Change #SCR-102 Removed optional PIN for OX Guard guests
In case the capability `guard-pin=true` was configured there existed an option to add a 4 digit pin when sending mail to OX Guard guest users, used as credential to log in. We moved OX Guard guests closer into OX App Suite and removed this functionality. Guests that still have PINs assigned will be pointed to the legacy OX Guard guest interface to have their PIN checked but then replaced with proper credentials and redirected to their new OX App Suite guest account

Change #SCR-100 Support API and CLT for upgrading OX Guard guests to full users
Changing the way OX Guard guest accounts are being handled had impact on upgrading guests to full user accounts. We no longer require user accounts to be migrated as they already exist at OX App Suite guest mode. Therefore, a new CLT and support API call has been created to allow administrators to upgrade a OX Guard guest account to a full user while maintaining their PGP key-pair. Assume guest user@domain is being upgraded to a full account with id 3, context 4:

CLT: `/opt/ox/sbin/guard -u [user@domain.com|mailto:user@domain.com] --context 4 --id 3`

Support API: `/guardSupport?action=upgrade_guest&email=user@domain&cid=4&user_id=3`

This process copies all keys from the OX Guard guest account to the new full OX App Suite user.

6 Tests

Open-Xchange 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 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

58503, 58431, 58230, 58157, 57636, 57436, 56796, 56640, 56376, 55961, 55843, 55553, 55019, 54728, 54727, 52637, 58258,