

E2EE - Administration

- System Configuration
 - License Installation
 - Key Storage Options
 - Access Restrictions
 - Enforce End-To-End-Encryption
 - Multiple Keys
 - Server-Side Encryption
 - Simple Share
 - Wizard Visibility
 - Status Report
 - Administrative Note
 - occ Commands
 - e2eeshare:list-keys
 - e2eeshare:add-key
 - e2eeshare:delete-key

System Configuration

As Admin user you will find the E2EE settings in the *Encryption* section of the Admin Settings.

Encryption

License Installation

Copy/paste your license key and click on *Change License* to install a new one or update it.

License Key

```
-----BEGIN LICENSE-----
MjR0OUppqYm9BZ3dSd3F5OV1KK2xUdCdWc0lw5XMvSHBKNXIwb1FrOGREvH1UZ1RvYU45TFhOd1Z6
Zmd2YXFje2hYQmJFd2Z0SDFqSEIxQS93M0JVUh1tNWZlWnZCbzNZU2EyZmN6WVRweER0dzYreHBR
WfhzUFdFbGRHeTdML0NxYktzUWdHeitFeG1SdfZyb2dwS010WnZ3RHNNK2VTejhRRDdEd3ZzaJdy
MDVSK01KY2E5NXFXc1ZHb1V5eT1P6WFTd01UVXRXWtRnNVVQMzVnbHfuTUV2NUM00FEvQT1zWXNp
NkowQmVnbDeyNGxKQ0pR3nYz5TMvL2xBbDVRMDbhQ2VGR0V0Q25haDNVU0RZWXF1NjBtM116aVo4
TDU0U1E9PTtkVDB5TURJd01EVXd0enRrUFd4d1kyRnNhRz16ZER0b1BUTXpORE00T1RBME9HSTRO
ekpoT1RNek1EQXldak0wWkRje1pqaGpNamxtWkRBNVpXWmpOVEE3WXoweE1EdGxPdZ0900VvU0tF
cEJPcnRaV it0UX1TQWt2bmtJSnRQUT0=
-----END LICENSE-----
```

Change license

Your license is active until May 7, 2020

You will see until when your license is active and for how many users.

Key Storage Options

Select, which key storages will be available for your users. You may provide different settings for ownCloud and guest users.

Key Storage

Select below which private key storages are provided for e2ee Users.

ownCloud Users

- ☐ User's Computer/Device
- ☒ External Key/Smartcard
- ☒ Manual input for each download
- ☒ Local decryption, download only

Guest Users

- ☒ User's Computer/Device
- ☐ External Key/Smartcard
- ☒ Manual input for each download
- ☒ Local decryption, download only

If you provide more than one key storage options, users must set up their key storage in their personal settings prior to being able to read and save encrypted files. This must be communicated in advance to avoid any confusion.

The handling of the private key is - from a security perspective - the most important part. The private key must be kept safe but still be used when you want to decrypt data.

There is a clear trade-off between security and usability, depending on which option you want:

	Description	Usability	Security
User's Computer/Device	The private key is stored in the browser local storage (similar to a cookie)	★★★	👍
External Key/Smartcard	The private key is available through an external process running on the client machine. Then the browser can only request decryption. You have to install an extra Key Server on your machine, which is able to both recognize provided key files or Smart Cards (currently Windows only). The key is never saved in the browser. The Key Server supports reading the key from a storage location (.pem file) or from a pkcs#11 compatible hardware device.	★★★	👍👍👍
Manual Input for each download	When downloading an E2EE file, the private key has to be copy/pasted into a browser form. The key is never saved in the browser.	★	👍👍
Local decryption, download only	The E2EE file is downloaded locally and a secondary tool is required to decrypt (E2EE Reader). The E2EE Reader supports both file and Smart Card decryption (currently Windows only). The key is never saved in the browser.	★★★	👍👍👍

General remarks about security:

- Even with access to a server backup no data can be decrypted (you need a private key)
- Access to a private key only allows to decrypt that users data
- When a private key is removed, all decryptable information is purged from the server (i.e. even if recovered, it cannot be used to decrypt data any more)

Access Restrictions

By default all users are enabled to use the E2ee app. If you want to restrict usage to specific groups only, you may set them in the *Authorized Groups* section. If you provide one or more groups here, only members of those groups may set a folder as E2ee encrypted. Click the apply button, when you are done.

Authorized Groups

✕ admin

By default all users are enabled to use the E2ee app.

If you provide one or more groups here, only members of those groups may set a folder as E2ee encrypted. (guests and E2EE enabled (virtual group) are virtual groups and cannot be selected).

Apply E2ee Groups

The authorized groups will be applied when a user logs in for the first time.

To see exactly how many users are enabled to use the E2EE app, you may click the *Apply E2ee Groups*. After a reload the Summary section shows the number of currently enabled users.

Summary

Your license is active until May 7, 2020 for oc3.oem-cloud.com

E2ee Share is activated for 6 of 100 possible users.

Request Admin Report

Enforce End-To-End-Encryption

You may configure a system wide setting where it is only allowed to upload e2ee files. To enable, set the e2eeshare key `enforced_e2ee` to `true` in your `config.php`. When you want to exclude some groups from this behavior, add them comma separated as value for `enforced_excluded_groups`.

A configuration snippet with e2ee enforced and the groups admin and helpdesk excepted looks like below

config.php

```
'e2eeshare' =>
    array (
        'enforced_e2ee' => true,
        'enforced_excluded_groups' => 'admin, helpdesk'
    ),
```

Multiple Keys

Allow multiple keys



Allow multiple keys per user.

Checking this option means, that multiple private key

Users can only have one public key assigned to them by default. This is a security feature. If you want users to have multiple keys (i.e. one for each of their device or for backup purposes) you may enable this option.

Server-Side Encryption

For those cases where it is necessary that users can upload files via ownCloud client to an e2ee encrypted share, there is an option to permit uploads of unencrypted files.

In that case any files dropped into a local folder will be sent unencrypted to the server. When https is enabled for the site the upload will be still encrypted via Transport Layer Security. The file on the ownCloud server is encrypted immediately and the original contents is replaced. The original upload is unencrypted on the ownCloud server for a very short time however. This is a convenience feature an administrator has to weigh up based on business requirements.

To enable this feature check the box *Permit upload of unencrypted files*.

Permit upload of unencrypted files

☒ Permit upload of unencrypted files

Simple Share

To simplify the end-to-end-encryption workflow, a private key can be created when sharing with a new user. This private key will be stored AES encrypted in the database and new users will receive an email with the password.

Upon first login new users unlock the initial private key with the password and a new key pair will be created. Shared files are reencrypted with the new key on the fly and the initial private key will be deleted.

The password itself is only delivered by email and never stored.

Simple Share requires the **key storage *User's Computer/Device* enabled** for both guests and ownCloud users. It cannot be enabled unless both of the storages are enabled.

Be sure that the share **recipients have got valid email addresses** (check the *Users* page) or the email providing the private key password can never be sent. This affects ownCloud users only since for guest users the email address is required for invitation.

When a user did not receive or lost the password for the initial private key it cannot be resent. To have the user receive a password again, remove all shares with this user and recreate them. Then a new initial private key will be generated and the new password will be sent to the user.

To enable this feature check the box *Enable Simple Share*:

Simple Share

☐ Enable Simple Share.

Wizard Visibility

By default, after login, all users are shown the key generation wizard unless they generated their encryption keys.

There is an option to only show this wizard to certain group members. Define one or more groups in Show key generation wizard, then only for those group members the wizard will pop up.

All other users still can generate their keys in Personal Settings -> Security.

Show key generation wizard

wizard x

By default after login all users are shown the key generation wizard unless they generated their encryption keys.

This setting is active when **no** groups are selected in the above input field.

When you define one or more groups here, **only for those group members** the wizard will pop up.

All users still can generate their keys in Personal Settings -> Security.

Status Report

Request Admin Report

You can generate a status report of your E2EE installation by clicking the button in the *Summary* section: The report will be mailed to the logged in administrator's email address. It includes the current license information such as the number of enabled users.

Administrative Note

This functionality provides an information text area which is shown on top of every users' E2ee Section in the Personal Settings. You may use this, for instance, for a detailed guide about the setup or contact information.

When the text area is left blank, nothing will be shown.

Administrative note

You may provide some additional information to your users. When this text area is not empty, its contents will be shown in the end-to-end encryption panel of a user's personal settings page

A user guide and proposed settings are available at e2ee documents.

If you need specific support, please call our helpdesk at 0123 456 789

Save note

occ Commands

As an administrator you might want to perform certain operations by using scripts. The following commands are available:

e2eeshare:list-keys

Show all public keys for the provided user

Syntax

```
sudo -u www-data php occ e2eeshare:list-keys <user>
```

e2eeshare:add-key

Add a new public key to provided user

Syntax

```
sudo -u www-data php occ e2eeshare:add-key <user>  
<local-path-to-public-key>
```

e2eeshare:delete-key

Delete a public key from provided user

Syntax

```
sudo -u www-data php occ e2eeshare:delete-key <user> <key id>
```

e2eeshare:encrypt-folder

Convert an unencrypted folder to an e2ee encrypted folder.

```
sudo -u www-data php occ e2eeshare:encrypt-folder <user> <path>
```

where path is absolute from a user's root directory, e.g. /Documents