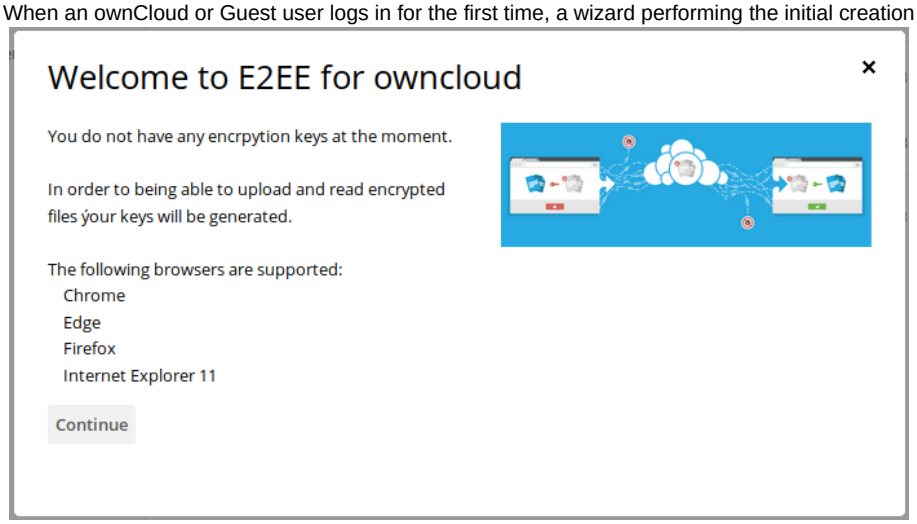
E2EE - Encrypted Sharing of Files

Share with ownCloud Users, Groups or Guest Users

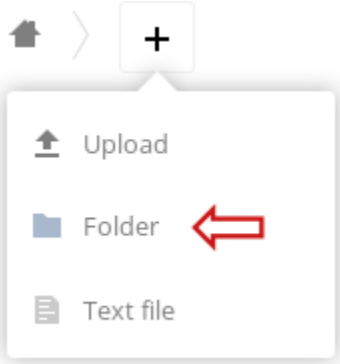
It only takes some simple steps to share files using End-to-End-Encryption:

1. When an ownCloud or Guest user logs in for the first time, a wizard performing the initial creation of the keys is shown

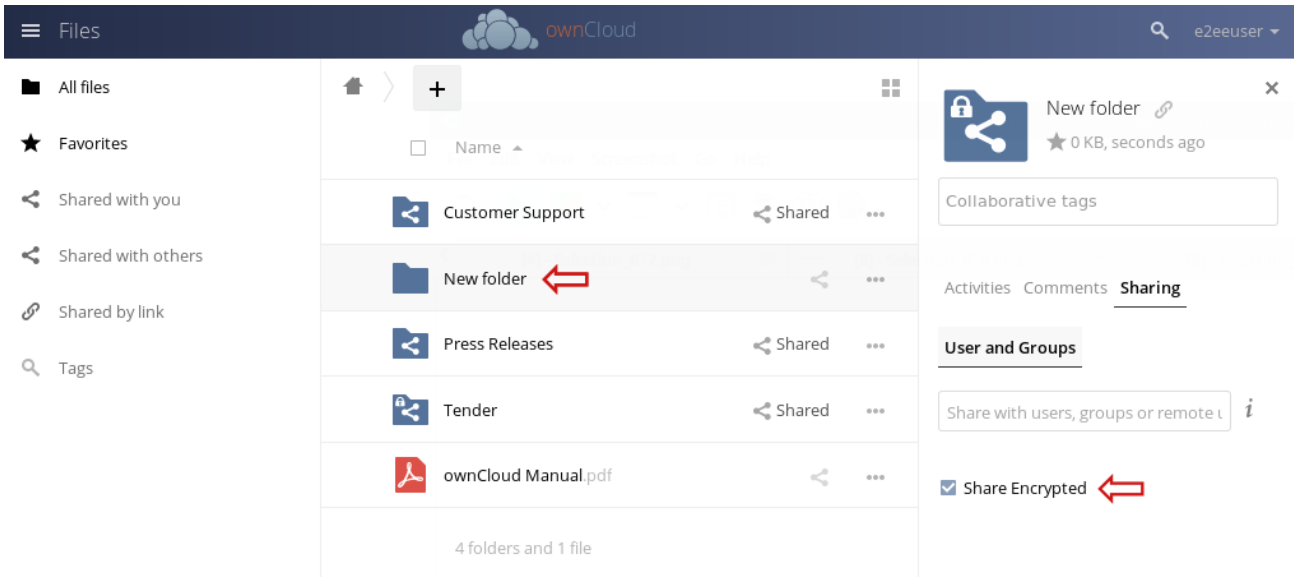


   Detailed information about the setup process is found in the E2EE - User Manual

2. Create a folder which should contain encrypted files. Single, previously uploaded files cannot be converted to encrypted files.

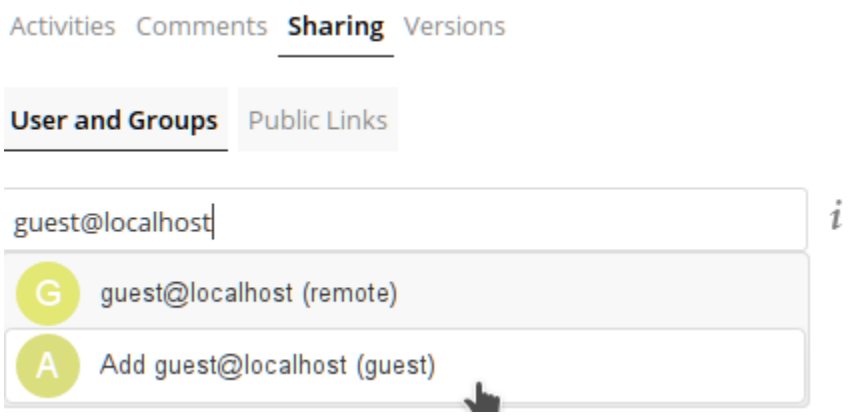


3. Open the folder's *Sharing* properties and check the *Share Encrypted* option to enable encrypted sharing.



If you start uploading right away, the files will be encrypted for you only. If you want to share files with other users, make sure to invite them and double check, if they have a valid public key in the system.

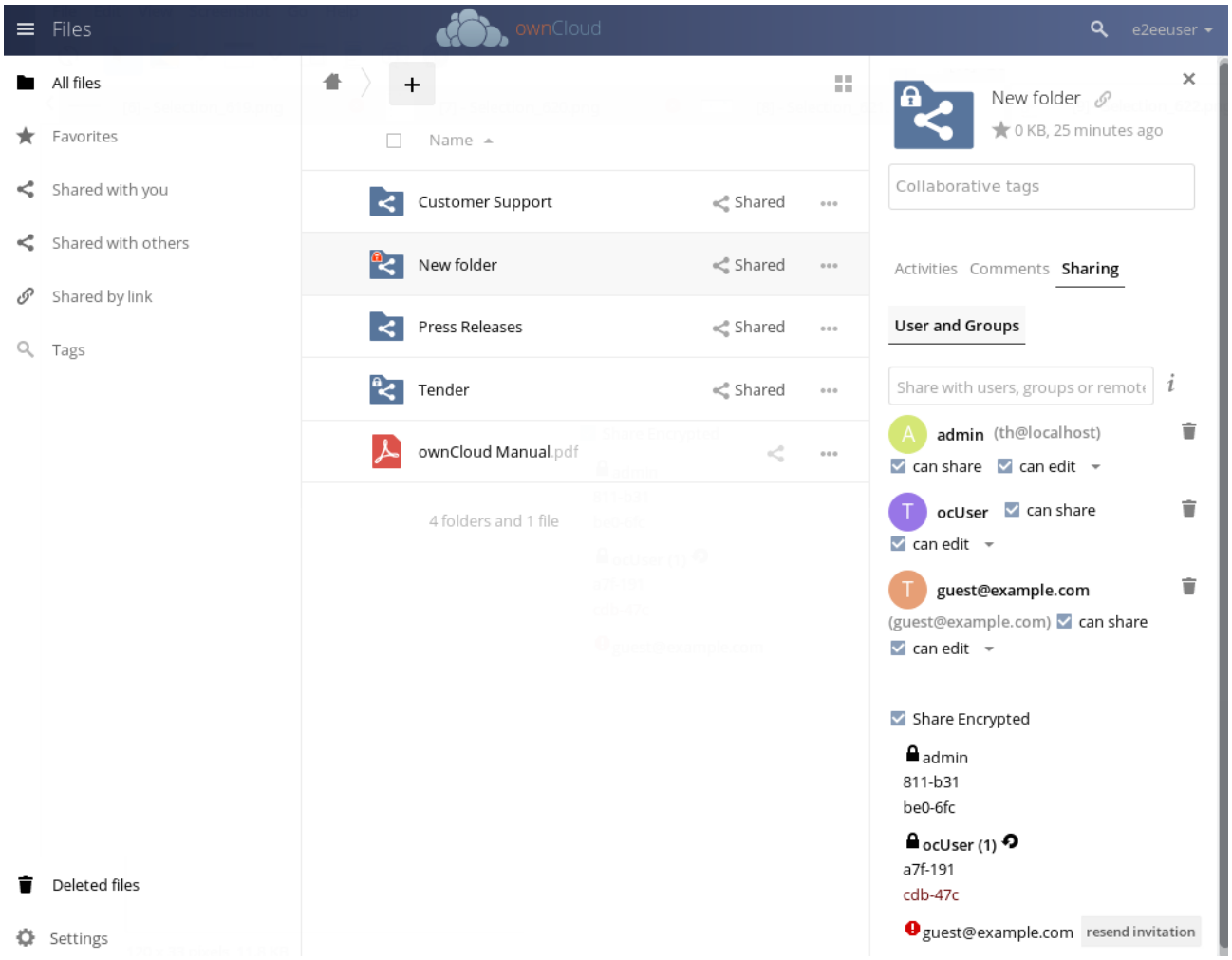
4. Next you need to share this folder. Add ownCloud users, groups or guest users the same way you would do in a standard ownCloud installation by entering the user name into the *Share with* input field or by inviting a guest user by entering the email address:



If you shared with a guest user, you will receive an email notification **once the guest has logged in the first time** (and thus created the key). You may spot this in the Sharing tab as well, when the user name is shown with a lock symbol instead of an exclamation mark symbol (see *Sharing* tab below). Only then **it makes sense to start uploading files**.

If you add an **existing ownCloud or guest user** who already has got keys all files in the **directory will be re-encrypted on the fly** so the users can read them instantly. When sharing with a group, files will be re-encrypted for all group members.

5. Once a folder is shared you can view the details in the *Sharing* tab



In this screenshot you see the file list (middle) and the *Sharing* tab (right) for the folder *New Folder*.

Share Tab View

Users who have got **at least one key** are indicated with a black lock symbol

Users who **do not have any keys** are indicated with a red exclamation mark symbol

When sharing with one or more groups, all group members will be listed.

Below each user a list of abbreviated key ids is shown fore reference, when you move the mouse pointer over it the full key id is shown.

If a user has generated a new key after a file was uploaded to the directory, this key is missing in the folder and therefore that user would not be able to open the mentioned file without re-encrypting the folder.
In this case the user name is shown bold, followed by the number of new keys in the parentheses. The **missing key id is shown in red color**.

As a Sharer, by clicking the arrow button

next to the user name you can **re-encrypt the folder**, which adds the new keys. A confirmation window will open, indicating how many files would have to been re-encrypted.

Guest users receive an invitation email upon sharing with them for the first time. As long as they have not yet registered the

resend invitation

button is shown. By clicking this button the original invitation email containing the login credentials are resent to that user.

File List View

Every folder, which is shared encrypted carries a lock symbol in the folder icon.

A white lock indicates that the folder is **encrypted for all keys** for all users the folder was shared with.

A red lock indicates that at least for one user **at least one key is missing**.

Share with Groups

Sharing end-to-end-encrypted with groups is done the same way as with the ownCloud default.

- When users are added to a group and they already have got keys, all group shares will be re-encrypted on the fly, so they can see and open the shares immediately.
- When users are removed from a group, all their keys are removed so they immediately cannot see (and open) the shares any longer.
- When you share with a user AND with a group, where this user is a member of and you remove the share with the group the user still can see and open the share since the single share remains untouched
- When you share with a user AND with a group, where this user is a member of and you remove the share with the user the user still can see and open the share as long this user is member of the group

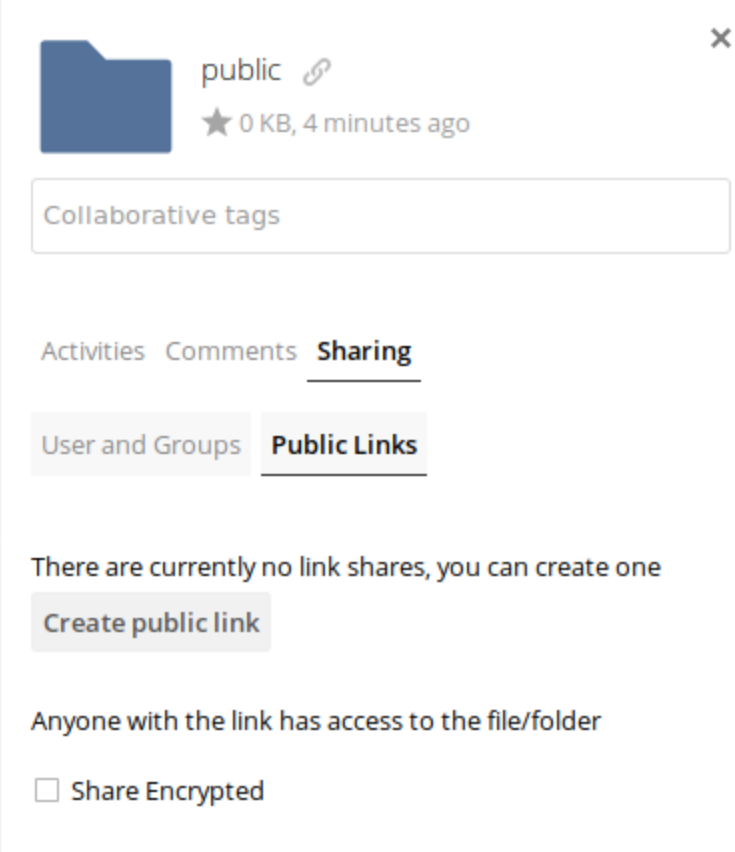
Share with Public Links

Starting with version 1.3.0 it is possible to have files, uploaded to a public share, end-to-end-encrypted. The uploaded file will be encrypted with the share initiator's public keys.

There is no way uploaders can add their keys, so the files can be opened by the recipient only.

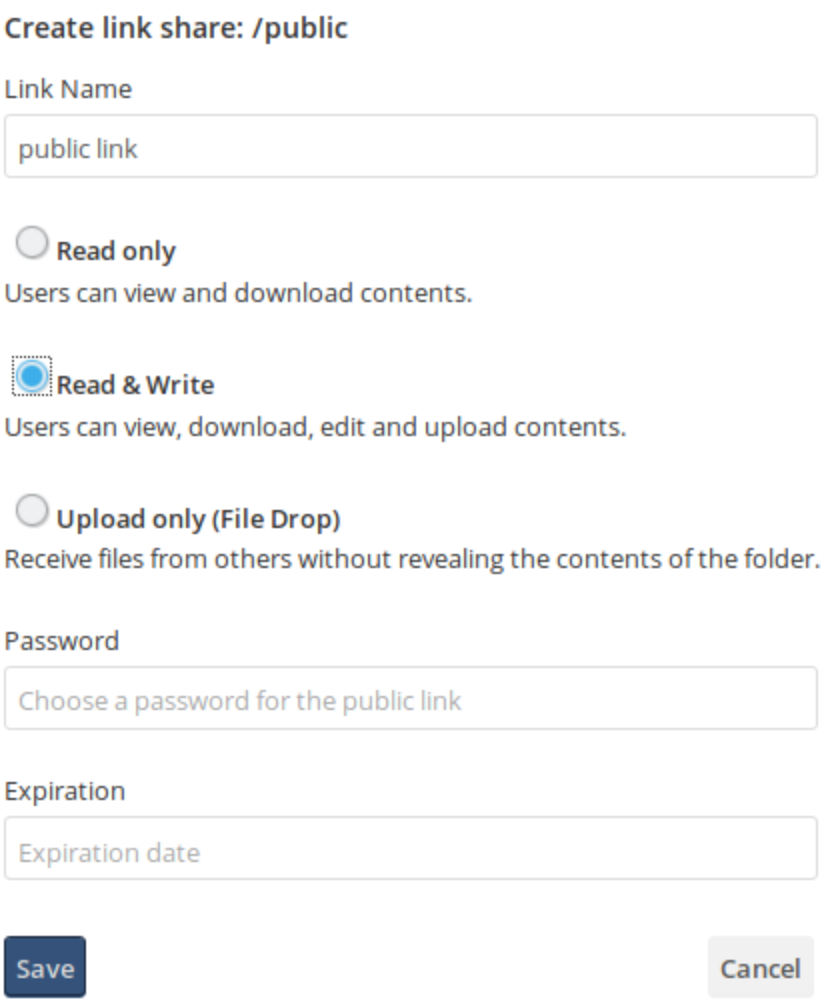
E2EE for Public Links is set up in three little steps:

1. Create a folder and open its *Sharing* properties:



2. Create a public link and make sure, that the share is writable by users, i.e. choose **Read & Write** or **Upload only**:

> When choosing **Read & Write** public users can see their and previously uploaded e2ee-files and even download them. However, they would not be able to open them since they never have a private key to decrypt.
>
> If uploaded files should be invisible to your share recipients, choose **Upload only (File drop)**



3. Mark the folder as an e2ee folder by clicking the **Share encrypted** checkbox

> While drag and drop is supported for logged in users (even guest users) this feature is not available for public link shares.