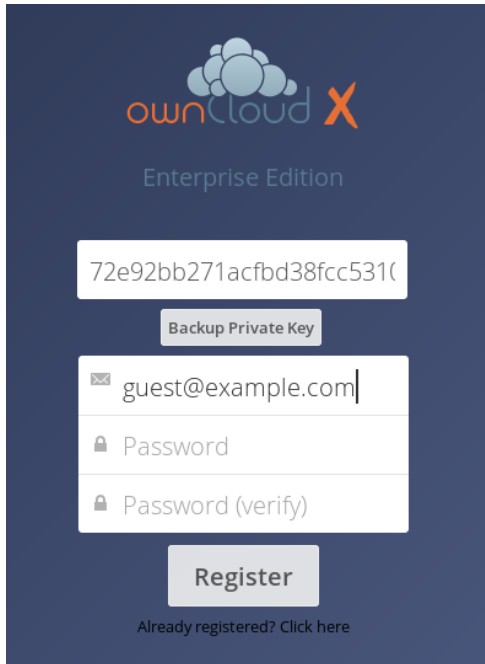# E2EE - Guest User Manual
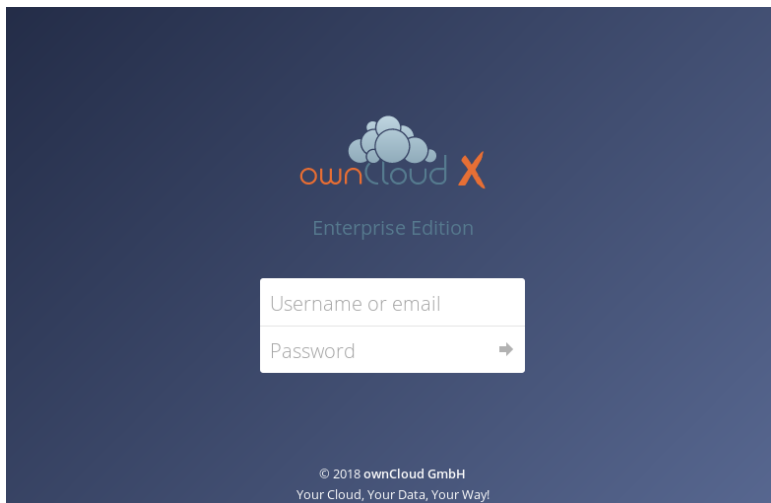
In order to register with a guest account you need to set a password on the provided registration page. The link to that page (e.g. http://mycompany.tld/oc/index.php/apps/e2eeshare/register/oEOsFpFZVD55HmT4MtKl4/guest@example.com) is sent by email after having shared a folder with a guest for the first time.

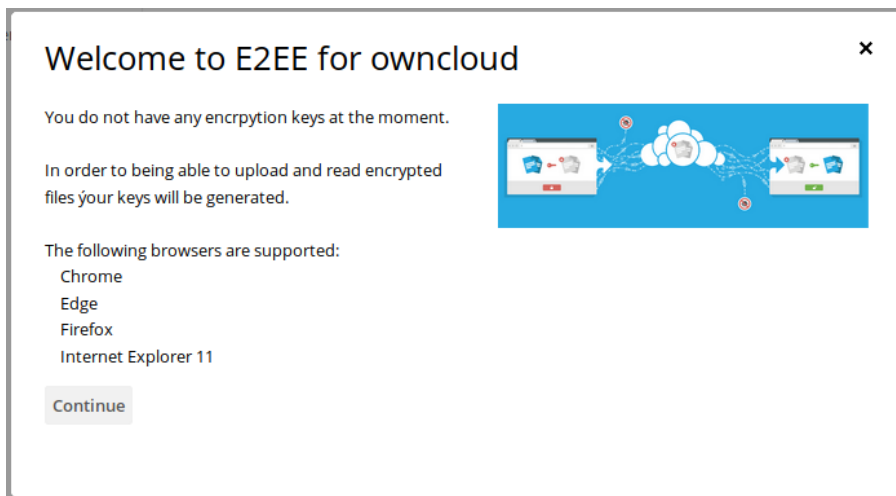For Registration you just have to enter and confirm the password.

After Registration the user will land at the default ownCloud login page.

At first login a wizard will open which guides through the creation of a key pair for encrypting and decrypting files.

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

After setup, you can upload encrypted files using the *Upload* menu item. All files uploaded will only be readable the owner of the folder and all users the owner shared this folder with.
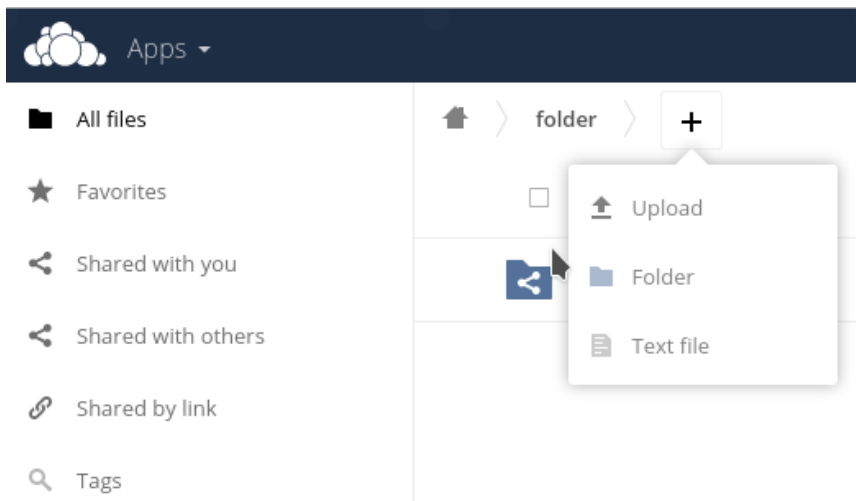
You can only view files AFTER you registered. Anything what was uploaded before is not viewable with your private key without further actions by the sharer.

Settings / Key Management

E2eeShare settings are found in the *Security* section of the Personal Settings panel.

Depending on the server setup, there you can generate a new private key or download the current one.

Settings ▾   testuser ▾

Personal

👤 General

📁 Storage

🔒 Security

••• Additional

E2EE Share
Key Management
───

E2EE Share allow you to share End-To-End encrypted files with other users or create encrypted shares.
Note that since these are encrypted on your local hardware, there is no way for the server or server administrators to recover the data if you have lost your private key

Local Key

Public Key ID: f55adef6d5b30faea26bb5289aca6e43

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA1PRh8SzfPPLry04YFcnw0UednSesoR71eGjLNsSToLP6GGxp
                                            ...nc0H9R06UNjaAR
                                            ...UY1AkTaoqtUn
                                            ...CSVNSE/x3rw3vPA
                                            ...sPUfjHG+
                                            ...6d1w50i
W-                                          ...lIWlSJA
cB                                          ...iGsTNFC
2A                                          ...uJrxtnq
RCP                                         ...VRayPhi
b20                                         ...f4LwHj4P
E9BmV                                       ...iW6fms
mFe0Y                                       ...PNAHiUCP
9es7                                        ...fAoGBAKnS
xBG                                         ...Db7dOc+UE
vGt+                                        ...y0kD4/6RT
dail                                        ...9+y1IYJzB
Kyt0P                                       ...xUqJYbdMY
1/DhC                                       ...uirnPGAu
ds7EF                                       ...14rbx1J
vs7                                         ...oebhuCm
WGF             ...rtuvJLDQ2TyPMzoK
od6FltkCQYApGVRP3PN000iZZzhqSBBEMVUUhooizawnW+0efGd0YYpGm69SzZNN
C+r5SWroYsMhRIMKnj2hLGhSiWbcrfcFXvHAjQJ0GHTvrz+oaT1p1NSklpG83m7a
kprnrwM4siafv+rACIkBws25RwMqJ0EfqiKPHhsXmjPcAseCsa9TTw==
-----END RSA PRIVATE KEY-----
```
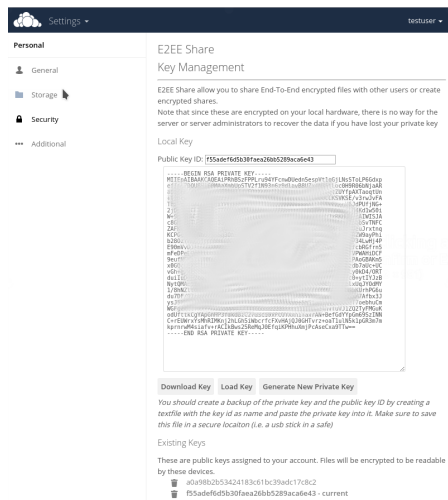
[Download Key] [Load Key] [Generate New Private Key]

You should create a backup of the private key and the public key ID by creating a textfile with the key id as name and paste the private key into it. Make sure to save this file in a secure locaiton (i.e. a usb stick in a safe)

Existing Keys

These are public keys assigned to your account. Files will be encrypted to be readable by these devices.

🗑 a0a98b2b53424183c61bc39adc17c8c2
🗑 f55adef6d5b30faea26bb5289aca6e43 - current

The key management is the same as for non guest users. You find all instructions at E2EE - User Manual.

> If you see more keys than you added by yourself, or your current key does not match any more, notify the administrator immediately as this is a sign of an incursion attempt.