

# E2EE - User Manual

- User Setup (default wizard)
- Key Storages
  - External Key/Smartcard Configuration
  - All other storages
- User Setup (Simple Share)
- Key Management
  - Manage Existing Keys
  - Key Management depending on your Key Storage
    - Your Computer/Device - Local Key
    - Key Storages Manual input for each download and Local decryption
- Decrypting Files
  - Your Computer/Device
  - External Key/Smartcard
  - Manual input for each download
  - Local decryption

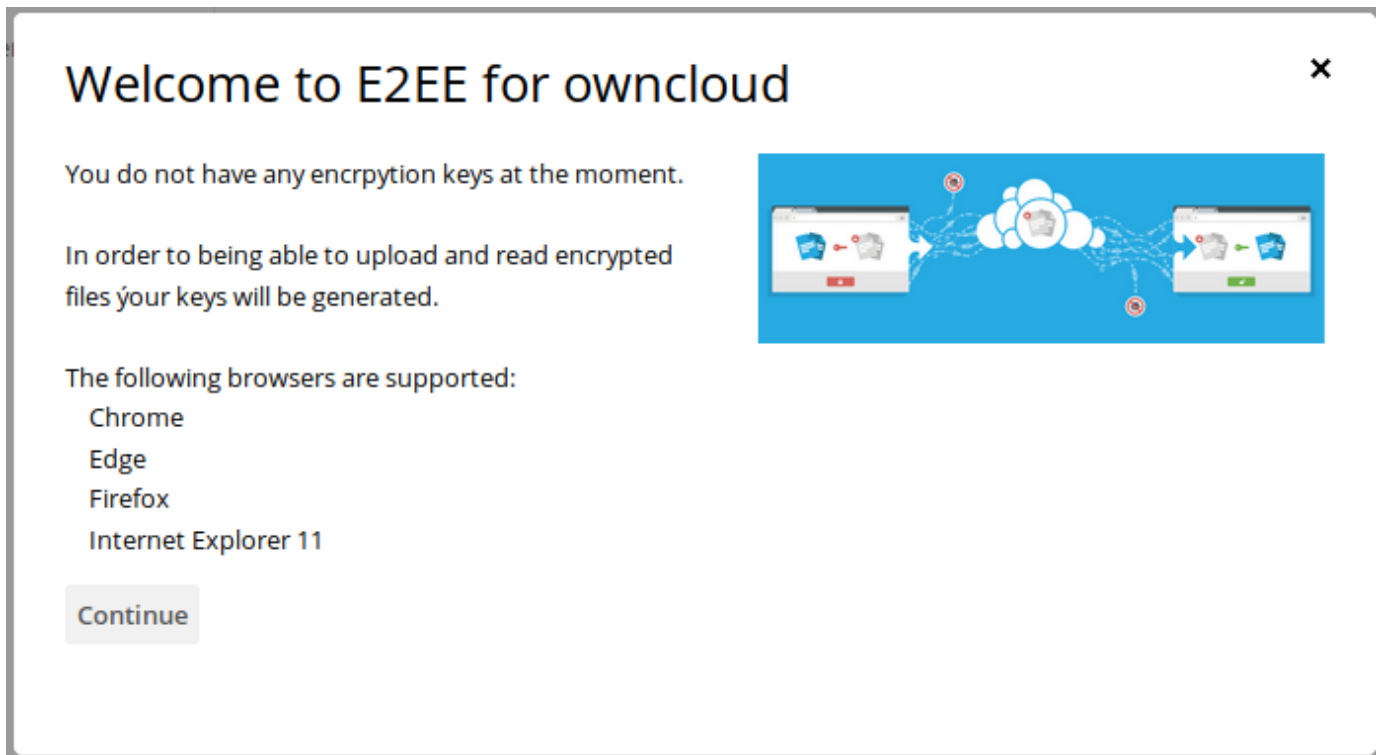
At first login a wizard will open which guides through the creation of a key pair for encrypting and decrypting files. This pair comes with a private (secret) key and a public (not secret) key.

- The **public key** will be used to encrypt files
- The **private key** will be used to decrypt files

While the public key will be saved in the server's database ("anybody may encrypt files for me"), the private key must be kept secret ("only I may decrypt files").

Depending on the server administrator's configuration you will see the default wizard or the Simple Share wizard.

## User Setup (default wizard)



After the welcome screen you choose the key storage, where your keys will be saved.

The select box provides all available key storages, as they were set up by the administrator.

# Select your key storage



The key storage defines the way you want to provide access to your private key.

Select your key storage ▼

Save Storage

Select your key storage

Your Computer/Device

External Key/Smartcard

Manual input for each download

Local decryption, download only

Depending on the system settings you can choose if and where the private key is saved and how you want the decryption to be performed. This depends on your security requirements and possibilities:

|                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Usability | Security |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------|
| Your Computer/Device           | The private key is stored in the browser local storage (similar to a cookie)                                                                                                                                                                                                                                                                                                                                                                                                          | ★★★<br>★  | 👍        |
| External Key/Smartcard         | <p>The private key is available through an external process running on the client machine. Then the browser can only request decryption.<br/>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).<br/>The key is never saved in the browser.</p> <div>The Key Server supports reading the key from a storage location (.pem file) or from a pkcs#11 compatible hardware device.</div> | ★★★       | 👍👍<br>👍  |
| 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               | <p>The E2EE file is downloaded locally and a secondary tool is required to decrypt (E2EE Reader).<br/>The E2EE Reader supports both file and Smart Card decryption (currently Windows only).<br/>The key is never saved in the browser.</p>                                                                                                                                                                                                                                           | ★★★<br>★  | 👍👍<br>👍  |

## Key Storages

### External Key/Smartcard Configuration

For the *External Key/Smartcard* key storage, a key server URL has to be provided. In most cases this will be the default value <http://localhost:9080>.

## Key Storage

Key Server ▼

## Key Server

Key Server URL:

By clicking the *Test Connection* button you will receive a message whether the key server was found or not. You will be asked to register your Smartcard when it had been found.

An additional button *Connection Info* will show up which either opens the key server's status information or a browser error page, in case the key server did not respond.

## All other storages

Except of the variant External Key/Smartcard, where the key is retrieved from the hardware, in any other keys a new key pair will be generated.

The public key will be uploaded to the server's database, the private key is shown in the next step.

## Generate Keys

This is your private key. Be sure to save it to a safe place.

Your storage method is: **Your Computer/Device**  
The key was saved in your local storage.

It is required to save the key to be able to recover in case of a computer crash or if you want to decrypt files from another device.

Key Id:

-----BEGIN RSA PRIVATE KEY-----  
MTTFnOTRAAKCAGFA1bFk1dD0IiQ7hI DnQ7uFhzi rCnMaCrYnk7ive /rAuh1bHDn

From now on you are able to create or read end-to-end encrypted files.

**Be sure to save the private key** and store it at a secure location (e.g. in a safe). Make a backup of this key. Without the private key you cannot open any files, e.g. when the web browser was reinstalled.

**The private key is never sent to the server.** The private key cannot be restored.

In case this key is lost, you have to create a new one. However, you only can access files encrypted for your old key when

- You re-upload the files
- Another user who shared an encrypted folder with you re-encrypts it for your new key.

For key storage **Your Computer/Device** you can **only use one browser or browser profile for one account**. Since the private key is

stored in the browser (or the profile) a different ownCloud user would receive the message *Your key was not found on the server*, because the stored private key does not match the other user's public key.

After you are done with the wizard, the key management is always available in your **Personal Settings - section Security**

## E2EE Setup finished

You now can upload and open encrypted files

Whenever you want to change your settings, add or revoke a key, this can be done in your personal settings.

Do you want to see these settings now?

No thanks, I'll look later

Yes, take me there

Click **Yes, take me there** to find the section Security in your Personal Settings.

User can have multiple private keys assigned to their accounts i.e. for multiple devices. Files uploaded into one of their encrypted folders will automatically be encrypted for ALL of their private keys.

## User Setup (Simple Share)

When the server administrator had set up Simple Share, then a password protected private key was already generated, so you can open your shares shortly after login. You have received your key password by email. When the wizard below appears, please enter or paste the provided password:

Welcome to E2EE for ownCloud

Your encryption keys are being created now, this might take a moment.

Do not close this window unless the Done button appears!

Enter your Key Password

Continue

A new key pair will be generated where the private key is only stored in your device's browser and never sent to or retrieved from the internet. The setup process is finished when you reach the following page:

Your keys are ready!

It is required to save the key to be able to recover in case of a computer crash or if you want to decrypt files from another device.

Backup Private Key

Continue without saving (dangerous)

Key Id:

9e5a2a7a7bbcceb747167971ca8a072e

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzOMiBFFaxJu0zPw7xgn4VUq2j+jKn1h+FWt/qVewfaGx2+vK
BN4sYeJ+1OdEMeyH1zA+Tptbol23Zbtbn5dov4j1qeyvLbf0Zak7d8+MBX0U+gz
pQTo08Ys5KhqdekLIw7rK9DUrtBu0bqL0w5984fph2pKpEWvMVBK9Rsu/yYa0
KTFXPh8Q2f0pVn1L8QKCCQqAzmnDHFav+ZFaWrvNeNqcs5ezqWj15jYuiK7qLXi
IduVpybjTn1Y0DaGoL9sZ9AnAWYtdxUr5VDgxuZ/g5CAg89RzffYrmR0kEpRZhtV
XZ17a3cFcsMNa33HvVfD0tN7ky2pU080w6J0wIDaQAB4o1BAAKMeTYXdygqN1a
I3eLVR12nMbaS8JmC0D+/bK1bHF+M4IDKwWzp1i0Ls7Kr50tD5s1RP2B8rtH90
jZaYR+7Lr+fhI/f7CFvjVuSU/5SB0ETj1xEuOH/U5naM05fxKrRrUUEjGTL7P+4g
FsBPh50Tw67A1GpFvci5sx9h2NEzhDZvmnk82sAU+UemP80ofLUB2zC5PZCRyKj
xF/LkyuA0ym45sjpzS0sw0H1RMr6AxBLUPJ1d1ueX04CpXhcX0dAXZQdLVhsjw6Qs
AVBR5Vnj19nSag0YWeE7cmI0GfT4NEp95khk89TRo1NX3PJTzW0fKtM0r+Bvfx0y
NE0754ECqYEA5HvGLvGVJSC4P41cse4GTB72jNyRzYJxhI+wx2VEK1HEfVCHEmcd
Iq07Wx1wz+HGBtWu0Uj2q5BHaQYhD8ncgBNRkcUE6j7qKGF+Rb3QCPMX8sdZ
rMuA24ys0sy07D7/7x8KGUCIqugHkxj00E0uD/IaWoN831e0n1b1ECqYEA4zNF
a6tEK6dW46Rutwvm1X0IRBw4vBPaexH1fdrTABCWknzzhwHPKYtLcm5mPrZs3tL
yq9cZK1EAv9Uao5s0+zh2vgsR0/H2dtXuYrNQ01o4TPKBVJ1d8BHMv+IbVaiGL0g
5G/m5PS1u51uMb4fjYVjtj0LgYBK01v8DCZMS8CgYEAqy/yTVsvhd1PW0458Av5
```

**Be sure to save the private key** and store it at a secure location (e.g. in a safe). Make a backup of this key. Without the private key you cannot open any files, e.g. when the web browser was reinstalled.

**The private key is never sent to the server.** The private key cannot be restored.

In case this key is lost, you have to create a new one. However, you only can access files encrypted for your old key when

- You re-upload the files
- Another user who shared an encrypted folder with you re-encrypts it for your new key.

From then on you can manage your keys in your *Personal Settings*, details are found in the section below.

## Key Management

The key management is found in your Personal Settings. You may reach this space by clicking on your user name in the upper right corner of your ownCloud. This opens a dropdown menu, choose **Settings**. The settings for end-to-end encryption are found in the section **Security**.

### Manage Existing Keys

- 5 -

## Existing Keys

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

| Key                                    | Description Created | IP        | User-Agent                                                                   |                                                                                     |
|----------------------------------------|---------------------|-----------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| ac9538559c1292b5d19db1fa3ce626c3       | 12 minutes ago      | 127.0.0.1 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0 |  |
| <b>f3eb5bbff78acf8ab51c15935e2c749</b> | seconds ago         | 127.0.0.1 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0 |  |

All public keys, which are stored on the server are shown here, including the date and IP address of creation as well as the user agent (usually browser) from which the public key was uploaded.

In case you use the Your Computer/Device storage, the public key, which matches your stored private key is marked bold.

You can delete public keys by clicking the trash bin icon. From then on all files cannot be decrypted with the corresponding private key any longer.

## Key Management depending on your Key Storage

### Your Computer/Device - Local Key

#### Local Key

Public Key ID: **f3ef5bbf3178ac78cb50c15935e2c74a**

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAoEBqcPx0b9v/byr2b76tymLE0H4vomx0LjjBo0jrxiCgUj7
RuB2hWLG8Lg1MJVnB17+YGxJDZIQH1I+TL077ICTv6pqiGnBYsd0S3NIDGFGRthD
m8wBmVGyyEpaMG1UjF04IH+eLkuxIGZqAjyhbpd0EKHIyYzmEwrQL7nBuMbMhLU+
DY0FuHTumVyrG0PbPAvJYYP1LiQlXk/XW3RPmL/Cvg42DgxFrr67630vlx2x6ix
BdIom/amPw15+y7yyC+GCjMnFtPM/+E0JhJoNRV0skc1tnqKZmY0DVmVCzw7/qDL
2s39c5RKlMqaAtXmf5Wzum87j4vMDaFaU1QjQvzhkqI02i0rBCLQhF+47Q5+vPHs
pN9cZzPbXSpAwBemcFy61NFMelVMkav+q1AAwIDAQABAOIBAGxd4xzwoaInJT7p
0KiU5zXXQLy0+EVf9CZxmw7PM6lmM6p1zeaKF9vvhhR2nRFz1q53YJGX6HbS1TA5
D4Q57vvpnwA3n78LtQil0o7vME0e7EUwLXfWa43k+4bK35cWUR4b9eXsGHYDKtLJ
5KW03XECgYEAOCgXebIx2FTGEqbv3yXbscW3qBR4eDgWk93CNtvDDEJk+8pdXND
oT3u61bC3zFt1hLxPNDgNJ0sB5tKHcaMlJV95kGjVrVhGHLA7FFqWZDL4bwmTJLn
mGxChZ95rHGSwHl9liYcnpXD/FzqxKig392jZyXAr1sRdEfms2KetaRa0sZBNo40
TPH0BoV0sKSkwvuyMDZ92zwmRIYf0b6+b9U8WM+rcglguJA++RwjSuWfaXlkwC
Znof0gQl7FnpS2hCRXZbxvoEdd6+mPTN2RqJCqM0qytGvlKlKQCgXQ+Ly0dDwMb
o0/Km/E6xNc00+6MwzxxTPmprhMPDpRge4/CPD4rPcw5MLP00f0Hut8CgYEAxRWa
0Q0YwmxPu41P///snIqh/PQf8QxeNuElwjdo0BXX1YnekkShRKgtJ8Y0iaUPTKr
sf1sAR31ykTNDmnk6aGHNjoAe975Cu0P5/L9bpj7f/jeRuJB3TVXmX0xLiBxLLqP
Q2KTutI3+gptRmEf8qVgXdnCw+qP23KwWvKQ10CgYEA1WtwiabW12igCqX5hQJ
xWEHSqTNn8vvwC0VLyouXRWkxiPUIZ0EQDxNxrNNDgDjy3EcFzYfUI0ISACB0s2A
H91HlfbJRfHfAaacPGop0jdXmgxK2ZzT7TYL0Di985BzQMBJDqaGurRE78aF+/TJ
+mSHBy2nY0b7lf9jPwS47QkCgYEAChhiLvt1LrhXmTbS2z0jxJ0BUTC8Fh/ZD5yW
z40BCfo0bwi9uvDVRwW+P6JkpjEdtmjMrLBbg08k8Ph3PH7GIAWLJibyEWZJgXpI
AU3oTW0CgYBT/YfHK/4JwhoHFDKJ58grTn50PUeDiu45CEUA+TUwxU7wg49qq7nf
hMXr1MuE2zgGxdm6/x7VgFqzM2nHXFJlWVcU1+fxqAbavz2JD+nDf/J5yahnj7RS
gwjKdG1YhnWo3p0NmAUxefl2FkzV8YZoNi/yhT6JdCoCo5TDBhK08Q==
-----END RSA PRIVATE KEY-----
```

Download Key

Load Key

Delete Local 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)*

#### Download Key

Save the private key which is currently stored on the server/device to a file

#### Load Key

Paste a previously downloaded key and click load to be ready to use it in your current device. With this feature you can transfer the key from one browser/device to another when you download it in the first browser/device and load it into the second.

### Delete Local Key

Delete a key from local storage only. The corresponding public key on the server is not touched.

If you **do not have a copy** of your private key **it cannot be restored**

### Generate New Private Key

When you lost your private key or you want to create a new one for another device, click **Generate New Private Key**. The private key in the browser is replaced and the new public key is uploaded to the server. The previous public key on the server is not touched.

In case you lost your private key be sure to delete the corresponding public key before (see Manage Existing Keys above)

## Key Storages *Manual input for each download and Local decryption*

Both storage options require, that your public key is available on the server. It will be used for encrypting files.

In the Security section of your Personal settings you find a text area:

Add Public Key

Public Key ID:

Save

You might already have keys when

- you at least once have generated a public key in the Personal Settings
- you at least registered once with the Key Server (file key or Smart Card)
- the administrator added your key on the server (occ command)

## Decrypting Files

### Your Computer/Device

Files will be decrypted on the fly. No interaction is required.

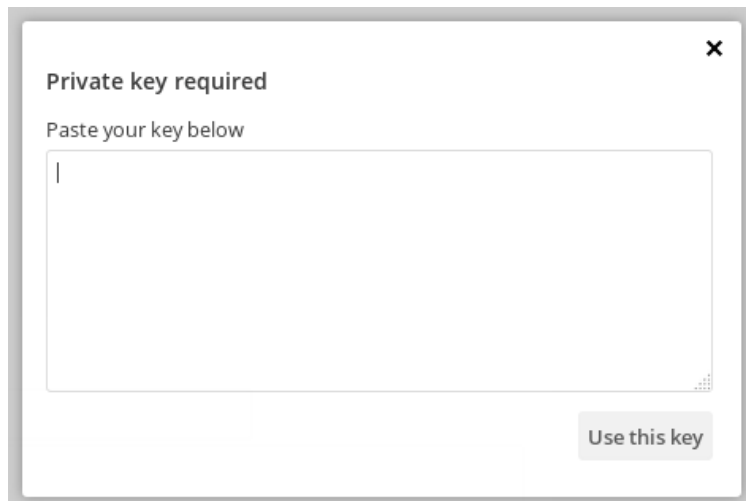
### External Key/Smartcard

The key server pops up a notification that you are about to decrypt a file. You must confirm the decryption.

When re-encrypting a folder you will be asked for a confirmation as well.

## Manual input for each download

Every time you want to open an encrypted file the browser opens a modal window where you have to provide your private key.



A modal window titled "Private key required" with a close button (X) in the top right corner. Below the title, it says "Paste your key below". There is a large text input field with a cursor at the top left. At the bottom right of the modal, there is a button labeled "Use this key".

The file is decrypted in the browser only, the private key is never sent to the server.

## Local decryption

The raw E2EE file will be downloaded. You need the E2EE Reader to be able to decrypt those files.