



SWISS DATA DEFENCE

# **MOUNT10**

# **CloudDrive**

## **User Manual**

Version 1.0 / Januar 2017

**MOUNT10 AG**

Haldenstrasse 5, 6340 Baar, Switzerland

info@mount10.ch, Tel. +41 41 726 03 20

## Inhaltsverzeichnis

<b>Introduction.....</b>	<b>3</b>
<b>Web Interface .....</b>	<b>3</b>
<b>Navigating the Main User Interface .....</b>	<b>3</b>
<b>Files &amp; Synchronization.....</b>	<b>5</b>
<b>Accessing your Files Using the MOUNT10 CloudDrive Web Interface .....</b>	<b>5</b>
<b>Favorites .....</b>	<b>5</b>
<b>Share .....</b>	<b>5</b>
<b>Previewing Files.....</b>	<b>6</b>
<b>Navigating Inside your MOUNT10 CloudDrive .....</b>	<b>7</b>
<b>Sharing Status Icons .....</b>	<b>7</b>
<b>Creating or Uploading Files and Directories.....</b>	<b>7</b>
<b>Selecting Files or Folders.....</b>	<b>8</b>
<b>Filtering the Files View .....</b>	<b>8</b>
<b>Moving Files .....</b>	<b>8</b>
<b>Accessing MOUNT10 CloudDrive Files Using WebDAV.....</b>	<b>9</b>
<b>Desktop and Mobile Clients.....</b>	<b>9</b>
<b>WebDAV Configuration .....</b>	<b>9</b>
<b>Mapping Drives with Windows Explorer.....</b>	<b>10</b>
<b>Accessing Files Using Mac OS X .....</b>	<b>11</b>
<b>Managing Deleted Files.....</b>	<b>12</b>
<b>Setting Your Preferences .....</b>	<b>13</b>
<b>Using two-factor authentication .....</b>	<b>14</b>
<b>Configuring two-factor authentication .....</b>	<b>14</b>
<b>Recovery codes in case you lost your 2nd factor .....</b>	<b>16</b>
<b>Logging in with two-factor authentication .....</b>	<b>17</b>
<b>Using client applications with two-factor authentication .....</b>	<b>17</b>
<b>Managing Devices .....</b>	<b>18</b>

## Introduction

Our product MOUNT10 CloudDrive is an easy to use sharing- and cloud-platform, hosted in Switzerland and only able to store encrypted data. With MOUNT10 CloudDrive, the data connection is encrypted by SSL and transported over the public internet into the SWISS FORT KNOX.

This cloud works like a local folder or drive, with the difference that it is offsite and highly available. The data on the cloud, can be shared with 3<sup>rd</sup> party users using an URL-link.

## Web Interface

You can connect to your MOUNT10 CloudDrive using any Web browser; just point it to your MOUNT10 CloudDrive and enter your username and password. Supported Web browsers are:

Firefox 14+

Chrome 18+

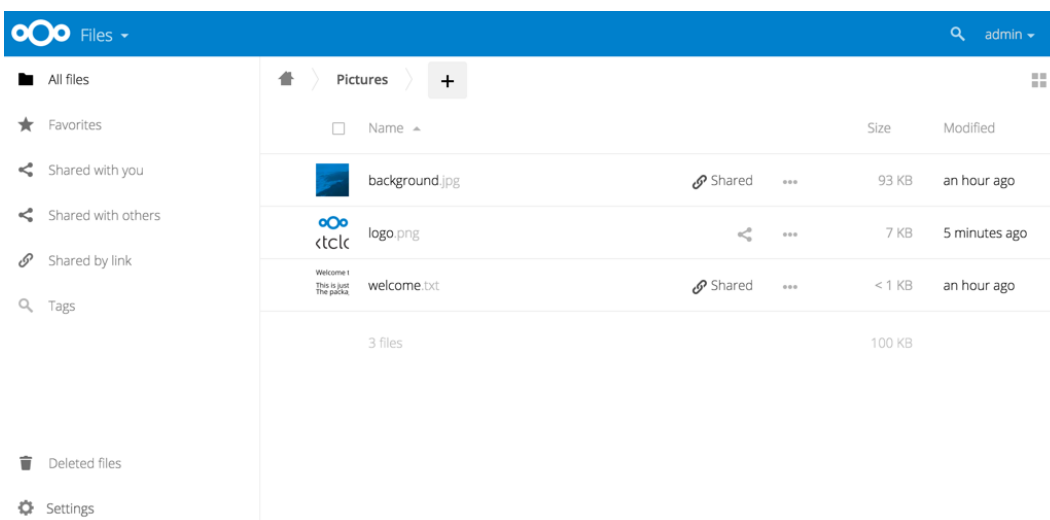
Safari 7+

IE11+

Microsoft Edge

## Navigating the Main User Interface

By default, the MOUNT10 CloudDrive Web interface opens to your Files page. You can add, remove, and share files, and make changes based on the access privileges set by you.



### MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

The MOUNT10 CloudDrive user interface contains the following fields and functions:

- ➔ **View Selection** menu: Located in the upper left corner. Click the arrow to open a dropdown menu to switch between File and Activity view.
- ➔ **Search** field: Click on the magnifier in the upper right hand corner of to search for files.
- ➔ **Personal Settings** menu: Click on your username, located to the right of the Search field, to open your Personal Settings dropdown menu. Your personal page provides the following settings and features:
  - Name, email, and profile picture settings
  - Password management
  - Interface language settings
  - Manage connected browsers and devices
  - Manage notifications
  - Links to download desktop and mobile apps
  - Re-run the First Run Wizard

See *Setting Your Preferences* section to learn more about these settings.

- ➔ **Navigation Bar**: Located over the main viewing window, this bar provides a type of breadcrumbs navigation that enables you to switch to higher levels of the folder hierarchy up to the root level (home).
- ➔ **New** button: Located in the Navigation bar, *the New button* enables you to create new files, new folders, or upload files.

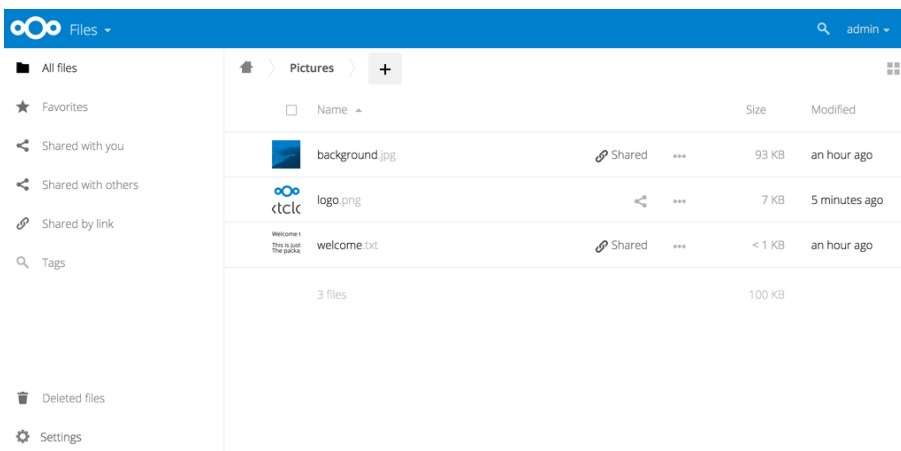
## Note

*You can also drag and drop files from your file manager into the MOUNT10 CloudDrive Files Application View to upload them to your MOUNT10 CloudDrive. Currently, the only Web browsers that support drag-and-drop folders are Chrome and Chromium.*

## Files & Synchronization

### Accessing your Files Using the MOUNT10 CloudDrive Web Interface

You can access your MOUNT10 CloudDrive files with the MOUNT10 CloudDrive Web interface and create, preview, edit, delete and share files.



MOUNT10 CloudDrive can display thumbnail previews for images and text files. Hover your cursor over a file or folder to expose the controls for the following operations:

### Favorites

Click the star to the left of the file icon to mark it as a favorite, and quickly find all of your favorites with the Favorites filter on the left sidebar.

### Share

Share the file or folder with other users, and create public shares with hyperlinks. You can also see who you have shared with already, and revoke shares by clicking the trash can icon.

#### You can set several share permissions:

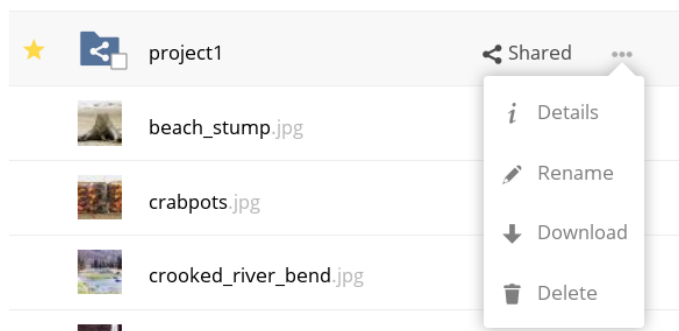
- Can edit; allows the users you share with to edit your shared files, and to collaborate using the Documents view. Allows uploading a new version of a shared file and replacing it
- Create; allows the users you share with to create new files and add them to the share.
- Delete; allows the users you share with to delete shared files.

### MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20


## Overflow Menu

The Overflow menu (three dots) displays file details, and allows you to rename, download, or delete files.



The **Settings** gear icon at the lower left allows you to show or hide hidden files in your MOUNT10 CloudDrive Web interface. These are also called dotfiles, because they are prefixed with a dot, e.g. mailfile.

The dot tells your operating system to hide these files in your file browsers, unless you choose to display them. Usually these are configuration files, so having the option to hide them reduces clutter.

 Settings

Show hidden files

## Change in Share Expiration Date

You can set an expiration date on public shares. Local shares do not expire when public shares expire. To “expire” a local share, click the trash can icon to un-share your files.

## Previewing Files

MOUNT10 CloudDrive cannot display a file, it starts a download process and downloads the file to your computer.

## MOUNT10 AG

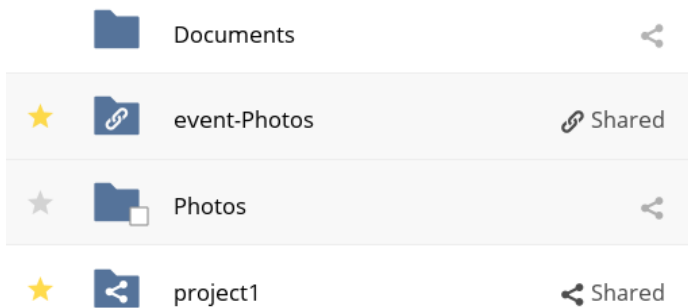
Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

## Navigating Inside your MOUNT10 CloudDrive

Navigating through folders in MOUNT10 CloudDrive is as simple as clicking on a folder to open it and using the back button on your browser to move to a previous level. MOUNT10 CloudDrive also provides a navigation bar at the top of the Files field for quick navigation.

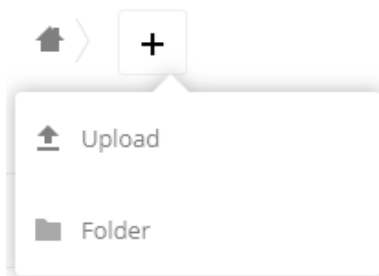
## Sharing Status Icons

Any folder that has been shared is marked with the Shared overlay icon. Public link shares are marked with a chain link. Un-shared folders are blank.



## Creating or Uploading Files and Directories

Upload or create new files or folders directly in an MOUNT10 CloudDrive folder by clicking on the New button in the Files app. The New button provides the following options:



### Up arrow

Upload files from your computer into MOUNT10 CloudDrive. You can also upload files by dragging and dropping them from your file manager.

### Folder

Creates a new folder in the current folder.

## MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

## Selecting Files or Folders

You can select one or more files or folders by clicking on their checkboxes. To select all files in the current directory, click on the checkbox located at the top of the files listing.

When you select multiple files, you can delete all of them, or download them as a ZIP file by using the Delete or Download buttons that appear at the top.

## Filtering the Files View

The right sidebar on the Files page contains several filters for quickly sorting and managing your files.

### All files

The default view; displays all files that you have access to.

### Favorites

Files or folders marked with the yellow star.

### Shared with you

Displays all files shared with you by another user or group.

### Shared with others

Displays all files that you have shared with other users or groups.

### Shared by link

Displays all files that are shared by you via public link.

## Moving Files

You can move files and folders by dragging and dropping them into any directory.



## Accessing MOUNT10 CloudDrive Files Using WebDAV

MOUNT10 CloudDrive fully supports the WebDAV protocol, and you can connect and synchronize files with your MOUNT10 CloudDrive. In this chapter, you will learn how to connect Mac OS X, Windows, and mobile devices to your MOUNT10 CloudDrive via WebDAV. Before we get into configuring WebDAV, let's take a quick look at the recommended way of connecting client devices to your MOUNT10 CloudDrive.

### Desktop and Mobile Clients

For synchronizing files with your desktop computer, we recommend using the Nextcloud Sync Client for Windows, Mac OS X and Linux. The Nextcloud Desktop Sync Client enables you to connect to your MOUNT10 CloudDrive. You can create folders in your home directory, and keep the contents of those folders synced with your MOUNT10 CloudDrive.

Simply copy a file into the directory and the Nextcloud desktop client does the rest. Make a change to the files on one computer, you will always have your latest files with you wherever you are.

You can configure the client to save files in any local directory you want, and you choose which directories on the MOUNT10 CloudDrive to sync with. The client displays the current connection status and logs all activity, so you always know which remote files have been downloaded to your PC, and you can verify that files created and updated on your local PC are properly synchronized with the server.

The recommended method for syncing your MOUNT10 CloudDrive with Android and Apple iOS devices is by using the mobile apps.

To connect to your MOUNT10 CloudDrive with the mobile apps, use your login credentials you received from the MOUNT10 Support Center.

### WebDAV Configuration

If you prefer, you may also connect your desktop PC to your MOUNT10 CloudDrive by using the WebDAV protocol rather than using a special client application.

With WebDAV you can access your MOUNT10 CloudDrive shares on Mac OS X, Windows or even Linux in the same way as any remote network share, and stay synchronized.

### MOUNT10 AG

## Mapping Drives with Windows Explorer

To map a drive using the Microsoft Windows Explorer:

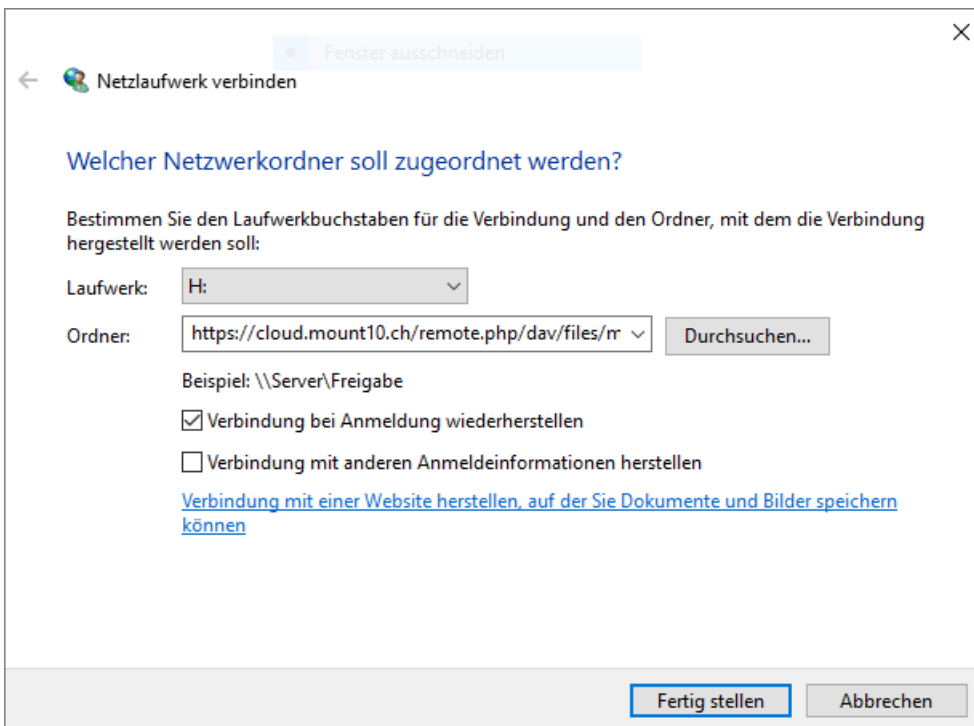
1. Open Windows Explorer on your Windows Computer.
2. Right-click on Computer entry and select Map network drive... from the drop-down menu.
3. Choose a local network drive to which you want to map your MOUNT10 CloudDrive.
4. Specify the address to your MOUNT10 CloudDrive, followed by /remote.php/dav/files/USERNAME

### For example:

`https://cloud.mount10.ch/remote.php/dav/files/myusername`

### Note

Check *Reconnect at logon* to ensure that the mapping is persistent upon subsequent reboots. If you want to connect to the MOUNT10 CloudDrive as a different user, check *Connect using different credentials*.



5. Click the Finish button.

Windows Explorer maps the network drive, making your MOUNT10 CloudDrive available.

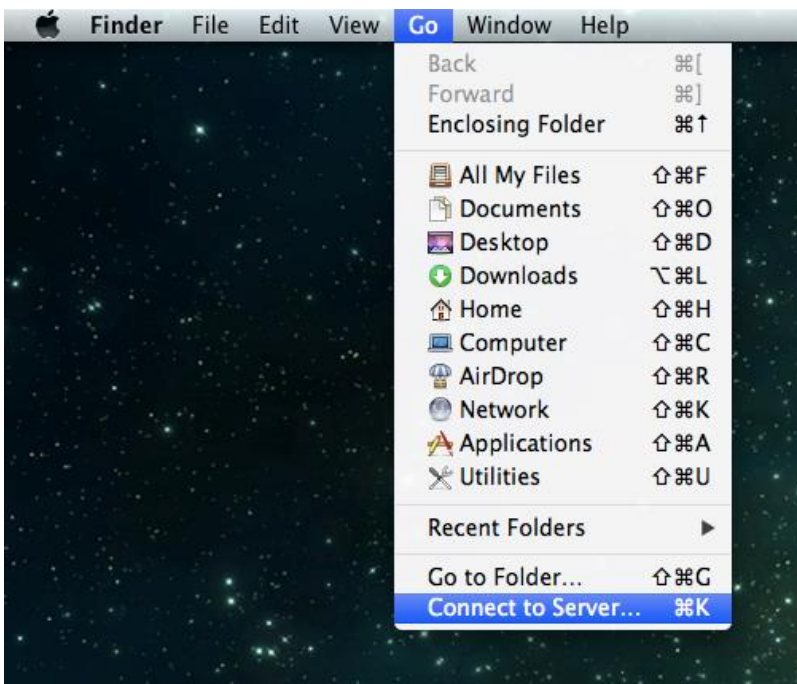
## MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

## Accessing Files Using Mac OS X

To access files through the Mac OS X Finder:

1. Choose Go > Connect to Server.
2. The “Connect to Server” window opens.
3. Specify the address of the server in the **Server Address** field.



For example, the URL used to connect to the MOUNT10 CloudDrive from the Mac OS X Finder is:

*<https://example.com/nextcloud/remote.php/webdav>*

4. Click Connect.
5. The device connects to the server.

### Note

*For added details about how to connect to an external server using Mac OS X, check the vendor documentation*

## MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

## Managing Deleted Files

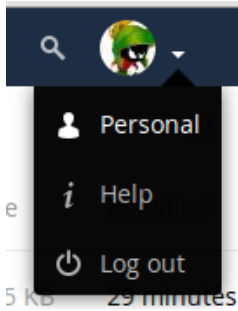
When you delete a file in your MOUNT10 CloudDrive, it is not immediately deleted permanently. Instead, it is moved into the trash bin. 30 days after deleting your data from your cloud, the trashcan content will be automatically and definitely erased by the system.

Find your deleted files by clicking on the deleted files button on the Files page of the MOUNT10 CloudDrive Web interface. You'll have options to either restore or permanently delete them.

## Setting Your Preferences

As a user, you can manage your personal settings by clicking on your username in the top, right corner of your MOUNT10 CloudDrive WebGUI.

The Personal Settings Menu opens.



Choose Personal from the drop down menu.

You are using 698 KB of Unlimited

Profile picture



png or jpg, max. 20 MB

Full name

bernie madhatter

Email

bernie@example.com


For password recovery and notifications

Groups

You are member of the following groups:  
graphics, users, video

Password

Current password

New password 

Change password

Your Personal Settings Page offers you the options in the following.

- ➔ Usage and available quota
- ➔ Manage your profile picture.
- ➔ Full name. You can make this anything you want, as it is separate from your MOUNT10 CloudDrive login name, which is unique and cannot be changed.
- ➔ Email address.
- ➔ Manage your password.
- ➔ Using two-factor authentication.
- ➔ Choose the language for your Nextcloud interface.
- ➔ Links to desktop and mobile apps.
- ➔ Manage your Activity stream and notifications.
- ➔ Default folder to save new documents to.

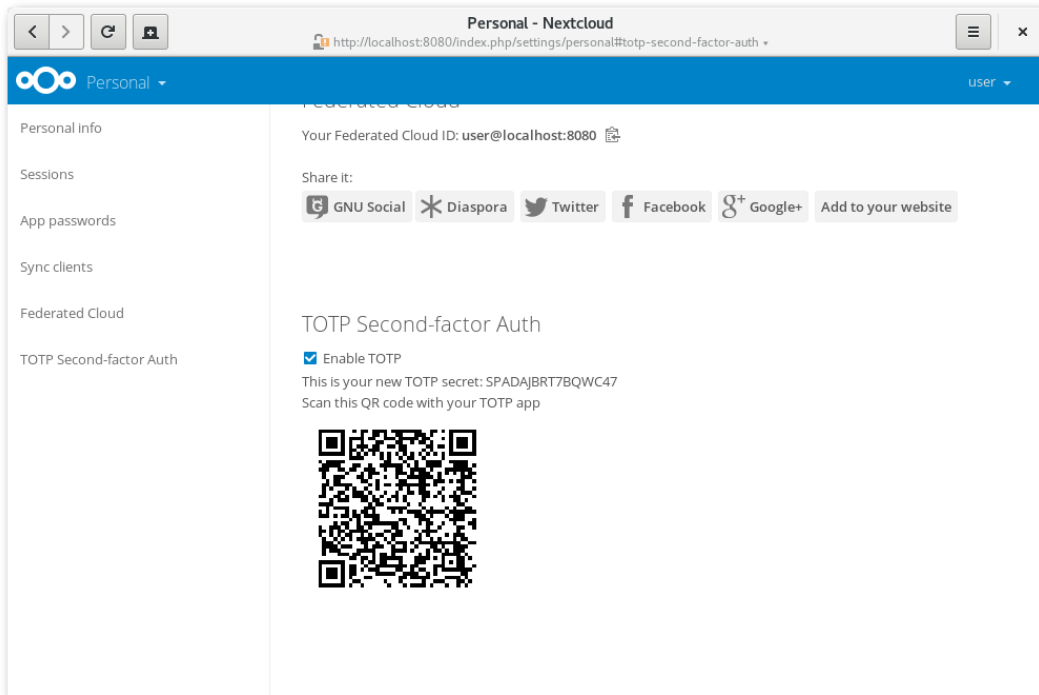
## Using two-factor authentication

Two-factor authentication (2FA) is a way to protect your MOUNT10 CloudDrive account against unauthorized access. It works by requiring two different 'proofs' of your identity. For example, something you know (like a password) and something you have like a physical key.

Typically, the first factor is a password like you already have and the second is a code you generate on your phone or another device (something you have).

## Configuring two-factor authentication

In your Personal Settings look up the Second-factor Auth setting, activate a Google Authenticator compatible time based code.



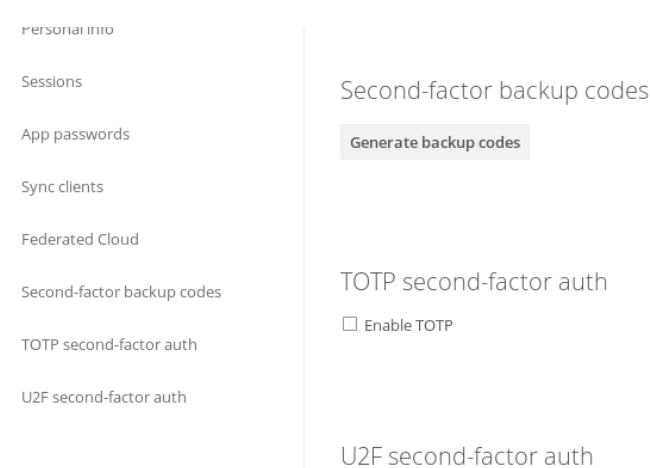
You will see your secret and a QR code which can be scanned by the TOTP app on your phone (or another device). Depending on the app or tool, type in the secret or scan the QR and your device will show a login code which changes every 30 seconds.

### Note

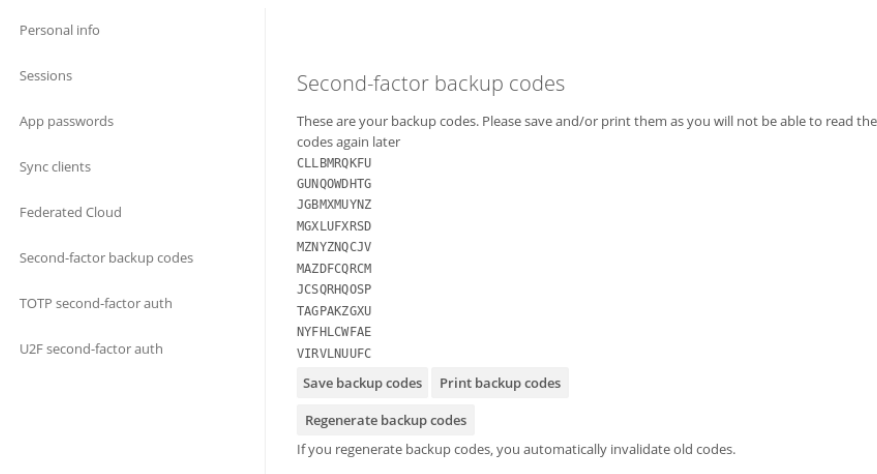
*Your TOTP QR code changes whenever you re-enable this option by clicking the checkbox. The code previously created will expire immediately. You have to scan it again with your device.*

## Recovery codes in case you lost your 2nd factor

You should always generate backup codes for 2FA. If your 2nd factor device gets stolen or is not working, you will be able to use one of these codes to unlock your account. It effectively functions as a backup 2nd factor. To get the backup codes, go to your Personal Settings and look under Second-factor Auth settings. Choose Generate backup codes.



You will then be presented with a list of one-time-use backup codes.



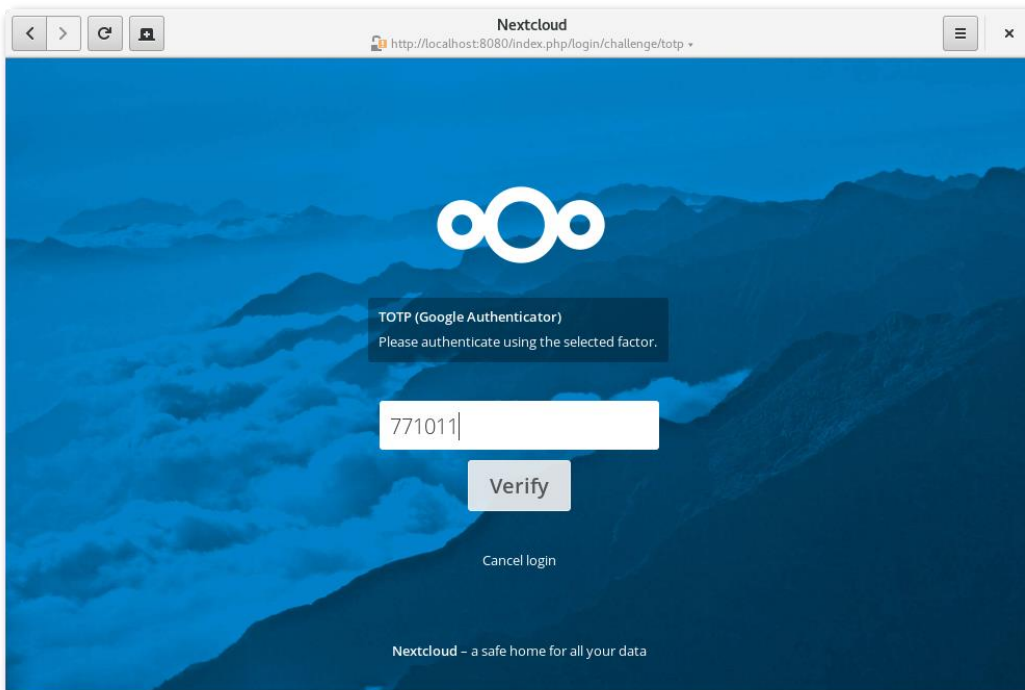
You should put these codes in a safe spot, somewhere you can find them. Don't put them together with your 2nd factor like your mobile phone but make sure that if you lose one, you still have the other. Keeping them at a safe place is a good idea.

### MOUNT10 AG



## Logging in with two-factor authentication

After you have logged out and need to log in again, you will see a request to enter the TOTP code in your browser. Just enter your code:



If the code was correct you will be forwarded directly to your MOUNT10 CloudDrive account.

### Note

*Since the code is time-based, it's important that your server's and your smartphone's clock are almost in sync. A time drift of a few seconds won't be a problem.*

## Using client applications with two-factor authentication

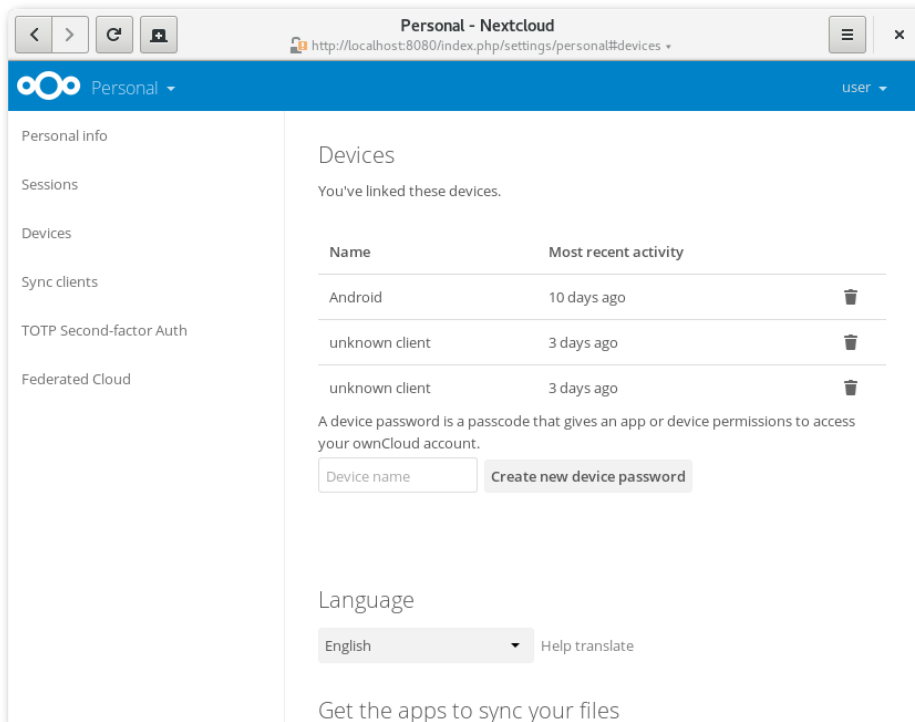
Once you have enabled 2FA, your clients will no longer be able to connect with just your password unless they also have support for two-factor authentication. To solve this, you should generate device specific passwords for them.

### MOUNT10 AG

Haldenstrasse 5, 6340 Baar, Switzerland  
info@mount10.ch, Tel. +41 41 726 03 20

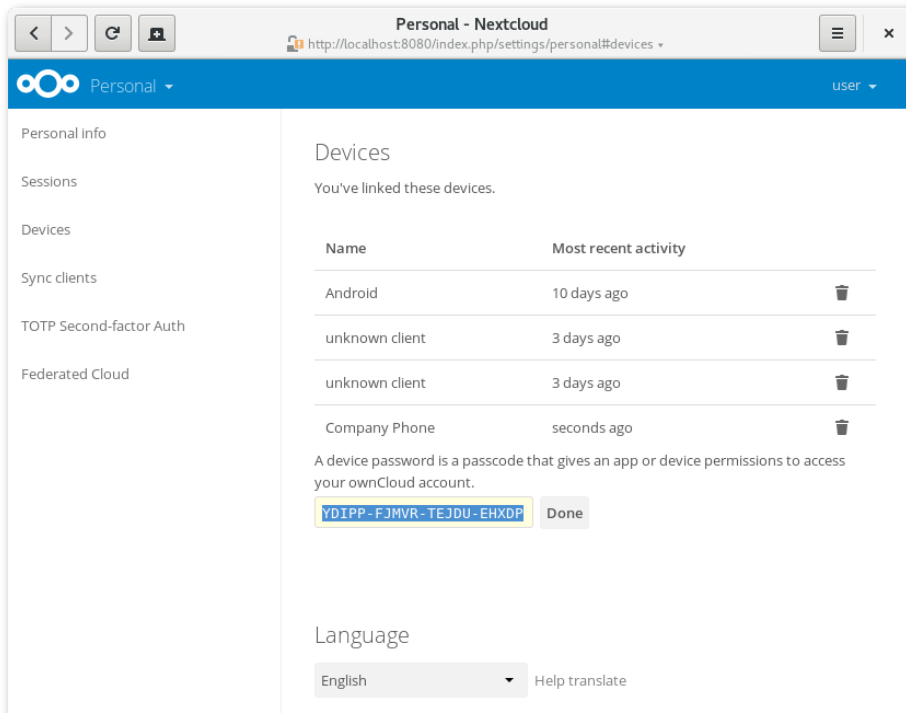
## Managing Devices

In the list of connected devices, you see all the devices and clients you generated a device password for and their last activity:



You can use the trash icon to disconnect any of the devices in the list.

At the bottom of the list you find a button to create a new device-specific password. You can choose a name to identify the token later. The generated password is used for configuring the new client. Ideally, generate individual tokens for every device you connect to your account, so you can disconnect those individually if necessary.



### Note

*You have only access to the device password when creating it, Nextcloud will not save the plain password, hence it's recommended to enter the password on the new client immediately.*

*If you are Using two-factor authentication for your account, device-specific passwords are the only way to configure clients. The client will deny connections of clients using your login password then.*