

Using two-factor authentication

Two-factor authentication (2FA) is a way to protect your Nextcloud 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 can be a text message you receive or a code you generate on your phone or another device (*something you have*). Nextcloud supports a variety of 2nd factors and more can be added.

Once a two-factor authentication app has been enabled by your administrator you can enable and configure it in [Setting your preferences](#). Below you can see how.

Configuring two-factor authentication

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

The screenshot shows the Microsoft 365 Personal settings page. The left sidebar is titled 'Personal' and includes 'Personal info', 'Security', 'Accessibility', and 'Sharing'. Below this is the 'Administration' section with 'Overview', 'Basic settings', 'Sharing', 'Security', 'Theming', 'Groupware', and 'Workflow'. The main content area is titled 'Two-Factor Authentication' and contains three sections: 'Backup code' with a 'Regenerate backup codes' button and a note that 0 of 10 codes have been used; 'TOTP (Authenticator app)' with an 'Enable TOTP' radio button, a secret key 'BDYEWVMHZNSPDQD2I', a QR code, and a 'Verify' button; and 'U2F device' with a note that no devices are configured and an 'Add U2F device' button.

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 code or scan the QR and your device will show a login code which changes every 30 seconds.

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*.

Two-Factor Authentication

Backup code

Generate backup codes

TOTP (Authenticator app)

Enable TOTP

U2F device

No U2F devices configured. You are not using U2F as second factor at the moment.

Add U2F device

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

Two-Factor Authentication

Backup code

These are your backup codes. Please save and/or print them as you will not be able to read the codes again later

YQTF3MKJTP6UTS71

1JF2NFPVHXVJ5934

G3DZ28HXC5YKS6MK

UC20TNSQ00SN35JE

NYU84I4X8JFA2TCZ

SJKVNULTU7733W2Y

TFBF7FDN3VWVD5ZH

20JV65T5EQAN7G12

6B02WNAVIN3KPYNW

R9TYF8NMNSZGLZ3E

Save backup codes

Print backup codes

Regenerate backup codes

If you regenerate backup codes, you automatically invalidate old codes.

TOTP (Authenticator app)

Enable TOTP

U2F device

No U2F devices configured. You are not using U2F as second factor at the moment.

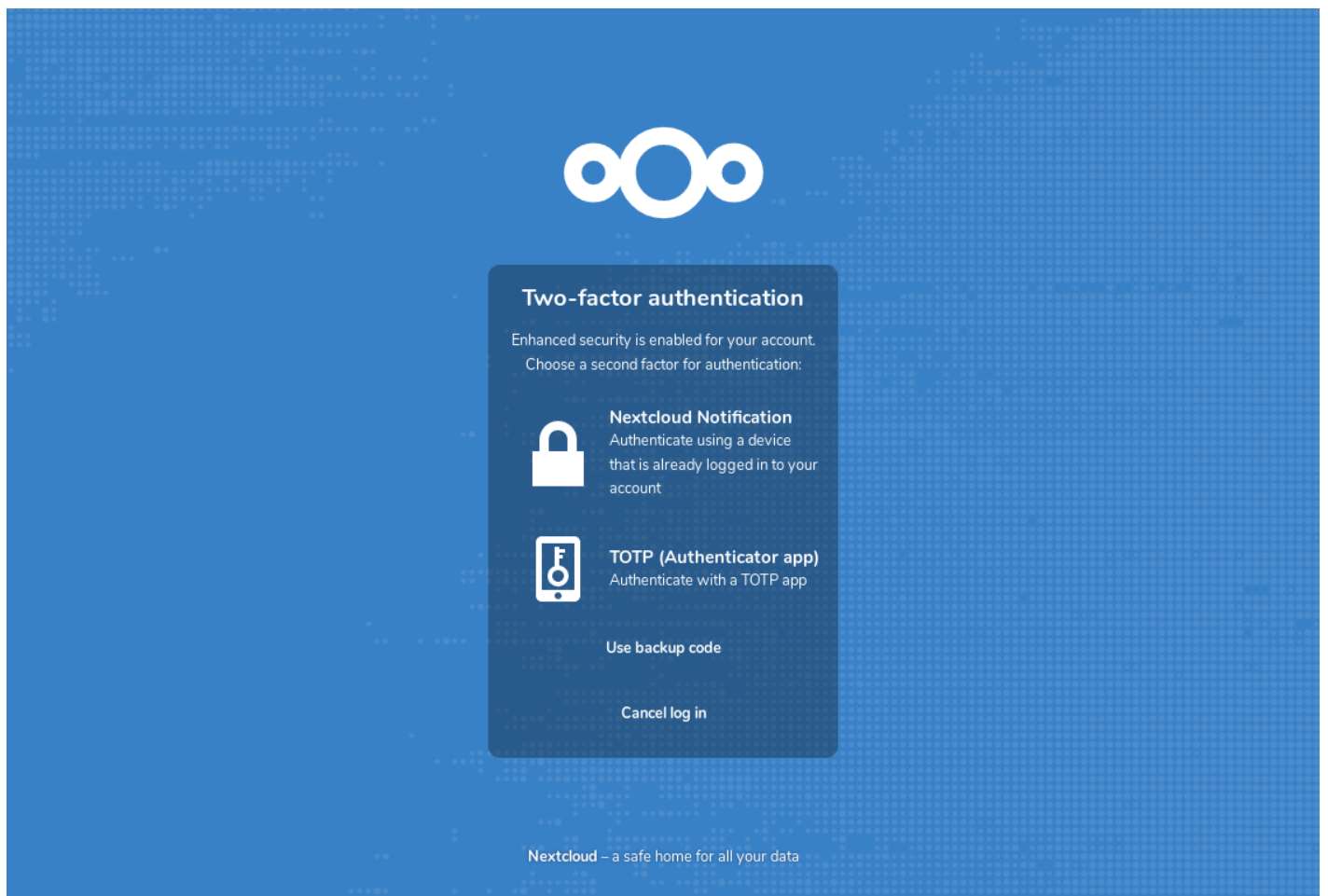
Add U2F device

You should put these codes in a safe spot, somewhere you can find them. Don't put them together

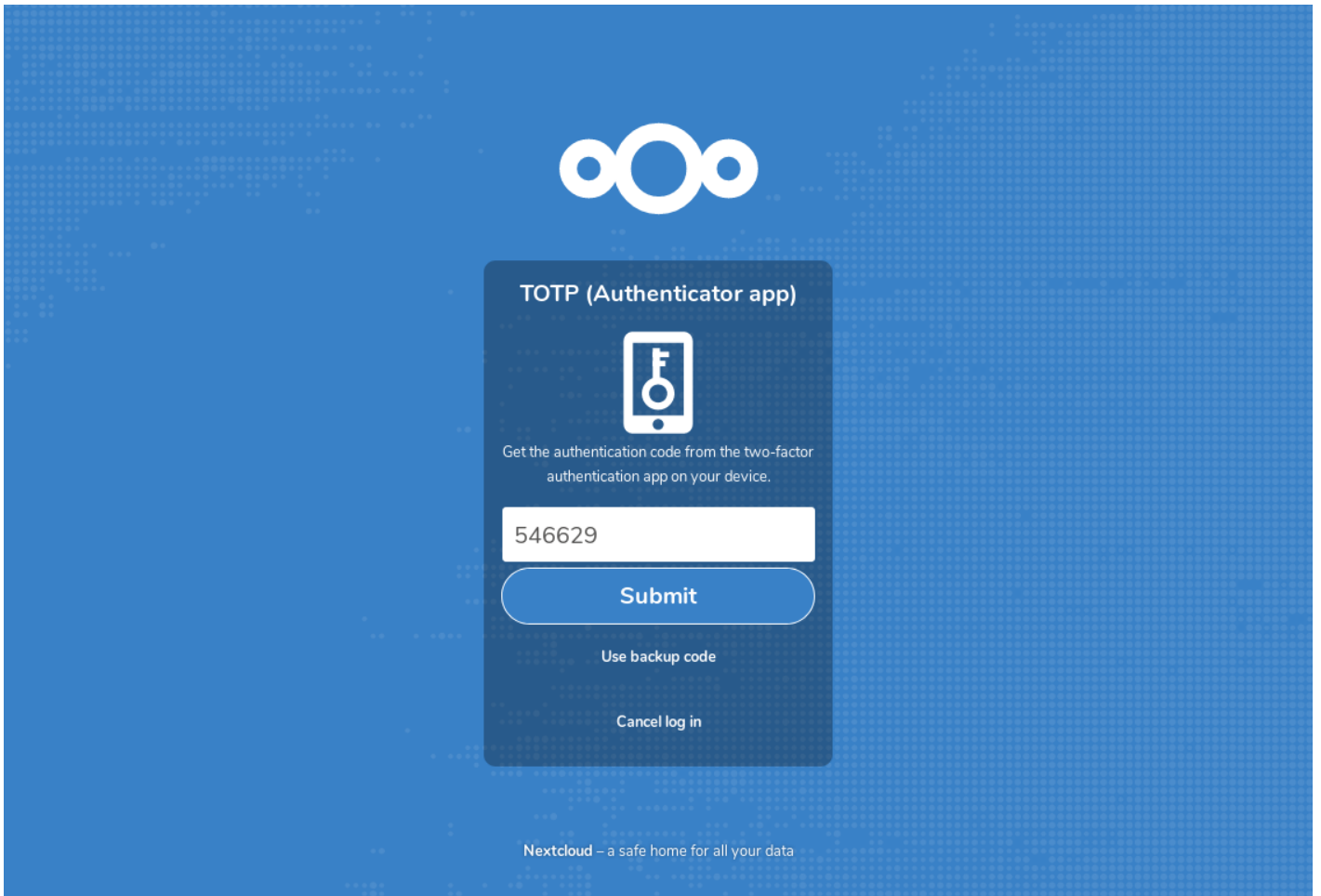
with your 2nd factor like your mobile phone but make sure that if you lose one, you still have the other. Keeping them at home is probably the best thing to do.

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. If you enable not only the TOTP factor but another one, you will see a selection screen on which you can choose two-factor method for this login. Select TOTP.



Now, just enter your code:



If the code was correct you will be redirected to your Nextcloud 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 two-factor authentication with hardware tokens

You can use two-factor authentication based on hardware tokens. The following devices are known to work:

- TOTP based:
 - [Nitrokey Pro](#)
 - [Nitrokey Storage](#)
- FIDO U2F based:
 - [Nitrokey FIDO U2F](#)

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. See [Manage connected browsers and devices](#) for more information on how to do this.

Revision #1

Created Fri, Aug 14, 2020 1:59 AM by [Travis](#)

Updated Fri, Aug 14, 2020 1:59 AM by [Travis](#)