SIGN UP AS A SIF USER

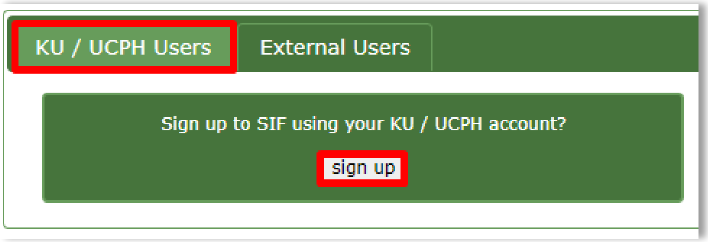
As a UCPH employee/student (see pages 1-4) or an external collaboration partner (see pages 5-9), you must sign up as a user of SIF with so-called two-factor authentication before you can access a project that uses sensitive data.

SIGN UP WITH A UCPH ACCOUNT

SIGN UP

Go to https://sif.ku.dk/

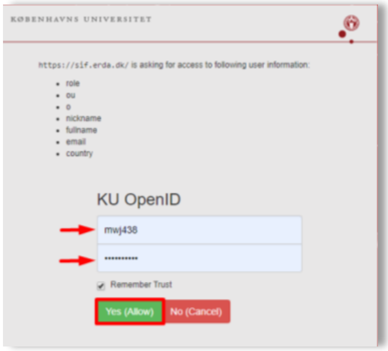
Click 'sign up'



Sign up to SIF using your KU / UCPH account?

In the pop-up window under 'UCPH OpenID', enter:

1. Your UCPH username (consists of three letters and three digits).
2. Your personal UCPH password, which you also use, e.g. for KUnet.
3. Then click 'Yes (Allow)'



https://sif.erda.dk/ is asking for access to following user information:

- role
- ou
- o
- nickname
- fullname
- email
- country

mwj438

••••••••••

You are now registered as a SIF user.

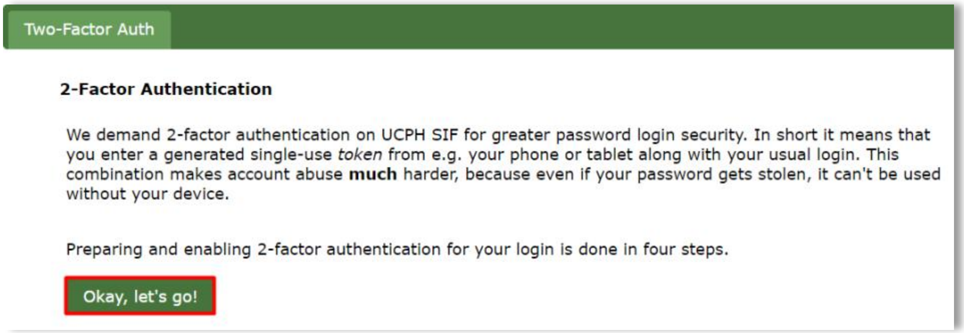
TWO-FACTOR AUTHENTICATION

To increase security, it is *compulsory* to use two-factor authentication for all SIF access.

With two-factor authentication, you add an extra control step to the login process which authenticates you. In addition to asking about something you know (in this case your username and password), an account protected by two-factor authentication will also request information about something you have (a token from an app on mobile/tablet).

When you sign up for SIF, you must complete a one-time wizard to configure the compulsory two-factor authentication.

Click ‘Okay, let’s go!’



2-Factor Authentication

We demand 2-factor authentication on UCPH SIF for greater password login security. In short it means that you enter a generated single-use *token* from e.g. your phone or tablet along with your usual login. This combination makes account abuse **much** harder, because even if your password gets stolen, it can't be used without your device.

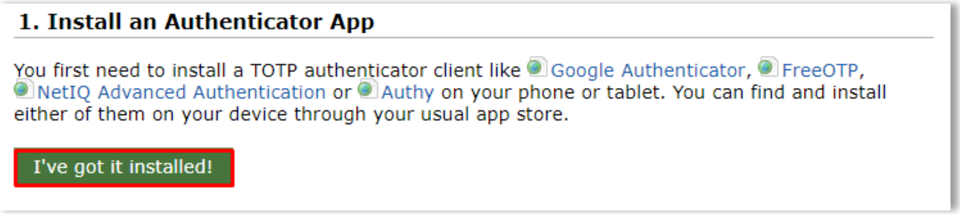
Preparing and enabling 2-factor authentication for your login is done in four steps.

A wizard will now appear in SIF which you must carefully follow.

STEP 1. DOWNLOAD APP

You have to download one of the following apps on your mobile or tablet*: *Google Authenticator*, *FreeOTP*, *NetIQ Advanced*, *Authentication* or *Authy*. Find the app where you normally download apps.

Then click “I’ve got it installed!”



1. Install an Authenticator App

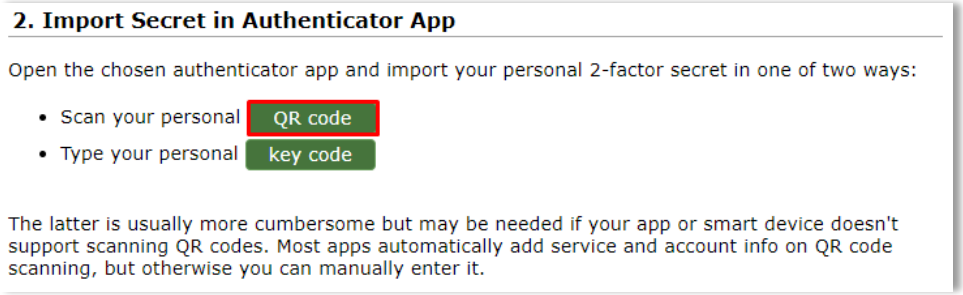
You first need to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Authy on your phone or tablet. You can find and install either of them on your device through your usual app store.

*If you only have a private mobile/tablet and you do not want to use it, you may request a small device that you can use instead. Contact support@sif.erda.dk for further information.

STEP 2. IMPORT PERSONAL TWO-FACTOR CODE

Import your personal two-factor code with ‘Scan your personal QR code’ or ‘Enter your personal key’. An example with ‘Scan your personal QR code’ follows below.

Click ‘QR code’ in SIF.



2. Import Secret in Authenticator App

Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:

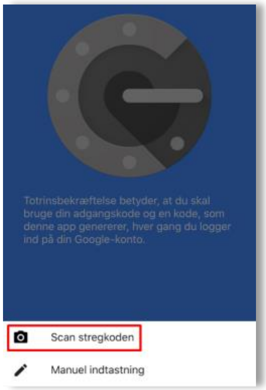
- Scan your personal QR code
- Type your personal key code

The latter is usually more cumbersome but may be needed if your app or smart device doesn't support scanning QR codes. Most apps automatically add service and account info on QR code scanning, but otherwise you can manually enter it.

A QR code pops up in SIF.

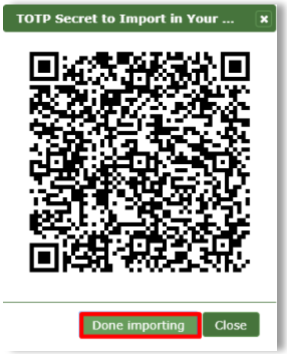
Open your downloaded app.
The apps are slightly different. The screenshot shown below is from the

Google Authenticator app. Click ‘Scan barcode’.

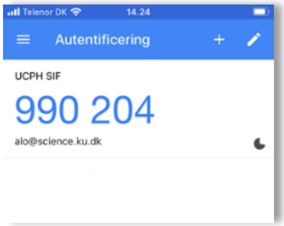


Totrinsbekræftelse betyder, at du skal bruge din adgangskode og en kode, som denne app genererer, hver gang du logger ind på din Google-konto.

Now scan the QR code you have just opened in the wizard on SIF. I.e. point the camera of your mobile at the QR code (the app may ask permission to use your camera). The app will now scan the QR code. Then click ‘Done importing’.

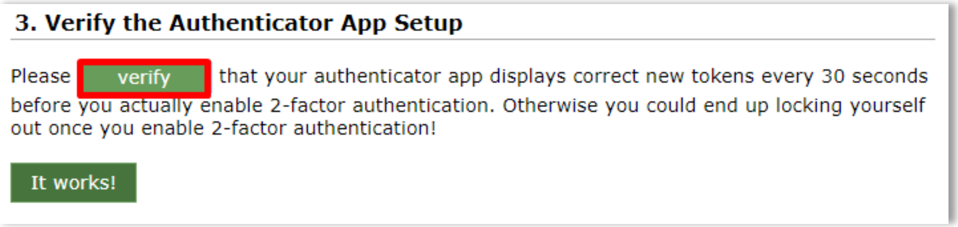


Your app can now generate six-digit tokens. In the example below, the token used is ‘990 204’.



STEP 3. VERIFY THAT IT WORKS

Next you need to check that your two-factor authentication has been set up correctly and that the app supplies the right tokens.

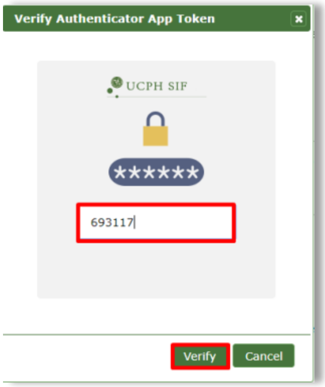


3. Verify the Authenticator App Setup

Please verify that your authenticator app displays correct new tokens every 30 seconds before you actually enable 2-factor authentication. Otherwise you could end up locking yourself out once you enable 2-factor authentication!

A pop-up window will appear, where you enter the token that the app displays (if it does not appear, click ‘verify’ in the above). Please note that the token changes after 30 seconds.

Enter the six-digit token and click the ‘Verify’ button in the pop-up window.

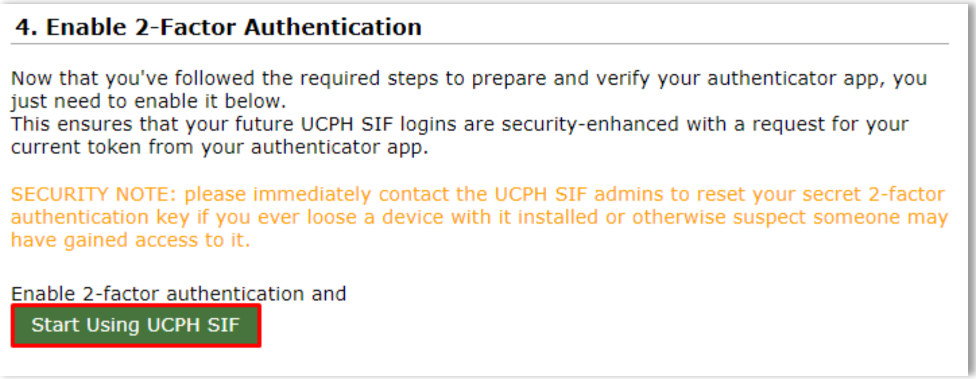


693117

If your two-factor authentication is successful, you will be taken directly to the next step.

STEP 4. ENABLE TWO-FACTOR AUTHENTICATION

Click ‘Start Using UCPH SIF’.



4. Enable 2-Factor Authentication

Now that you've followed the required steps to prepare and verify your authenticator app, you just need to enable it below.
This ensures that your future UCPH SIF logins are security-enhanced with a request for your current token from your authenticator app.

SECURITY NOTE: please immediately contact the UCPH SIF admins to reset your secret 2-factor authentication key if you ever loose a device with it installed or otherwise suspect someone may have gained access to it.

Enable 2-factor authentication and

YOU ARE NOW SIGNED UP

Congratulations! You are now signed up on SIF with two-factor authentication.

In the future, you can enter https://sif.ku.dk/ and log in using your UCPH username and personal UCPH password followed by two-factor authentication.

Please remember to always click ‘Log out’ when done working in SIF. In that way you ensure that nobody else gains unauthorised access to your sensitive data.

HELP

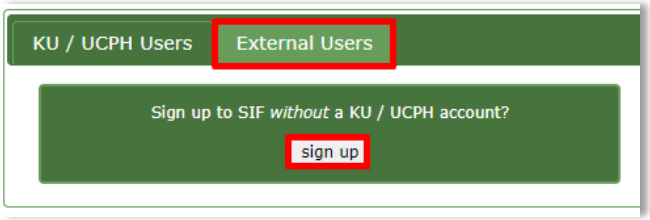
Read more guides and instructions at https://sif.ku.dk/ or get help at support@sif.erda.dk

SIGN-UP FOR EXTERNAL COLLABORATION PARTNER

SIGN UP

Go to https://sif.ku.dk/

Click the ‘External Users’ tab. Then click ‘sign up’:

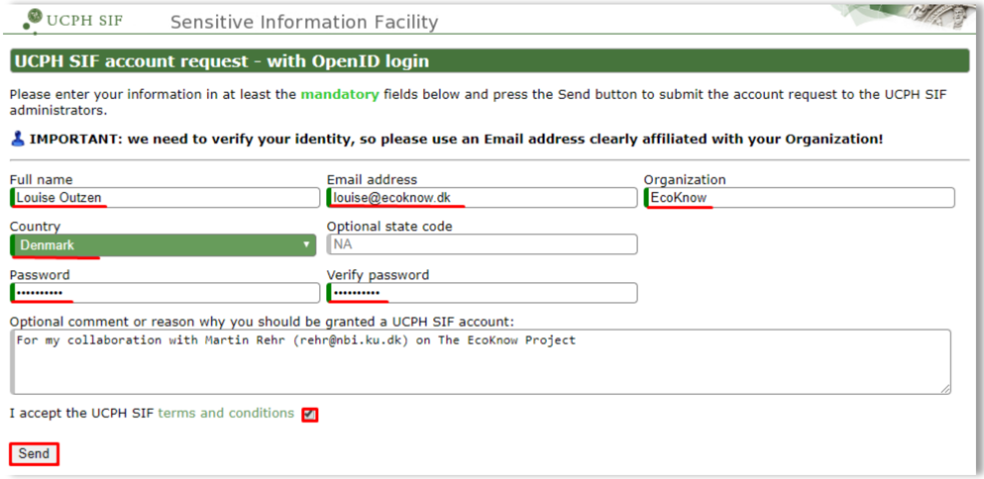


Sign up to SIF *without* a KU / UCPH account?

Please fill the form with your details:

- Full name: *Enter your full name*
- Email address: *Your work email (no third-party email services such as hotmail, gmail or yahoo)*
- Organization: *The name of your workplace/company*
- Country: *Select your country in the dropdown menu*
- Password: *Create a sufficiently difficult password for your SIF access. It must consist of at least 10 characters and contain both upper and lower case letters as well as digits and special characters. In* ‘Verify password’, *you repeat the password.*
- Optional comment ..: *Refer to the University of Copenhagen employee with whom you are collaborating (name + email) and specify which project.*
- I accept ..: *Read the ‘Terms and conditions’ and tick the box*

Click ‘Send’



UCPH SIF account request - with OpenID login

Please enter your information in at least the mandatory fields below and press the Send button to submit the account request to the UCPH SIF administrators.

IMPORTANT: we need to verify your identity, so please use an Email address clearly affiliated with your Organization!

Full name: Louise Outzen

Email address: louise@ecoknow.dk

Organization: EcoKnow

Country: Denmark

Optional state code: NA

Password: ••••••••••

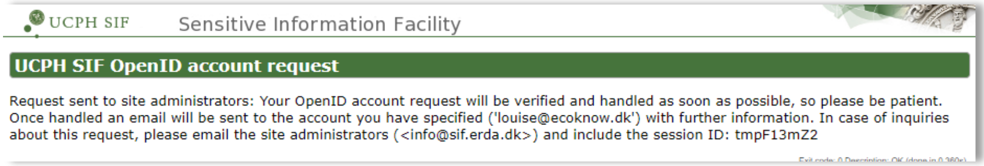
Verify password: ••••••••••

Optional comment or reason why you should be granted a UCPH SIF account:

For my collaboration with Martin Rehr (rehr@nbi.ku.dk) on The EcoKnow Project

I accept the UCPH SIF terms and conditions ☑

Your request to sign up as an SIF user will now be sent to the SIF administrators.



UCPH SIF OpenID account request

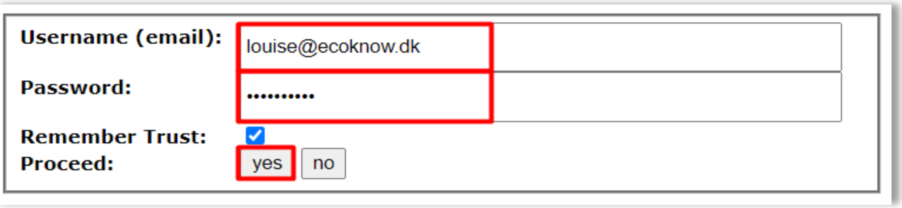
Request sent to site administrators: Your OpenID account request will be verified and handled as soon as possible, so please be patient. Once handled an email will be sent to the account you have specified ('louise@ecoknow.dk') with further information. In case of inquiries about this request, please email the site administrators (<info@sif.erda.dk>) and include the session ID: tmpF13mZ2

When the SIF administrators have accepted your request, you'll receive an email.

LOG IN

Click the link to SIF in the email and log in on SIF.

Enter your email address and your SIF password. Click ‘yes’.



Username (email): louise@ecoknow.dk

Password: ••••••••••

Remember Trust: ☑

Proceed:

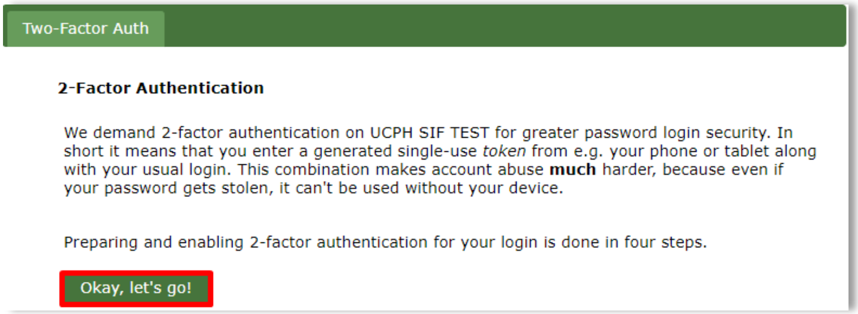
TWO-FACTOR AUTHENTICATION

To increase security, it is *compulsory* to use two-factor authentication for all SIF access.

With two-factor authentication, you add an extra control step to the login process which authenticates you. In addition to asking about something you know (in this case your username and password), an account protected by two-factor authentication will also request information about something you have (a token from app on mobile/tablet).

When you sign up for SIF, you must complete a one-time wizard to configure the compulsory two-factor authentication.

Click ‘Okay, let’s go!’



2-Factor Authentication

We demand 2-factor authentication on UCPH SIF TEST for greater password login security. In short it means that you enter a generated single-use *token* from e.g. your phone or tablet along with your usual login. This combination makes account abuse **much** harder, because even if your password gets stolen, it can't be used without your device.

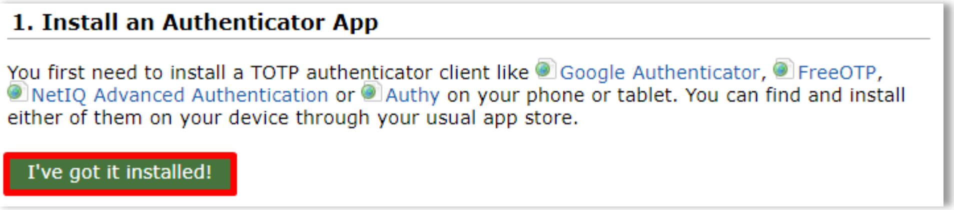
Preparing and enabling 2-factor authentication for your login is done in four steps.

A wizard will now appear in SIF which you must carefully follow.

STEP 1. DOWNLOAD APP

You have to download one of the following apps on your mobile or tablet: *Google Authenticator*, *FreeOTP*, *NetIQ Advanced*, *Authentication* or *Authy*. Find the app where you normally download apps.

Then click “I’ve got it installed”



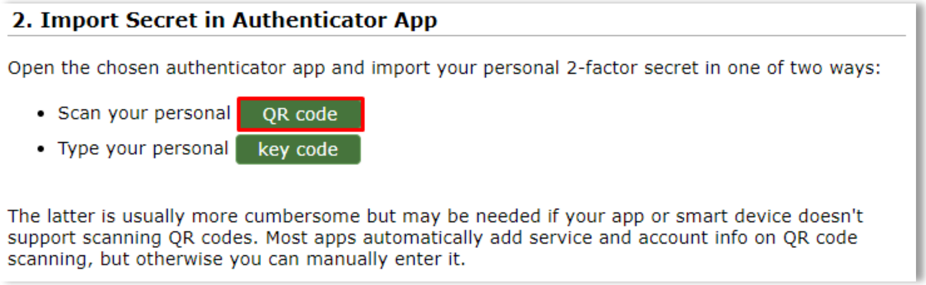
1. Install an Authenticator App

You first need to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Authy on your phone or tablet. You can find and install either of them on your device through your usual app store.

STEP 2. IMPORT PERSONAL TWO-FACTOR CODE

Import your personal two-factor code with ‘Scan your personal QR code’ or ‘Enter your personal key’. An example with ‘Scan your personal QR code’ follows below.

Click ‘QR code’ in SIF



2. Import Secret in Authenticator App

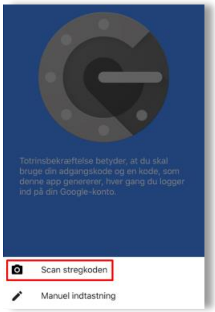
Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:

- Scan your personal QR code
- Type your personal key code

The latter is usually more cumbersome but may be needed if your app or smart device doesn't support scanning QR codes. Most apps automatically add service and account info on QR code scanning, but otherwise you can manually enter it.

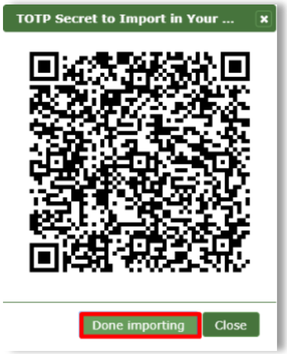
A QR code pops up in SIF:

Open your downloaded app.
The apps are slightly different. The screenshots shown below are from the *Google Authenticator* app. Click ‘Scan barcode’:



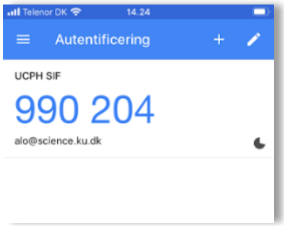
Totrinsbekræftelse betyder, at du skal bruge din adgangskode og en kode, som denne app genererer, hver gang du logger ind på din Google-konto.

Now scan the QR code you have just opened in the wizard on SIF. I.e. point the camera of your mobile at the QR code (the app may ask permission to use your camera). The app will now scan the QR code. Then click ‘Done importing’.



TOTP Secret to Import in Your ...

Your app can now generate six-digit tokens. In the example below, the token used is ‘990 204’.



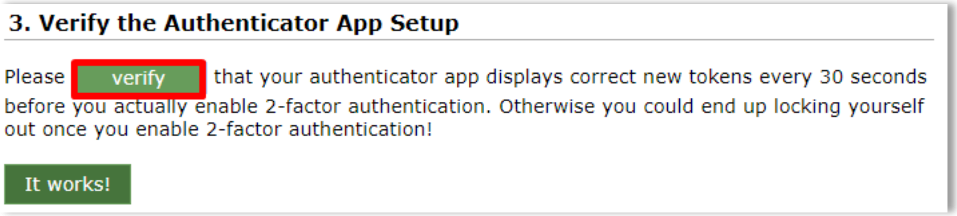
UCPH SIF

990 204

alo@science.ku.dk

STEP 3. VERIFY THAT IT WORKS

Next you need to check that your two-factor authentication has been set up correctly and that the app delivers the right one-off tokens.



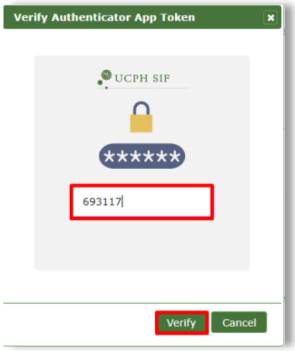
3. Verify the Authenticator App Setup

Please verify that your authenticator app displays correct new tokens every 30 seconds before you actually enable 2-factor authentication. Otherwise you could end up locking yourself out once you enable 2-factor authentication!

It works!

A pop-up window will appear, where you enter the token that the app displays (if it does not appear, click ‘verify’ in the above). Please note that the token changes after 30 seconds.

Enter the six-digit token and click the ‘Verify’ button in the pop-up window.



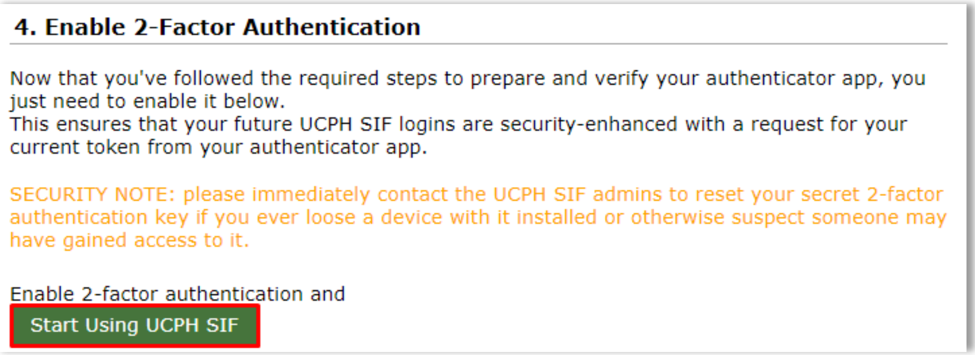
Verify Authenticator App Token

693117

If your two-factor authentication is successful, you will be taken directly to the next step.

STEP 4. ENABLE TWO-FACTOR AUTHENTICATION

Click ‘Start Using UCPH SIF’



4. Enable 2-Factor Authentication

Now that you've followed the required steps to prepare and verify your authenticator app, you just need to enable it below.
This ensures that your future UCPH SIF logins are security-enhanced with a request for your current token from your authenticator app.

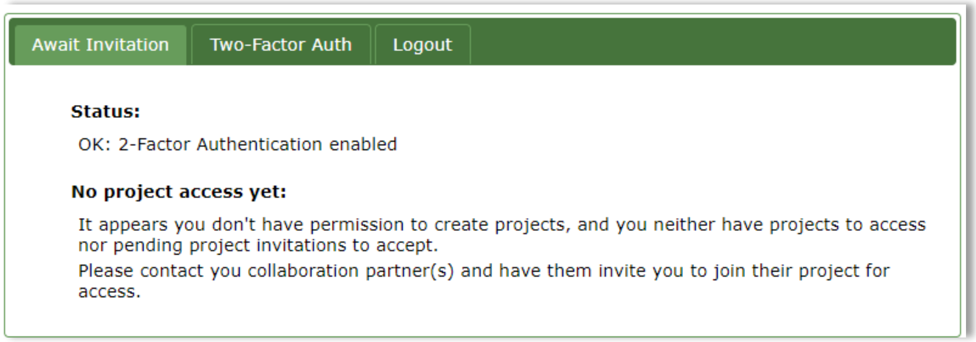
SECURITY NOTE: please immediately contact the UCPH SIF admins to reset your secret 2-factor authentication key if you ever loose a device with it installed or otherwise suspect someone may have gained access to it.

Enable 2-factor authentication and

Start Using UCPH SIF

YOU ARE NOW SIGNED UP

Congratulations! You are now signed up on SIF with two-factor authentication.



Status:

OK: 2-Factor Authentication enabled

No project access yet:

It appears you don't have permission to create projects, and you neither have projects to access nor pending project invitations to accept.
Please contact you collaboration partner(s) and have them invite you to join their project for access.

	Please await an invitation from your collaboration partner at University of Copenhagen to get project access. You will receive an email when this happens.
HELP	Read more guides and instructions at https://sif.ku.dk/ or get help at support@sif.erda.dk