

## 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

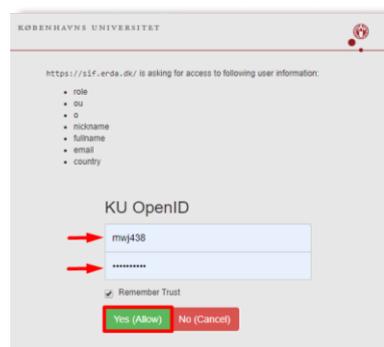
Go to [sif.ku.dk](http://sif.ku.dk)

Click 'sign up'



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)'



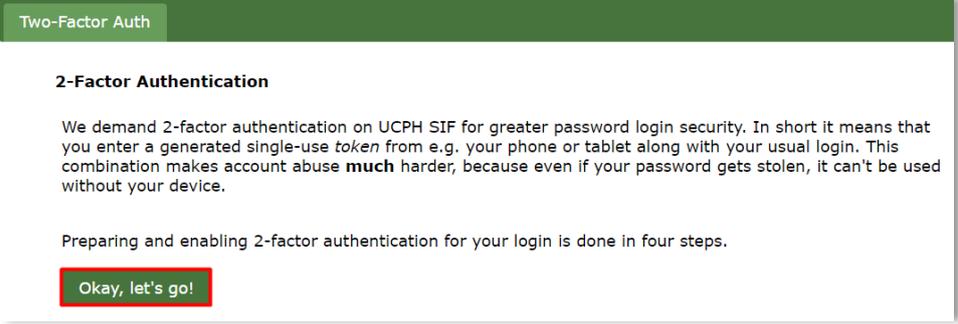
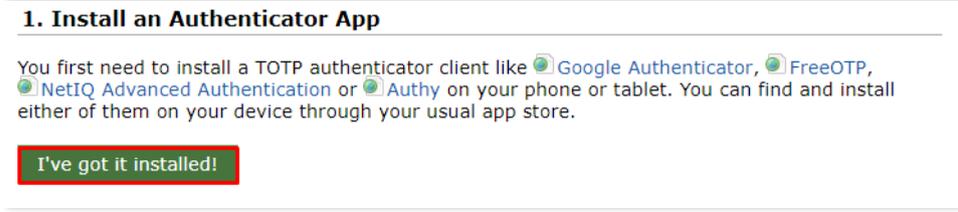
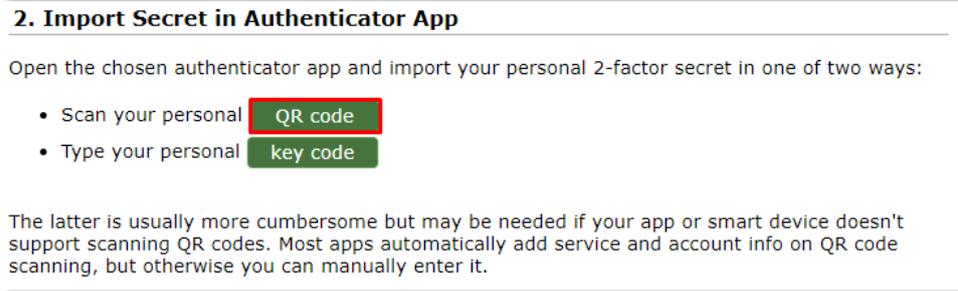
You are now registered as a SIF user.

### 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.

	<p>Click 'Okay, let's go!'</p>  <p>A wizard will now appear in SIF which you must carefully follow.</p>
<p><b>STEP 1. DOWNLOAD APP</b></p>	<p>You have to download one of the following apps on your mobile or tablet*: <i>Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Authy.</i> Find the app where you normally download apps.</p> <p>Then click "I've got it installed!"</p>  <p>*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 <a href="mailto:support@sif.erda.dk">support@sif.erda.dk</a> for further information.</p>
<p><b>STEP 2. IMPORT PERSONAL TWO- FACTOR CODE</b></p>	<p>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.</p> <p>Click 'QR code' in SIF.</p>  <p>A QR code pops up in SIF.</p>  <p>Open your downloaded app. The apps are slightly different. The screenshot shown below is from the</p>

Google Authenticator app. Click 'Scan barcode'.



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

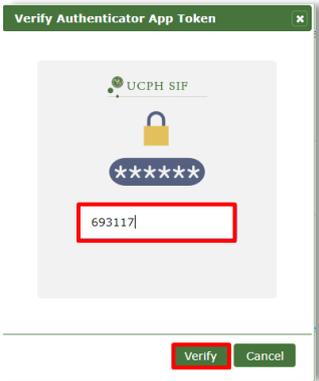
Next you need to check that your two-factor authentication has been set up correctly and that the app supplies the right tokens.

#### 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!

**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.

	<p>Enter the six-digit token and click the 'Verify' button in the pop-up window.</p>  <p>If your two-factor authentication is successful, you will be taken directly to the next step.</p>
<p><b>STEP 4. ENABLE TWO- FACTOR AUTHENTI- CATION</b></p>	<p>Click 'Start Using UCPH SIF'.</p> <div data-bbox="443 824 1410 1205" style="border: 1px solid #ccc; padding: 10px;"> <p><b>4. Enable 2-Factor Authentication</b></p> <p>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.</p> <p><b>SECURITY NOTE:</b> 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.</p> <p>Enable 2-factor authentication and</p> <p><b>Start Using UCPH SIF</b></p> </div>
<p><b>YOU ARE NOW SIGNED UP</b></p>	<p>Congratulations! You are now signed up on SIF with two-factor authentication.</p> <p>In the future, you can enter <a href="http://sif.ku.dk">sif.ku.dk</a> and log in using your UCPH username and personal UCPH password followed by two-factor authentication.</p> <p>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.</p>
<p><b>HELP</b></p>	<p>Read more guides and instructions at <a href="http://sif.ku.dk">sif.ku.dk</a> or get help at <a href="mailto:support@sif.erda.dk">support@sif.erda.dk</a></p>

# SIGN-UP FOR EXTERNAL COLLABORATION PARTNER

## SIGN UP

Go to [sif.ku.dk](http://sif.ku.dk)

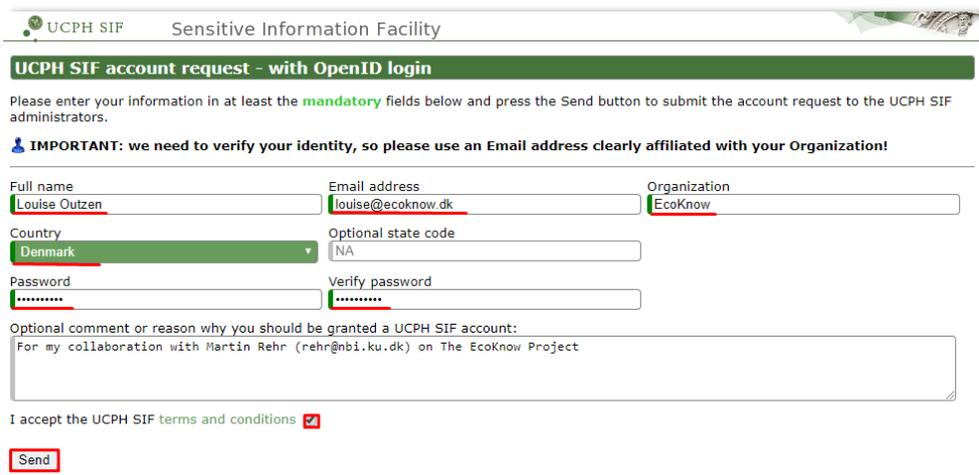
Click the 'External Users' tab. Then click 'sign up':



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*

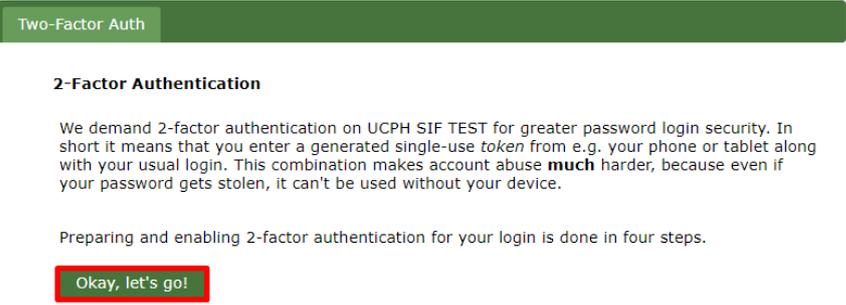
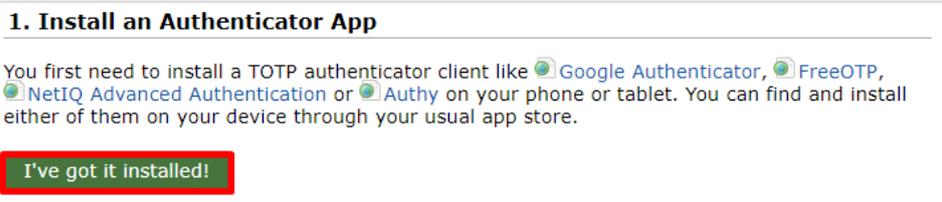
Click 'Send'

A screenshot of a web form titled 'UCPH SIF account request - with OpenID login'. The form is for sensitive information and includes fields for Full name (Louise Outzen), Email address (louise@ecoknow.dk), Organization (EcoKnow), Country (Denmark), and Password. There is also a field for an optional comment and a checkbox for accepting terms and conditions. A 'Send' button is at the bottom.

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

A screenshot of a confirmation page titled 'UCPH SIF OpenID account request'. It states that the request has been sent to site administrators and will be handled as soon as possible. It provides contact information for site administrators and includes a session ID: tmpF13mZ2.

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

<p><b>LOG IN</b></p>	<p>Click the link to SIF in the email and log in on SIF.</p> <p>Enter your email address and your SIF password. Click 'yes'.</p>  <p>The screenshot shows a login form with the following fields: 'Username (email):' containing 'louise@ecoknow.dk', 'Password:' containing '.....', 'Remember Trust:' with a checked checkbox, and 'Proceed:' with 'yes' and 'no' buttons. The 'yes' button is highlighted with a red box.</p>
<p><b>TWO-FACTOR AUTHENTICATION</b></p>	<p>To increase security, it is <i>compulsory</i> to use two-factor authentication for all SIF access.</p> <p>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).</p> <p>When you sign up for SIF, you must complete a one-time wizard to configure the compulsory two-factor authentication.</p> <p>Click 'Okay, let's go!'</p>  <p>The screenshot shows a 'Two-Factor Auth' wizard page. It has a title '2-Factor Authentication' and explains that UCPH SIF TEST requires 2-factor authentication for security. It states that this makes account abuse much harder. Below the text, it says 'Preparing and enabling 2-factor authentication for your login is done in four steps.' and features a button labeled 'Okay, let's go!' which is highlighted with a red box.</p> <p>A wizard will now appear in SIF which you must carefully follow.</p>
<p><b>STEP 1. DOWNLOAD APP</b></p>	<p>You have to download one of the following apps on your mobile or tablet: <i>Google Authenticator, FreeOTP, NetIQ Advanced, Authentication or Authy.</i> Find the app where you normally download apps.</p> <p>Then click "I've got it installed"</p>  <p>The screenshot shows the first step of the wizard: '1. Install an Authenticator App'. It instructs the user to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication, or Authy. It says 'You can find and install either of them on your device through your usual app store.' Below the text is a button labeled 'I've got it installed!' which is highlighted with a red box.</p>
<p><b>STEP 2. IMPORT PERSONAL TWO-FACTOR CODE</b></p>	<p>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.</p> <p>Click 'QR code' in SIF</p>

## 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':



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 delivers the right one-off tokens.

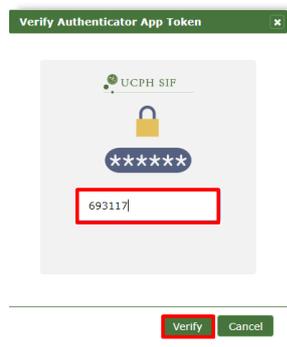
**3. Verify the Authenticator App Setup**

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.



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

**STEP 4.  
ENABLE  
TWO-  
FACTOR  
AUTHENTI-  
CATION**

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.

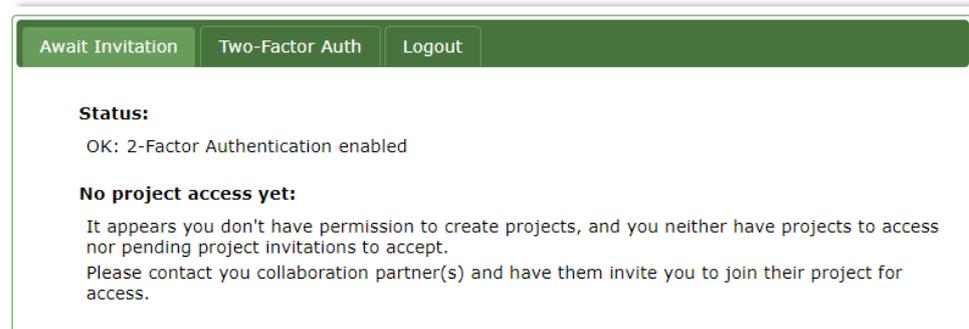
**SECURITY NOTE:** please immediately contact the UCPH SIF admins to reset your secret 2-factor authentication key if you ever loose a device with it installed or otherwise suspect someone may have gained access to it.

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.



	<p>Please await an invitation from your collaboration partner at University of Copenhagen to get project access.</p> <p>You will receive an email when this happens.</p>
<b>HELP</b>	<p>Read more guides and instructions at <a href="http://sif.ku.dk">sif.ku.dk</a> or get help at <a href="mailto:support@sif.erd.dk">support@sif.erd.dk</a></p>