SIGN UP AS AN ERDA USER

As a UCPH employee/student (see pages 1-5) or an external collaboration partner (see pages 6-11), you must sign up as a user before you can access ERDA. In addition, you have the option of further protecting your account by logging in with two-factor authentication.

SIGN UP WITH A UCPH ACCOUNT

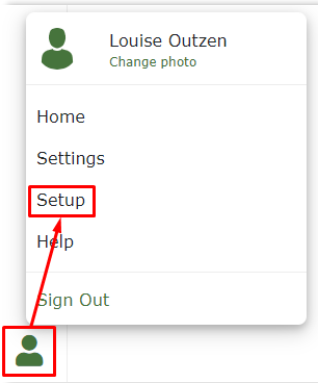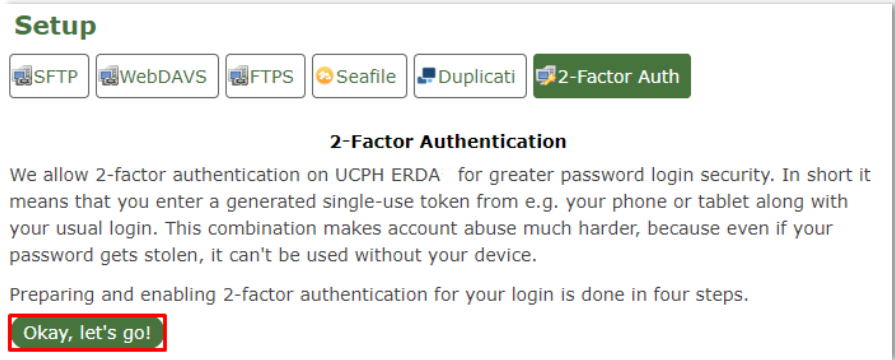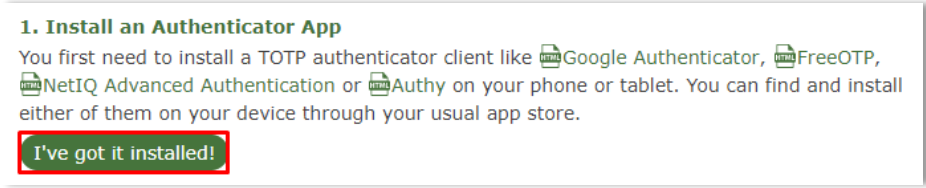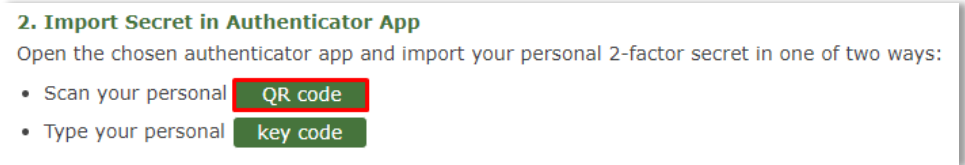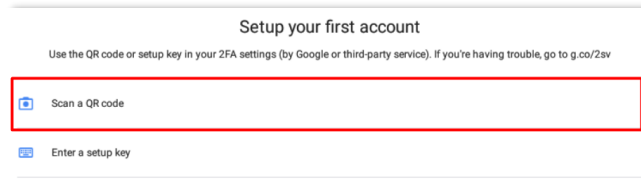|	
SIGN UP	Go to erda.ku.dk. Click "sign up". **Welcome to UCPH ERDA** KU / UCPH Users External Users Advanced Access Sign up to ERDA using your KU / UCPH account? sign up I'm already signed up to ERDA with my KU / UCPH account! log in In the pop-up window under "UCPH OpenID", enter: 1. Your UCPH username (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)" KØBENHAVNS UNIVERSITET https://erda.dk/ is asking for access to following user information: • role • ou • o • nickname • fullname • email • country KU OpenID mwj438 ●●●●●●●●●● ☑ Remember Trust Yes (Allow) No (Cancel) The site https://erda.dk/ has requested verification of your OpenID. You are now registered as an ERDA user.
TWO-FACTOR AUTHENTICATION	To increase security, we recommend that you use two-factor authentication for all ERDA access. With two-factor authentication, you add an extra verification 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 phone/tablet). When setting up two-factor authentication, you must complete a one-time wizard.

	Click the green avatar in the bottom left corner. Click "Setup".
	Click "Okay, let's go!"
	A wizard will now appear in ERDA which you must follow closely.
STEP 1. DOWNLOAD APP	You need to download one of the following apps on your mobile phone 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!"
	*If you only have a private mobile phone/tablet and you do not want to use it, you may request a small device that you can use instead. Contact support@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 "Type your personal key code". An example with "Scan your personal QR code" follows below.
	Click "QR code"

A QR code pops up in ERDA.
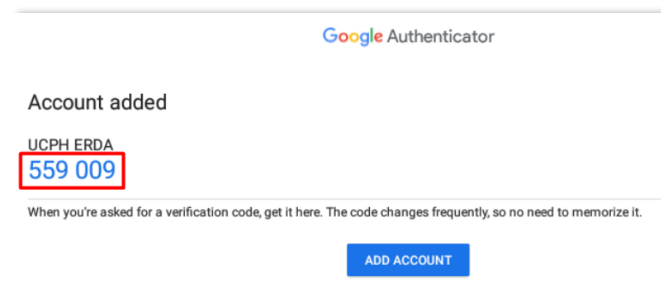

Open your downloaded app.
The apps are slightly different. The screenshot below is from the *Google Authenticator* app*.* Click "Scan a QR code".

Now scan the QR code you have just opened in the wizard on ERDA. I.e. point your mobile phone camera at the QR code (the app may ask for permission to use your camera). Now the app scans the QR code. Then click "Done importing".

Your app can now generate six-digit tokens. In the example below, the token used is "559 009".

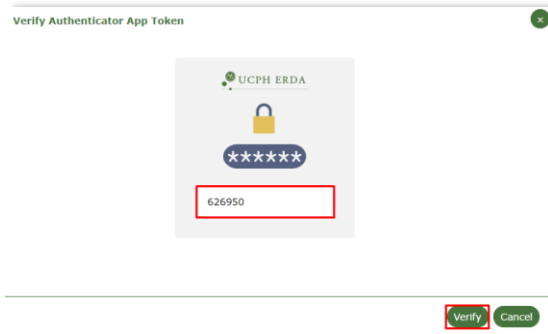| STEP 3. VERIFY THAT IT WORKS	Next, you need to check that your two-factor authentication has been set up correctly and that the app supplies the right tokens.

A pop-up window automatically appears, and you must enter the token which the app displays (if it does not appear, click "verify" above). Please note that the token changes after 30 seconds.

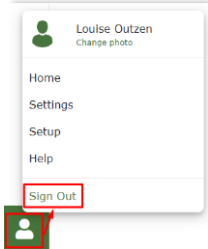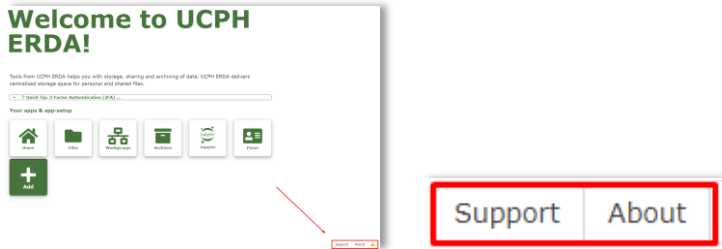|	
	Enter the temporal six-digit token and click the "Verify" button in the pop-up window. **Verify Authenticator App Token** UCPH ERDA 🔒 ✱✱✱✱✱ 626950 Verify Cancel If your two-factor authentication is successful, you will be taken directly to the next step.
STEP 4. ENABLE TWO-FACTOR AUTHENTICATION	Tap the slider button under "Enable 2-FA for KU/UCPH OpenID web login" to switch it from grey to green. **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 for login below. This ensures that your future UCPH ERDA logins are security-enhanced with a request for your current token from your authenticator app. SECURITY NOTE: please immediately contact the UCPH ERDA 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-FA for KU/UCPH OpenID web login** Add an extra layer of security to your KU/UCPH OpenID web logins through a personal auth token generator on your phone or tablet. **Enable 2-FA for Non-KU/UCPH OpenID web login** Add an extra layer of security to your Non-KU/UCPH OpenID web logins through a personal auth token generator on your phone or tablet. Additional two-factor authentication options for WebDAVS, SFTP and FTPS are now shown. These are protocols which you primarily need if you want to use ERDA as a network drive on your own computer. If you are not sure whether you are going to use ERDA as a network drive, we recommend that you activate all three slider buttons by switching them to green. **Enable 2-FA for WebDAVS network drive or client login** Add an extra layer of security to your WebDAVS logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into WebDAVS as usual. **Enable 2-FA for SFTP network drive or client login with password** Add an extra layer of security to your SFTP password logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into SFTP as usual. **Enable 2-FA for FTPS network drive or client login** Add an extra layer of security to your FTPS logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into FTPS as usual. Click "Save 2-Factor Auth Settings". Save 2-Factor Auth Settings Your ERDA account is now protected with two-factor authentication.

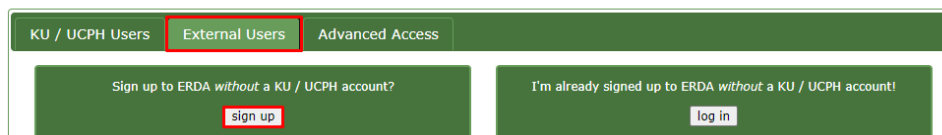|	From now on, you can enter erda.ku.dk and log in using your UCPH username and personal UCPH password followed by two-factor authentication with a six-digit token.
SIGN OUT	When you are done working in ERDA, please remember to always click "Sign Out" in the bottom left corner. This way, you ensure that no one else can gain unauthorised access to your data.
FURTHER INFO	Under the "Support" and "About" buttons in the bottom right corner, you can find guides, get answers to frequently asked questions and read more about ERDA etc. You can also find information about current or announced disruptions. A green check mark means that the system is running according to plan, while, for example, an orange triangle warning sign means that there are disruptions at the moment. You can click the status icon for more information.
HELP	Get help at support@erda.dk.

SIGN UP FOR EXTERNAL COLLABORATION PARTNER	
SIGN UP	Go to erda.ku.dk.
	Click the "External Users" tab and then click "sign up".

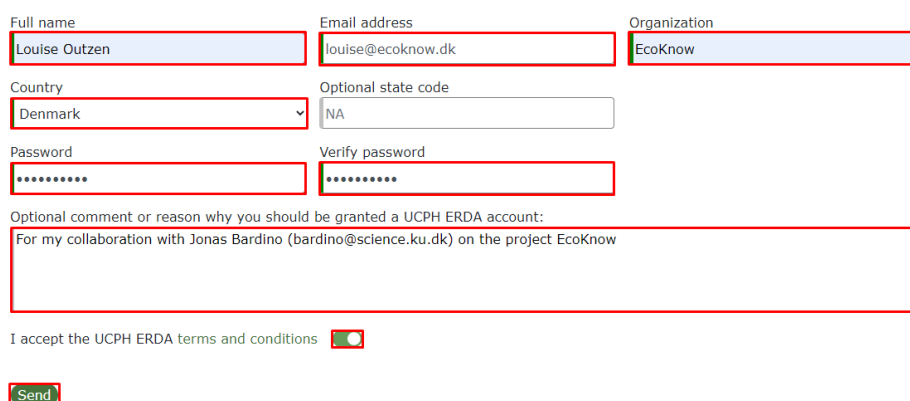Please complete the form with your details:

- 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 ERDA access. It must consist of at least eight characters and must contain a combination of lowercase and uppercase letters, digits and special characters (at least three of the four types mentioned). In "Verify password", you repeat the password*
- Optional comment ..: *Refer to your contact who is employed at the University of Copenhagen (name + email) and indicate any relevant project, course or collaboration.*
- I accept ..: *Read the "terms and conditions" and tick the box*

Click "Send".

Your request to sign up as an ERDA user will now be sent to the ERDA administrators, who will obtain consent from the UCPH employee regarding the collaboration.

UCPH ERDA 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 (ERDA Info <info@erda.dk>) and include the session ID: tmpw9tuon

When the ERDA administrators have accepted your request, you will receive an email.

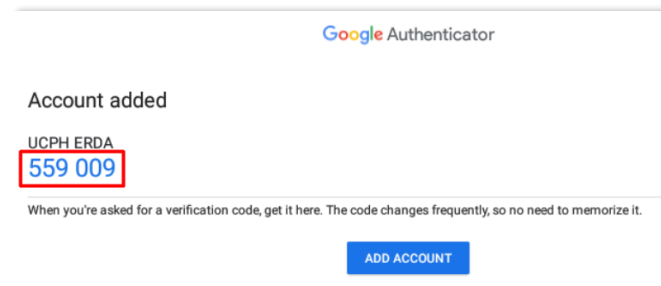|	
LOG IN	Click the link to ERDA in the email and log in to ERDA. Enter your email address and your ERDA password. Click "yes". **UCPH ERDA OpenID Login** Username (email): louise@ecoknow.dk Password: •••••••••• Remember Trust: ☑ Proceed: yes no
TWO-FACTOR AUTHENTICATION	To increase security, we recommend that you use two-factor authentication for all ERDA access. With two-factor authentication, you add an extra verification 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 phone/tablet). When setting up two-factor authentication, you must complete a one-time wizard. Click the green avatar in the bottom left corner. Click "Setup". Louise Outzen Change photo Home Settings Setup Help Sign Out

	Click "Okay, let's go!" **Setup** [SFTP] [WebDAVS] [FTPS] [Seafile] [Duplicati] [2-Factor Auth] **2-Factor Authentication** We allow 2-factor authentication on UCPH ERDA* 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. **Okay, let's go!** A wizard will now appear in ERDA which you must follow closely.
STEP 1. DOWNLOAD APP	You need to download one of the following apps on your mobile phone 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 [HTML]Google Authenticator, [HTML]FreeOTP, [HTML]NetIQ Advanced Authentication or [HTML]Authy on your phone or tablet. You can find and install either of them on your device through your usual app store. **I've got it installed!**
STEP 2. IMPORT PERSONAL TWO-FACTOR CODE	Import your personal two-factor code with "Scan your personal QR code" or "Type your personal key code". An example with "Scan your personal QR code" follows below. Click "QR code". **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** A QR code pops up in ERDA. Open your downloaded app. The apps are slightly different. The screenshot below is from the *Google Authenticator* app. Click "Scan a QR code". **Setup your first account** Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv [ ] Scan a QR code [ ] Enter a setup key

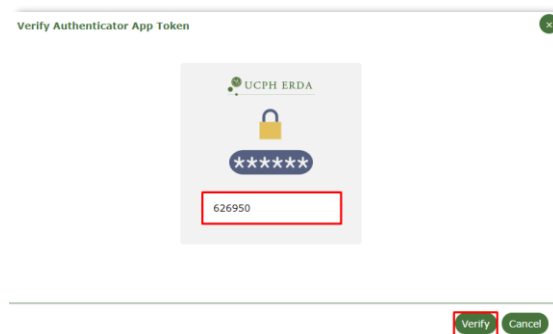|	
	Now scan the QR code you have just opened in the wizard on ERDA. I.e. point your mobile phone camera at the QR code (the app may ask for permission to use your camera). Now the app scans the QR code. Then click "Done importing". Your app can now generate six-digit tokens. In the example below, the token used is "559 009".
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. A pop-up window automatically appears, and you must enter the token which the app displays (if it does not appear, click "verify" above). Please note that the token changes after 30 seconds. Enter the temporal 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.

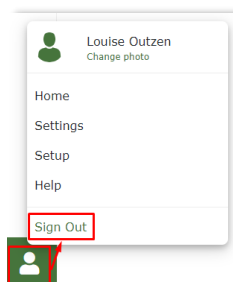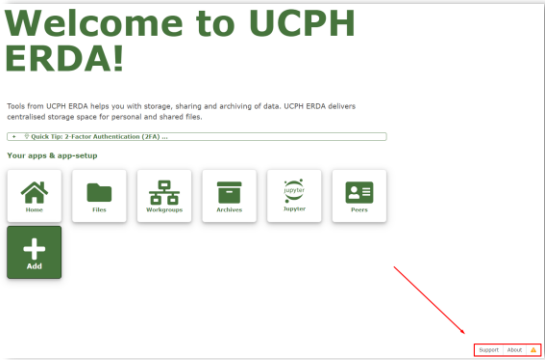|	
STEP 4. ENABLE TWO-FACTOR AUTHENTI-CATION	Tap the slider button under "Enable 2-FA for Non-KU/UCPH OpenID web login" to switch it from grey to green. **4. Enable 2-Factor Authentication** Now that you've followed the required steps to prepare and verify your authenticator app, you just need to enable it for login below. This ensures that your future UCPH ERDA logins are security-enhanced with a request for your current token from your authenticator app. SECURITY NOTE: please immediately contact the UCPH ERDA 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-FA for Non-KU/UCPH OpenID web login** Add an extra layer of security to your Non-KU/UCPH OpenID web logins through a personal auth token generator on your phone or tablet. **Enable 2-FA for KU/UCPH OpenID web login** Add an extra layer of security to your KU/UCPH OpenID web logins through a personal auth token generator on your phone or tablet. Additional two-factor authentication options for WebDAVS, SFTP and FTPS are now shown. These are protocols which you primarily need if you want to use ERDA as a network drive on your own computer. If you are not sure whether you are going to use ERDA as a network drive, we recommend that you activate all three slider buttons by switching them to green. **Enable 2-FA for WebDAVS network drive or client login** Add an extra layer of security to your WebDAVS logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into WebDAVS as usual. **Enable 2-FA for SFTP network drive or client login with password** Add an extra layer of security to your SFTP password logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into SFTP as usual. **Enable 2-FA for FTPS network drive or client login** Add an extra layer of security to your FTPS logins through a personal auth token generator on your phone or tablet. Works by logging in to the UCPH ERDA web site with 2FA enabled to start an authenticated session and then logging into FTPS as usual. Click "Save 2-Factor Auth Settings". **Save 2-Factor Auth Settings** Your ERDA account is now protected with two-factor authentication. From now on, you can enter erda.ku.dk and log in using your email address and password followed by two-factor authentication with a six-digit token.
SIGN OUT	When you are done working in ERDA, please remember to always click "Sign Out" in the bottom left corner. This way, you ensure that no one else can gain unauthorised access to your data. Louise Outzen Change photo Home Settings Setup Help Sign Out

FURTHER INFO	Under the "Support" and "About" buttons in the bottom right corner, you can find guides, get answers to frequently asked questions and read more about ERDA etc. You can also find information about current or announced disruptions. A green check mark means that the system is running according to plan, while, for example, an orange triangle warning sign means that there are disruptions at the moment. You can click the status icon for more information.
HELP	Get help at support@erda.dk.