

## REGISTER YOURSELF AS AN ERDA USER

Employees and students at AU (see pages 1-5) as well as collaboration partners (see pages 6-11) must register on ERDA before they can access a project. You can also secure your account by setting up 2-factor authentication.

## REGISTRATION WITH AN AU ACCOUNT

### REGISTER

Go to <https://erda-test.au.dk/> and click on 'Sign up for ERDA with an AU account?' If you are already logged in to your AU account, the next step will happen automatically. Otherwise, you must approve login via your Microsoft Authenticator app.



You have now registered as a user on ERDA.

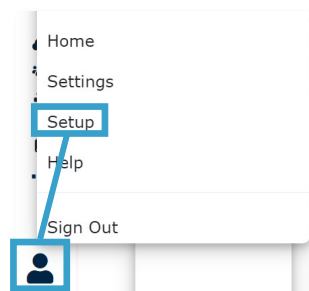
### 2-FACTOR AUTHENTICATION

For added security, we recommend that you secure your ERDA account with 2-factor authentication.

2-factor authentication adds an extra control step to your login: it asks for something you know (your username and password) as well as something you have (a number key from an app).


To enable 2-factor authentication, you will have to go through set up once.

Click on the profile icon in the bottom left-hand corner. Click on Setup.



A guide will pop up in ERDA, and you should follow it closely.

Click 'OK, let's go!'

	<div data-bbox="443 241 1350 479"> <p><b>Setup</b></p> <p>SFTP WebDAVS FTPS Duplicati <b>2-Factor Auth</b></p> <p><b>2-Factor Authentication</b></p> <p>We allow 2-factor authentication on 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.</p> <p>Preparing and enabling 2-factor authentication for your login is done in four steps.</p> <p><b>Okay, let's go!</b></p> </div>
<p><b>STEP 1: DOWNLOAD APP</b></p>	<p>Open <i>Microsoft Authenticator</i>, which is the app generally used by AU for 2-factor authentication.</p> <p>Then click 'I've got it installed!'</p> <div data-bbox="443 680 1401 792"> <p><b>1. Install an Authenticator App</b></p> <p>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.</p> <p><b>I've got it installed!</b></p> </div>
<p><b>STEP 2. IMPORT PERSONAL 2-FACTOR CODE</b></p>	<p>Click 'Scan your personal QR code' or 'Enter your personal key'. In the example below, we are using 'Scan your personal QR code': click 'QR code'.</p> <div data-bbox="443 992 1401 1149"> <p><b>2. Import Secret in Authenticator App</b></p> <p>Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:</p> <ul style="list-style-type: none"> <li>• Scan your personal <b>QR code</b></li> <li>• Type your personal <b>key code</b></li> </ul> </div> <p>A QR code similar to the one you can see here will pop up.</p>  <p>Click on 'Legitimationsoplysninger' in the bottom right-hand corner of <i>Microsoft Authenticator</i>.</p> <div data-bbox="437 1420 906 1541"> <p>Få mere at vide om V...gitimationsoplysninger</p> <p>Authenticator Adgangskoder Adresser <b>Legitimationsopi...</b></p> </div> <p>Now click on 'Scan en QR-kode'.</p>



Scan the QR code in ERDA: aim your phone's camera at the QR code (the app may need permission to use the camera), and the app will scan the code itself.

Then click 'Done importing' in ERDA.



Your app can now generate six-digit single-use passwords. You can find them on the front page of *Microsoft Authenticator*, under Aarhus University. In our example, the code is '472 580'.



### STEP 3. VERIFY THAT IT WORKS

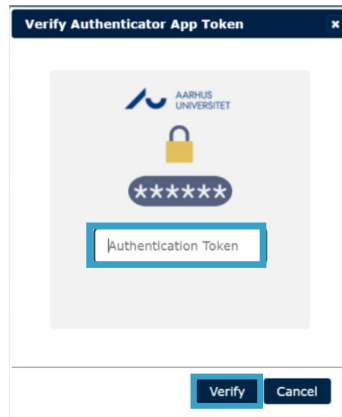
Now you need to test that your 2-factor authentication is correctly set up and that the app supplies the right tokens.

### 3. Verify the Authenticator App Setup

Please  that your authenticator app displays correct number that you are locking yourself out once you enable 2-factor authentication!

ERDA will display a pop-up window in which you have to enter the token displayed by the app (if the window does not pop up, click 'verify'). Please note that the token changes every 30 seconds.

Enter the token in ERDA and click 'Verify'.



If the 2-factor authentication is successful, you will be taken to the next step. If it is not successful, contact your local IT-support, and they will help you.

## STEP 4. ENABLE 2- FACTOR AUTHENTI- CATION

Switch on the button under 'Enable 2-FA for AU Web login' so it changes from grey to blue.

Now you can add additional 2-factor authentication by using WebDAVS, SFTP and FTPS. These protocols are mostly relevant if you want to use ERDA as a network drive on your own computer.

If you are unsure whether to use ERDA as a network drive, we recommend that you switch on all the buttons, turning them blue.

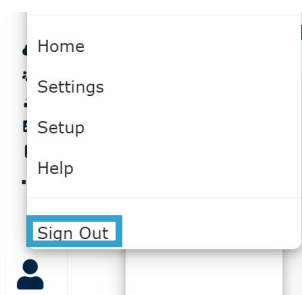
Click on 'Save 2-Factor Auth Settings'

Your ERDA account is now secured with 2-factor authentication.

In the future, you can go to <https://erda.au.dk>, log in with your AU username and code, and then 2-factor authentication with a six-digit token.

## LOG OUT

Always click 'Sign Out' in the bottom left-hand corner when you have finished working in ERDA, to ensure that no one can access your data without authorisation.



## READ MORE

Click on 'Support' and 'About' in the bottom right-hand corner for more guidelines and answers to frequently asked questions and to read more about ERDA.

**Welcome to ERDA!**

Tools from ERDA helps you with storage, sharing and archiving of data. ERDA delivers centralised storage space for personal and shared files.

Quick Tip: Cloud File Sync like Dropbox, OneDrive, etc. ...

Your apps & app-setup

Home Files Projects Archives Share Links Add

Support | About

You can also see current or upcoming service interruptions here. A green tick means that the system is running according to plan, while an orange warning triangle, for example, means that there are current interruptions. Click on the status icon to read more.

## HELP

For personal help, you can reach us at [erda-info.it@au.dk](mailto:erda-info.it@au.dk)

## REGISTRATION FOR EXTERNAL COLLABORATION PARTNERS

### REGISTER

Go to <https://erda-test.au.dk/>, click the 'Eksterne brugere' tab and then 'Tilmeld dig ERDA uden en AU-konto?'

#### Velkommen til ERDA

The screenshot shows a dark blue header with three tabs: 'AU brugere', 'Eksterne brugere' (highlighted), and 'Avanceret adgang'. Below the tabs are two buttons. The first button is labeled 'Tilmeld dig ERDA uden en AU-konto?' and has a 'tilmelding' button below it. The second button is labeled 'Jeg er allerede tilmeldt ERDA uden en AU-konto?' and has a 'log ind' button below it.

Complete the form with your data:

- Full name: *Your full name*
- Email address: *Your work email (no third-party services such as hotmail, gmail or yahoo)*
- Organisation: *Name of your workplace/company*
- Country: *Select your country from the drop-down menu*
- Password: *Find a sufficiently difficult password consisting of at least 10 characters with both lower-case and upper-case letters, numbers and special characters. Repeat the password in 'Verify password'.*
- Optional comment: *Enter the name and email of the AU employee you are working with, and the name of your project.*
- I accept: *Read 'terms and conditions' and tick the box*

Click 'Send'

#### ERDA account request - with OpenID login

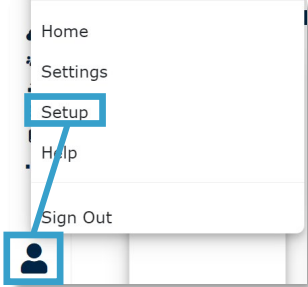
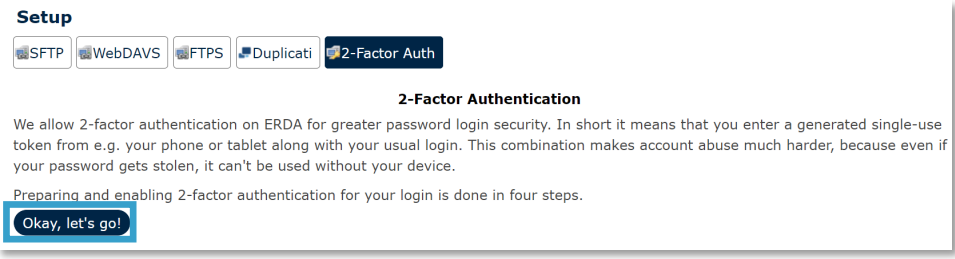

Please enter your information in at least the **mandatory** fields below and press the Send button to submit the account request to the ERDA administrators.

**IMPORTANT:** we need to identify and notify you about login info, so please use a working Email address clearly affiliated with your Organization!

The form contains the following fields and elements:

- Full name:
- Email address:
- Organization:
- Country:
- Optional state code:
- Password:
- Verify password:
- Comment with reason why you should be granted a ERDA account:
- I accept the ERDA terms and conditions:
- Send button:

Your request to be an ERDA user will be sent to the administrators.

	<p><b>ERDA OpenID account request</b></p> <p>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 ('samawe@au.dk') with further information. In case of inquiries about this request, please email the site administrators (ERDA Info &lt;erda-admin.it@au.dk&gt;) and include the session ID: tmpsZ0HGn</p> <p>Once they have accepted your request, they will send you an email.</p>
<p><b>LOGIN</b></p>	<p>Click on the link in the email from ERDA to access login. Enter your email and your ERDA password and click 'yes'.</p>
<p><b>2-FACTOR AUTHENTICATION</b></p>	<p>To increase security, we recommend that you secure your ERDA account with 2-factor authentication.</p> <p>2-factor authentication adds an extra control step to your login: it asks about something you know (your username and password) and something you have (a number key from an app).</p> <p>To set up 2-factor authentication, you will have to go through a guide once.</p> <p>Click on the profile icon in the bottom left-hand corner. Click on Setup.</p>  <p>A guide will then pop up in ERDA, and you should follow this closely.</p> <p>Click 'OK, let's go!'</p> 
<p><b>STEP 1: DOWNLOAD APP</b></p>	<p>Open <i>Microsoft Authenticator</i>, which is the app generally used by AU for 2-factor authentication. You can also use <i>Google Authenticator</i>, <i>FreeOTP</i>, <i>NetIQ Advanced Authentication</i> or <i>Athy</i>. Find them where you normally download apps.*</p> <p>Then click 'I've got it installed!'</p> <p><b>1. Install an Authenticator App</b></p> <p>You first need to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Athy on your phone or tablet. You can find and install either of them on your device through your usual app store.</p>  <p>*If you only have access to a private mobile phone/tablet and you don't want to</p>

use it, you can borrow one from us instead. Contact [support@sif.erda.dk](mailto:support@sif.erda.dk)

## STEP 2. IMPORT PERSONAL 2- FACTOR CODE

Click 'Scan your personal QR code' or 'Enter your personal key'. In the example below, we are using 'Scan your personal QR code': 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 similar to the one you can see here will pop up.



Click on 'Legitimationsoplysninger' in the bottom right-hand corner of *Microsoft Authenticator*.



Now click on 'Scan en QR-kode'.



Scan the QR code in ERDA: Aim your phone camera at the QR code (the app may need permission to use the camera), and the app will scan the code itself.

Then click 'Done importing' in ERDA.





Your app can now generate six-digit one-time passwords. You can find them on the front page of *Microsoft Authenticator*, under Aarhus University. In our example, the code is '472 580'.



### STEP 3. VERIFY THAT IT WORKS

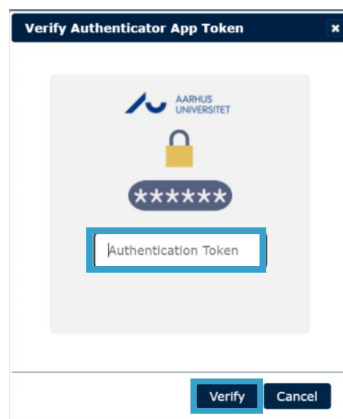
Now you need to test that your 2-factor authentication is correctly set up and that the app supplies the right tokens.

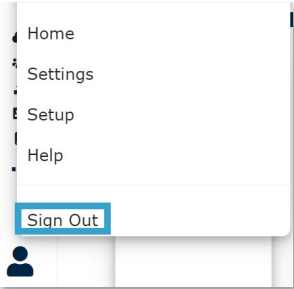
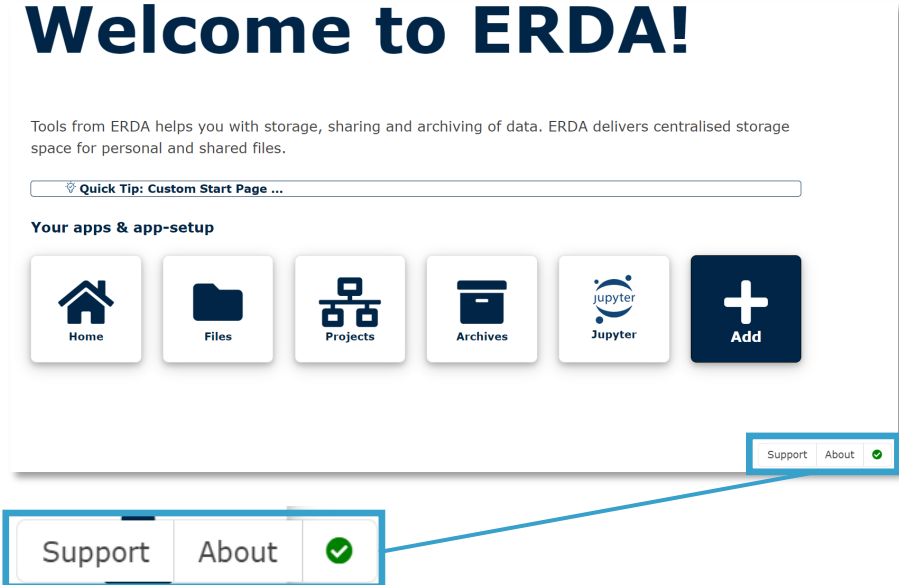
ERDA will display a pop-up window in which you have to enter the token displayed by the app (if the window does not pop up, click on 'verify'). NB: The token will change after 30 seconds.

#### 3. Verify the Authenticator App Setup

Please **verify** that your authenticator app displays correct notifications, locking yourself out once you enable 2-factor authentication!

Enter the token in ERDA and click 'Verify'.



	<p>If the 2-factor authentication is successful, you will be taken to the next step. If it is not successful, we recommend that you try with one of the other apps (<i>Google Authenticator, FreeOTP, NetIQ Advanced, Authentication or Authy</i>). If it still doesn't work, please contact AskOS, and we'll help you.</p>
<p><b>STEP 4. ENABLE 2- FACTOR AUTHENTI- CATION</b></p>	<p>Click the button under 'Enable 2-FA for AU Web login' to switch from grey to blue.</p> <p>Now you can add additional 2-factor authentication by using WebDAVS, SFTP and FTPS. These protocols are usually relevant if you want to use ERDA as a network drive on your own computer.</p> <p>If you are unsure whether to use ERDA as a network drive, we recommend that you click on all the buttons to make them blue.</p> <p>Click on 'Save 2-Factor Auth Settings'</p> <p>Your ERDA account is now secured with 2-factor authentication.</p> <p>In the future, you can go to <a href="https://erda-test.au.dk">https://erda-test.au.dk</a>, log in with your AU username and password, and then 2-factor authentication with a six-digit token.</p>
<p><b>LOG OUT</b></p>	<p>Always click 'Sign Out' in the bottom left-hand corner when you have finished working in ERDA, so that you're sure that no one can access your data without authorisation.</p> 
<p><b>READ MORE</b></p>	<p>Click on 'Support' and 'About' in the bottom right-hand corner for more guidelines and answers to frequently asked questions and to read more about ERDA.</p> 

	<p>You can also see current or upcoming service interruptions here. A green tick means that the system is running according to plan, while an orange warning triangle, for example, means that there are current interruptions. Click on the status icon to read more.</p>
<b>HELP</b>	<p>Find out more at <a href="https://erda-test.au.dk/">https://erda-test.au.dk/</a> or for personal help go to <a href="mailto:support@sif.erd.dk">support@sif.erd.dk</a></p>