

REGISTER YOURSELF AS AN ERDA USER

Since ERDA uses the central user database for user validation, all AU-employees can create an ERDA-account.

In other words, you sign up to ERDA with the same username and password you use for your AU computer, email and internal websites.

Here, we walk through sign up for ERDA as an internal user, as an external user, and adding 2-factor authentication on your ERDA account.

SIGN UP WITH AN AU ACCOUNT

SIGN-UP

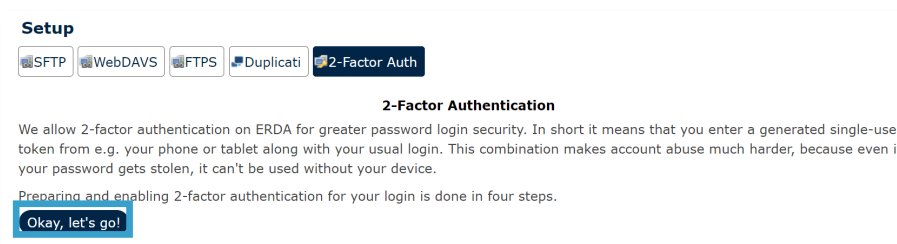
- Go to [ERDA's front page](#)
- Click on **Sign up for ERDA with an AU account?**
- Approve login via your Microsoft Authenticator app on your phone. If you are already logged in to your AU account, no approval is needed.
- You are now registered as an ERDA user.



2-FACTOR AUTHENTICATION

Due to the increasing risk of cyberattack, we recommend securing your ERDA account with 2-factor authentication. 2-factor authentication adds a step to login, demanding username, password, and a single-use numerical code.

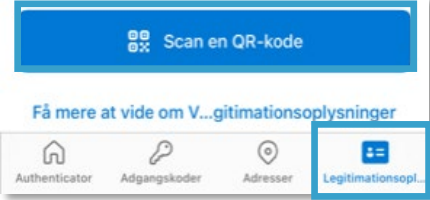
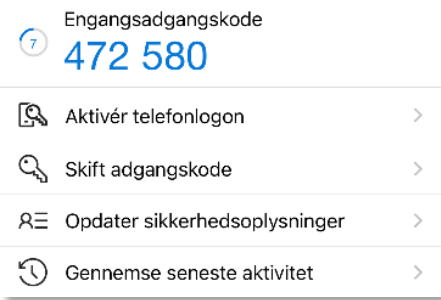
- Click the person icon at the bottom left corner of ERDA.
- Open ERDA and click **Setup** and the **2-Factor auth** banner.
- Click **Okay, let's go**.

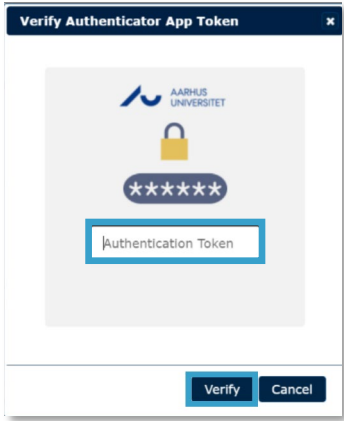


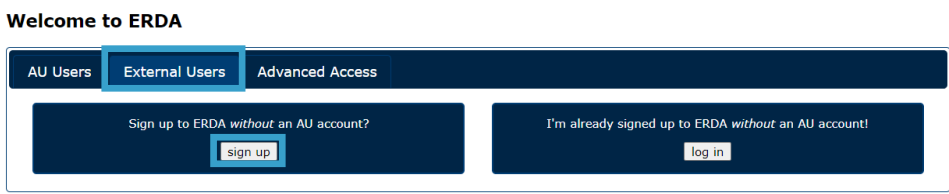
STEP 1: DOWN-LOAD APP

Open **Microsoft Authenticator**, the AU-approved app for 2-factor authentication. Find the app in your appstore, if it's not installed on your device.

Click **I've got it installed** in ERDA.

	<p>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.</p> <p>I've got it installed!</p>
<p>STEP 2: IMPORT PERSONAL CODE</p>	<p>To import a code in ERDA, either scan a QR-code or enter the key manually. If your device has a camera, scanning is by far the easiest way.</p> <p>Click Scan your personal QR code in ERDA.</p> <p>2. Import Secret in Authenticator App Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:</p> <ul style="list-style-type: none"> • Scan your personal QR code • Type your personal key code <p>ERDA will now open a window with a QR-code.</p> <ul style="list-style-type: none"> • Click Legitimation Information at the bottom right of Microsoft Authenticator and Scan a QR-code.  <ul style="list-style-type: none"> • Scan the QR code in ERDA: aim the camera on your device at the code. The app will scan the code automatically. • Click Done importing in ERDA. <p>Your app can now generate 6-digit single use codes, that change every 30 seconds. Find them at the front page of Microsoft Authenticator.</p> 
<p>STEP 3: VERIFY THAT IT WORKS</p>	<p>Test that the 2-factor authentication is correctly set up. Click verify in ERDA.</p> <p>3. Verify the Authenticator App Setup</p> <p>Please verify that your authenticator app displays correct notifications when locking yourself out once you enable 2-factor authentication!</p> <ul style="list-style-type: none"> • ERDA will open a pop-up window, where you must enter the code from the app.

	<ul style="list-style-type: none"> • Enter the code and once again click Verify.  <p>Contact your local IT-support for help, if the authentication fails.</p>
<p>STEP 4: DEFINE AUTHENTI- CATION BREADTH</p>	<p>You must now define the breadth of 2-factor authentication for your ERDA account.</p> <ul style="list-style-type: none"> • Click the button under Enable 2-FA for AU web login <p>You can now add 2-factor authentication for mounted access, that is WebDAVS, and SFTP. If in doubt whether you will use ERDA as a network drive, we recommend activating authentication for all access.</p> <ul style="list-style-type: none"> • Click Save 2-Factor Auth Settings to finish.
<p>HELP</p>	<p>You can find more guidance on the ERDA front page in the bottom right corner, under Support and About.</p> <p>For help with 2-factor authentication, contact your local IT-support.</p>

<h2>SIGN UP AS EXTERNAL PARTNER</h2>	
<p>REGISTER</p>	<ul style="list-style-type: none"> • Go to ERDA's front page. • Click the External users tab • Click Sign up for ERDA <i>without</i> an AU account?  <ul style="list-style-type: none"> • Complete the form with your information. • Note that email address must be your work-email. • Note that your password must consist of at least 10 characters and contain upper and lower case letters, number, and special characters.

	<ul style="list-style-type: none"> • Under Comment, enter name and email of your AU-partner and the name of your project. • Click Send. <p>ERDA account request - with OpenID login</p> <p>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.</p> <p>IMPORTANT: we need to identify and notify you about login info, so please use a working Email address clearly affiliated with your Organization!</p> <div data-bbox="438 539 1334 1043"> <p>Full name <input type="text" value="Full name"/> Email address <input type="text" value="username@organization.org"/> Organization <input type="text" value="Organization or company"/></p> <p>Country <input type="text" value=""/> Optional state code <input type="text" value="NA"/></p> <p>Password <input type="text" value="Your password"/> Verify password <input type="text" value="Repeat password"/></p> <p>Comment with reason why you should be granted a ERDA account: <input type="text" value="Typically which collaboration, project or course you need the account for AND the name and email of your affiliated contact"/></p> <p>I accept the ERDA terms and conditions <input checked="" type="checkbox"/></p> <p>Send</p> </div> <p>You will receive an email with further instructions when your request has been processed.</p> <p>If your request is denied, contact your AU-partner.</p>
<p>LOGIN</p>	<ul style="list-style-type: none"> • Click on the link in the email from ERDA to access login. • Enter your email and your ERDA password. • Click Yes.
<p>2-FACTOR AUTHENTICATION</p>	<p>Due to the increasing risk of cyber-attack, we recommend securing your ERDA account with 2-factor authentication. 2-factor authentication adds a step to login, demanding username, password, and a single-use numerical code.</p> <ul style="list-style-type: none"> • Click the person icon at the bottom left corner of ERDA. • Click Setup and the 2-Factor auth banner. • Click Okay, let's go. <div data-bbox="416 1644 1326 1883"> <p>Setup</p> <p>SFTP WebDAVS FTPS Duplicati 2-Factor Auth</p> <p>2-Factor Authentication</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>Okay, let's go!</p> </div>
<p>STEP 1: DOWNLOAD APP</p>	<p>Open Microsoft Authenticator, the AU-approved app for 2-factor authentication. Find the app in your appstore, if it's not installed on your device.</p>

Click **I've got it installed** in ERDA.

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.

I've got it installed!

STEP 2: IMPORT PERSONAL CODE

To import a code in ERDA, either scan a QR-code or enter the key manually. If your device has a camera, scanning is by far the easiest way.

Click **Scan your personal QR code** in ERDA.

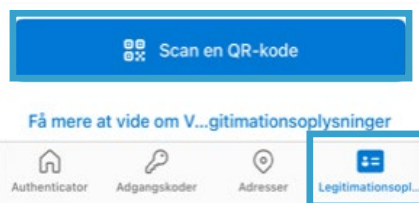
2. Import Secret in Authenticator App

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**

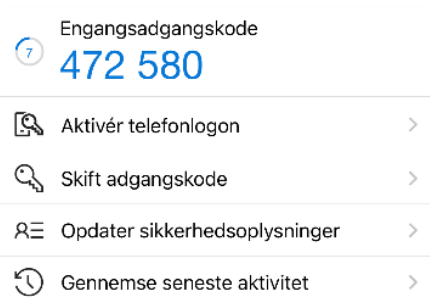
ERDA will now open a window with a QR-code.

- Click **Legitimation Information** at the bottom right of Microsoft Authenticator and **Scan a QR-code**.



- Scan the QR code in ERDA: aim the camera on your device at the code. The app will scan the code automatically.
- Click **Done importing** in ERDA.

Your app can now generate 6-digit single use codes, that change every 30 seconds. Find them at the front page of Microsoft Authenticator.



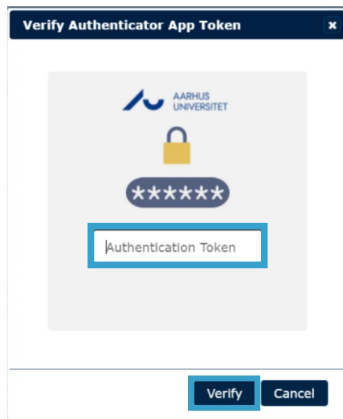
STEP 3: VERIFY THAT IT WORKS

Test that the 2-factor authentication is correctly set up. Click **verify** in ERDA.

3. Verify the Authenticator App Setup

Please **verify** that your authenticator app displays correct numbers. This will lock you out of the system. Please be careful not to lock yourself out once you enable 2-factor authentication!

- ERDA will open a pop-up window, where you must enter the code from the app.
- Enter the code and once again click **Verify**.



Contact your local IT-support for help, if the authentication fails.

STEP 4. DEFINE AUTHENTI- CATION BREADTH

You must now define the breadth of 2-factor authentication for your ERDA account.

- Click the button under **Enable 2-FA for AU web login**

You can now add 2-factor authentication for mounted access, that is WebDAVS and SFTP. If in doubt whether you will use ERDA as a network drive, we recommend activating authentication for all access.

- Click **Save 2-Factor Auth Settings** to finish.

HELP

You can find more guidance on the [ERDA front page](#) in the bottom right corner, under **Support** and **About**.

For help with 2-factor authentication, contact your local IT-support.