

TILMELD DIG SOM BRUGER AF ERDA

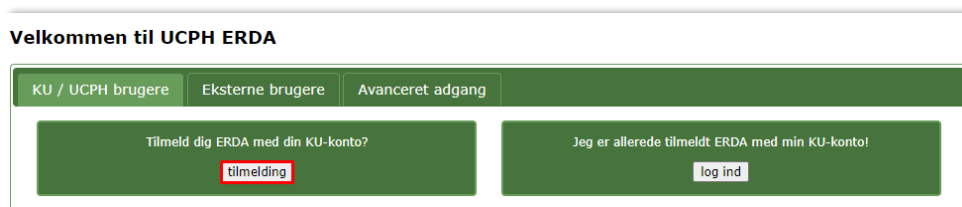
Som KU-ansat/studerende (se side 1-5) eller ekstern samarbejdspartner (se side 6-11) skal du tilmelde dig som bruger, før du kan tilgå ERDA. Du har derudover mulighed for yderligere at sikre din konto ved log ind med 2-faktor-godkendelse.

TILMELDING MED EN KU-KONTO

TILMELDING

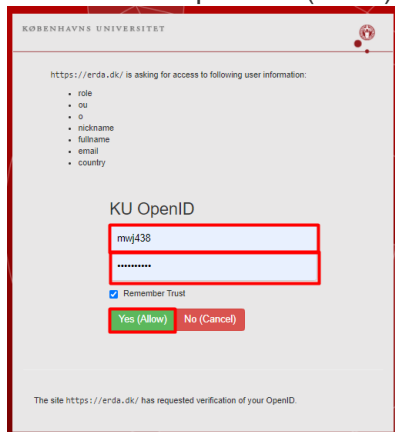
Gå på <https://erda.ku.dk/>

Klik på "tilmelding"



I pop-op-vinduet under "KU OpenID" skriver du:

1. Dit KU-brugernavn (Består af tre bogstaver og tre tal).
2. Dit personlige KU-kodeord, som du også bruger til f.eks. KUnet.
3. Klik derefter på "Yes (Allow)"



Nu er du oprettet som bruger på ERDA.

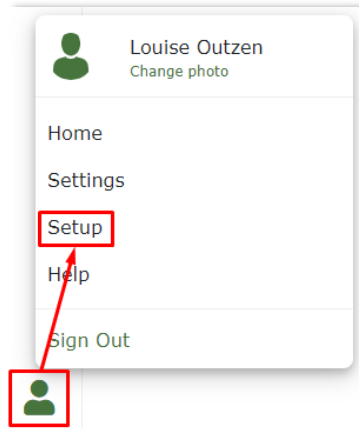
2-FAKTOR GOD- KENDELSE

For at øge sikkerheden, anbefaler vi, at benytte 2-faktor-godkendelse til al ERDA-adgang.

Med 2-faktor-godkendelse tilføjer du et ekstra kontroltrin til den login-proces, som autentificerer dig. Udover at anmode om noget man kender (i dette tilfælde dit brugernavn og kodeord), så vil en 2-faktor-beskyttet konto også anmode om information fra noget, man har (tal-nøgle fra app på mobil/tablet).

Ved oprettelse af 2-faktor-godkendelse skal du *én* gang igennem en guide.

Klik på det grønne personikon i nederste venstre hjørne. Klik på "Setup"



Nu kommer der en guide frem i ERDA, du skal følge nøje. Klik på "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!

TRIN 1. DOWNLOAD APP

På din mobil eller tablet* skal du downloade en af følgende apps: *Google Authenticator*, *FreeOTP*, *NetIQ Advanced Authentication* eller *Authy*. Find appen dér, hvor du normalt downloader apps.

Klik derefter på "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.

I've got it installed!

*Hvis du kun har en privat mobil/tablet og ikke ønsker at bruge den, har du mulighed for at få udleveret et lille apparat, som du kan bruge i stedet for. Kontakt support@erda.dk for yderligere information.

TRIN 2. IMPORTÉR PERSONLIG 2-FAKTOR- KODE

Importér din personlige 2-faktor-kode med "Scan your personal QR code" eller "Enter your personal key". Nedenfor følger eksempel med "Scan your personal QR code".

Klik på "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**

En QR-kode popper op i ERDA



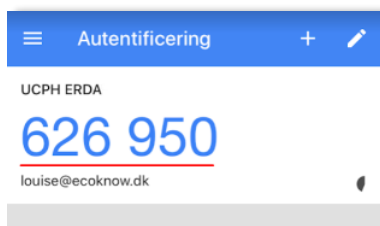
Åbn din downloadede app.
Appsene er lidt forskellige. I nedenstående er det skærmbillede fra appen *Google Authenticator*, der vises. Klik på "Scan strekkoden"



Scan nu QR-koden som du netop åbnede i guiden på ERDA. Dvs. ret mobilens kamera op på QR-koden (Appen skal muligvis have tilladelse til at bruge dit kamera). Nu scanner appen QR-koden. Klik derefter på "Done importing"



Din app kan nu generere 6-cifrede engangsnøgler (såkaldte tokens). I nedenstående eksempel er engangsnøglen "626 950".



TRIN 3. VERIFICÉR, AT DET VIRKER

Du skal nu teste, at din 2-faktor-godkendelse er sat korrekt op, og at appen leverer de rigtige engangsnøgler.

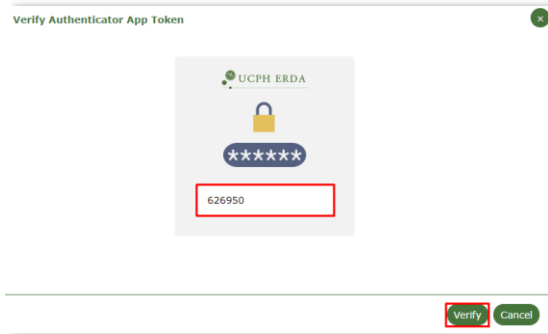
3. Verify the Authenticator App Setup

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!

Der kommer automatisk et pop-op-vindue frem, hvor du skal du skrive den engangsnøgle, appen viser (hvis det ikke kommer frem, skal du klikke på 'verify' i ovenstående). Vær opmærksom på, at engangs tal-nøglen skifter efter 30 sekunder.

Skriv den 6-cifrede engangsnøgle og klik på knappen "Verify" i pop-op-vinduet



Hvis din 2-faktor-godkendelse lykkes, føres du direkte til næste trin.

TRIN 4. AKTIVÉR 2- FAKTOR GODKEN- DELSEN

Klik på skydeknop under "Enable 2-FA for KU/UCPH OpenID web login", så den skifter fra grå til grøn

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.



Der fremkommer nu muligheder for yderligere at tilføje 2-faktor-godkendelse ved brug af WebDAVS, SFTP og FTPS. Det er protokoller, som hovedsageligt er aktuelle, hvis man vil bruge ERDA som netværksdrev på egen computer.

Er du i tvivl om, hvorvidt du skal bruge ERDA som netværksdrev, anbefaler vi, at du aktiverer alle tre skydeknapper, så de bliver grønne.

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.



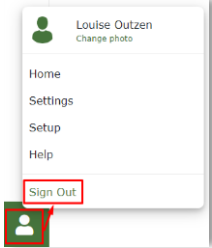
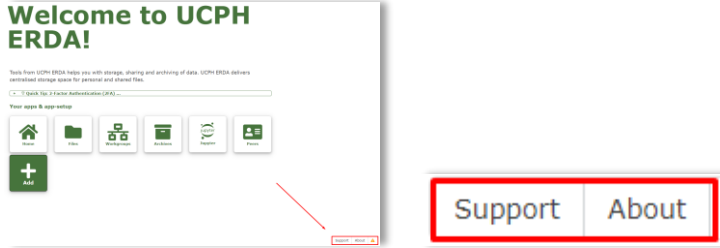

Enable 2-FA for FTPS network drive or client login

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.



Klik på "Save 2-Factor Auth Settings"

Save 2-Factor Auth Settings

	<p>Derved er din ERDA-konto sikret med 2-faktor-godkendelse.</p> <p>Nu kan du fremover gå på https://erda.ku.dk/, logge på med dit KU-brugernavn og personlige KU-kodeord efterfulgt af 2-faktor-godkendelse med en 6-cifret engangsnøgle.</p>
<p>LOG UD</p>	<p>Når du er færdig med at arbejde i ERDA, så klik altid på "Sign Out" i nederste venstre hjørne. Så er du sikker på, at ingen andre uretmæssigt får adgang til dine data</p> 
<p>LÆS MERE</p>	<p>I nederste højre hjørne på knapperne "Support" og "About" kan du finde vejledninger, få svar på ofte stillede spørgsmål og læse mere om ERDA m.m.</p>  <p>Du kan også se aktuelle eller varslede driftsforstyrrelser. Grønt flueben betyder, at systemet kører efter planen, mens f.eks. orange trekantvarsel betyder, der er aktuelle driftsforstyrrelser. Klik eventuelt på statusikonet og læs mere.</p> 
<p>HJÆLP</p>	<p>Få personlig hjælp på support@erda.dk</p>

TILMELDING FOR EKSTERN SAMARBEJDSPARTNER

TILMELDING

Gå på <https://erda.ku.dk/>

Klik på fanebladet "Eksterne brugere" og klik dernæst på "tilmelding"

Velkommen til UCPH ERDA

KU / UCPH brugere Eksterne brugere Avanceret adgang

Tilmeld dig ERDA uden en KU-konto? **tilmelding**

Jeg er allerede tilmeldt ERDA uden en KU-konto! **log ind**

Du skal nu udfylde formularen med dine oplysninger:

- Full name: *Skriv dit fulde navn*
- Email address: *Din arbejds e-mail (Ingen trejdepartes e-mail tjenester såsom hotmail, gmail eller yahoo)*
- Organization: *Navnet på din arbejdsplads/virksomhed*
- Country: *Vælg dit land i rullemenuen*
- Password: *Find på et tilpas svært kodeord til din ERDA-adgang. Det skal bestå af minimum 8 tegn og indeholde en kombination af små og store bogstaver samt tal og specialtegn (mindst tre af de nævnte fire slags). I "Verify password" gentager du kodeordet.*
- Optional comment ...: *Henvis til din kontakt, som er ansat på Københavns Universitet (navn + e-mail) og eventuelt til hvilket projekt, kursus eller samarbejde.*
- I accept ...: *Læs "terms and conditions" og sæt flueben i feltet*

Klik på "Send"

UCPH 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 UCPH 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!

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 ERDA account:
For my collaboration with Jonas Bardino (bardino@science.ku.dk) on the project EcoKnow

I accept the UCPH ERDA terms and conditions

Send

Dit ønske om at tilmelde dig som bruger af ERDA bliver nu sendt til ERDA-administratorerne som indhenter samtykke fra den KU-ansatte omkring samarbejdet.

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

Når ERDA-administratorerne har accepteret din anmodning, får du tilsendt en e-mail.

LOG IND

Klik på linket til ERDA i den tilsendt e-mail og log ind på ERDA.

Skriv din e-mail og dit ERDA-kodeord. Klik på "yes"

UCPH ERDA OpenID Login

Username (email):	<input type="text" value="louise@ecoknow.dk"/>
Password:	<input type="password" value="....."/>
Remember Trust:	<input checked="" type="checkbox"/>
Proceed:	<input checked="" type="radio"/> yes <input type="radio"/> no

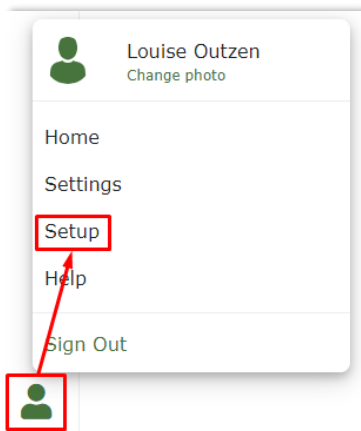
2-FAKTOR GOD- KENDELSE

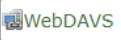

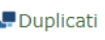




For at øge sikkerheden, anbefaler vi, at benytte 2-faktor-godkendelse til al ERDA-adgang.

Med 2-faktor-godkendelse tilføjer du et ekstra kontroltrin til den login-proces, som autentificerer dig. Udover at anmode om noget man kender (i dette tilfælde dit brugernavn og kodeord), så vil en 2-faktor-beskyttet konto også anmode om information fra noget, man har (tal-nøgle fra app på mobil/tablet).

Ved oprettelse af 2-faktor-godkendelse skal du *én* gang igennem en guide.

Klik på det grønne personikon i nederste venstre hjørne. Klik på "Setup"



	<p>Nu kommer der en guide frem i ERDA, du skal følge nøje. Klik på "Okay, let's go!"</p> <div data-bbox="435 300 1362 685" style="border: 1px solid #ccc; padding: 10px;"> <p>Setup</p> <p>       </p> <p style="text-align: center;">2-Factor Authentication</p> <p>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.</p> <p>Preparing and enabling 2-factor authentication for your login is done in four steps.</p> <p style="text-align: center;">Okay, let's go!</p> </div>
<p>TRIN 1. DOWNLOAD APP</p>	<p>På din mobil eller tablet skal du downloade en af følgende apps: <i>Google Authenticator</i>, <i>FreeOTP</i>, <i>NetIQ Advanced Authentication</i> eller <i>Authy</i>. Find appen dér, hvor du normalt downloader apps.</p> <p>Klik derefter på "I've got it installed!"</p> <div data-bbox="435 898 1401 1093" style="border: 1px solid #ccc; padding: 10px;"> <p>1. Install an Authenticator App</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 style="text-align: center;">I've got it installed!</p> </div>
<p>TRIN 2. IMPORTÉR PERSONLIG 2-FAKTOR- KODE</p>	<p>Importér din personlige 2-faktor-kode med "Scan your personal QR code" eller "Enter your personal key". Nedenfor følger eksempel med "Scan your personal QR code".</p> <p>Klik på "QR code"</p> <div data-bbox="435 1308 1401 1473" style="border: 1px solid #ccc; padding: 10px;"> <p>2. Import Secret in Authenticator App</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"> • Scan your personal QR code • Type your personal key code </div> <p>En QR-kode popper op i ERDA</p>  <p>Åbn din downloadede app. Appsene er lidt forskellige. I nedenstående er det skærmbillede fra appen</p>

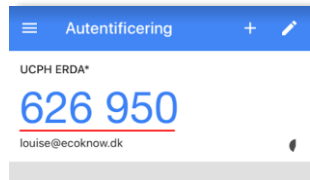
Google Authenticator, der vises. Klik på "Scan strekkoden"



Scan nu QR-koden som du netop åbnede i guiden på ERDA. Dvs. ret mobilens kamera op på QR-koden (Appen skal muligvis have tilladelse til at bruge dit kamera). Nu scanner appen QR-koden. Klik derefter på "Done importing"



Din app kan nu generere 6-cifrede engangsnøgler (såkaldte tokens). I nedenstående eksempel er engangsnøglen "626 950".



TRIN 3. VERIFICÉR, AT DET VIRKER

Du skal nu teste, at din 2-faktor-godkendelse er sat korrekt op, og at appen leverer de rigtige engangsnøgler.

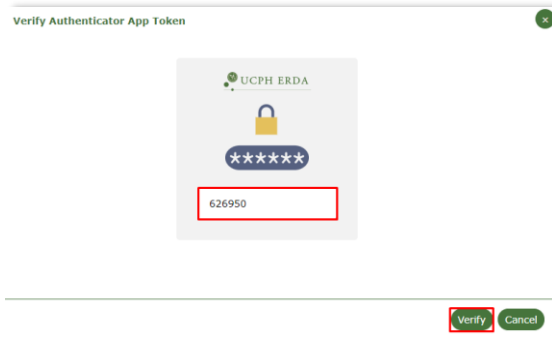
3. Verify the Authenticator App Setup

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!

Der kommer automatisk et pop-op-vindue frem, hvor du skal du skrive den engangsnøgle, appen viser (hvis det ikke kommer frem, skal du klikke på 'verify' i ovenstående). Vær opmærksom på, at engangs tal-nøglen skifter efter 30 sekunder.

Skriv den 6-cifrede engangsnøgle og klik på knappen "Verify" i pop-op-vinduet



Hvis din 2-faktor-godkendelse lykkes, føres du direkte til næste trin.

TRIN 4. AKTIVÉR 2- FAKTOR GODKEN- DELSEN

Klik på skydeknop under "Enable 2-FA for Non-KU/UCPH OpenID web login", så den skifter fra grå til grøn

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.



Der fremkommer nu muligheder for yderligere at tilføje 2-faktor-godkendelse ved brug af WebDAVS, SFTP og FTPS. Det er protokoller, som hovedsageligt er aktuelle, hvis man vil bruge ERDA som netværksdrev på egen computer.

Er du i tvivl om, hvorvidt du skal bruge ERDA som netværksdrev, anbefaler vi, at du aktiverer alle tre skydeknapper, så de bliver grønne.

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.



Klik på "Save 2-Factor Auth Settings"

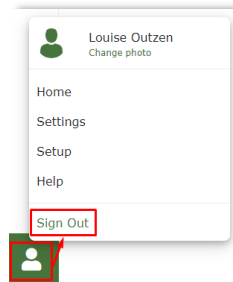
Save 2-Factor Auth Settings

Derved er din ERDA-konto sikret med 2-faktor-godkendelse.

Nu kan du fremover gå på <https://erda.ku.dk/>, vælge fanebladet 'Eksterne brugere' og logge på med din e-mail og password efterfulgt af 2-faktor-godkendelse med en 6-cifret engangsnøgle.

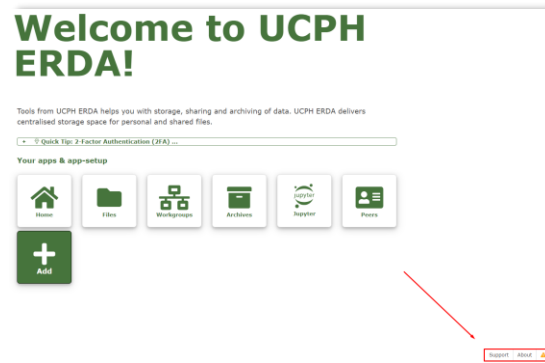
LOG UD

Når du er færdig med at arbejde i ERDA, så klik altid på "Sign Out" i nederste venstre hjørne. Så er du sikker på, at ingen andre uretmæssigt får adgang til dine data.



LÆS MERE

I nederste højre hjørne på knapperne "Support" og "About" kan du finde vejledninger, få svar på ofte stillede spørgsmål og læse mere om ERDA m.m.



Du kan også se aktuelle eller varslede driftsforstyrrelser. Grønt flueben betyder, at systemet kører efter planen, mens f.eks. orange trekantvarsel betyder, der er aktuelle driftsforstyrrelser. Klik eventuelt på statusikonet og læs mere.



HJÆLP

Få personlig hjælp på support@erda.dk