ERDA

User guide

Version 7

Aarhus University, October 2024

Contents

ERDA Intro

ERDA (Electronic Research Data Archive) is AU's digital solution for storing and sharing open research data. ERDA offers the following advantages over other storage solutions:

- ERDA is a free service tailored to research data
- ERDA is hosted on-premise
- ERDA uses strong user validation
- ERDA mounting is supported by a dedicated tool from AU IT

ERDA is an essential infrastructure in relation to two main strategic focus areas at AU:

In relation to The Danish Code of Conduct for Research Integrity, ERDA fulfils the demand placed on institutions to provide secure data storage facilities consistent with confidentiality requirements and applicable regulations and guidelines.

In relation to AU's Digitaliseringsstrategi (available only in Danish), ERDA fulfils the ambition to establish, develop, and maintain digital facilities and competencies to thereby retain and strengthen the university's position as an internationally leading research university and sustain a strong commitment to societal development.

ERDA Research data

ERDA must only be used for research data that can be open. In other words, you **MUST NOT** store your research data in ERDA if:

- They contain personal data
- When you know for certain that your research results will be patented (IP-data)
- They contain confidential information or IP-covered material from a third party
- They are of strategic importance, e.g. because sharing can pose a threat (URIS-data)
- They form part of research subject to export control
- They must, for any other reason, be protected from unauthorised access

If one or more of these points apply to your research, we recommend that you store your data in SIF instead of ERDA. SIF is currently undergoing silent roll-out at AU. Contact your local coordinator for more information.

ERDA has an anchor point at each faculty, that offers guidance on using ERDA in the different fields, data management support, and help related to local guidelines for best practice.

ARTS: All queries please contact CHC Services and Support via ticket at https://chc.au.dk/

BSS: bss.it@au.dk

HEALTH: askOS.health@au.dk

NAT: dm.support@nat.au.dk

TECH: askOS.tech@au.dk

ERDA replication

ERDA uses replication by default, which protects against system errors and ensures continuous access to files. ERDA replication basically functions like this:

- Snapshots are taken on ERDA's primary site every 15. mins. These are saved for 8 days.
- ERDA is copied to a secondary site (>14km distant from the primary site) every 24 hours.
- Snapshots are taken on the secondary site once a day. These are saved for 30 days.

ERDA files can therefore be recreated if more than 15 mins. AND less than 30 days have lapsed since the error was discovered.

NB the system administration will **not** be able to recreate single files based on replication.
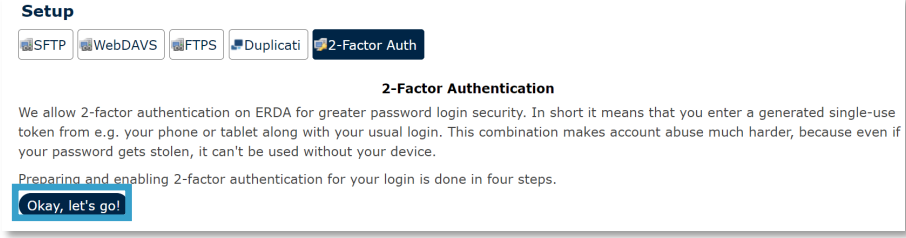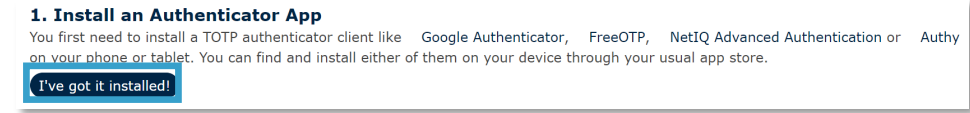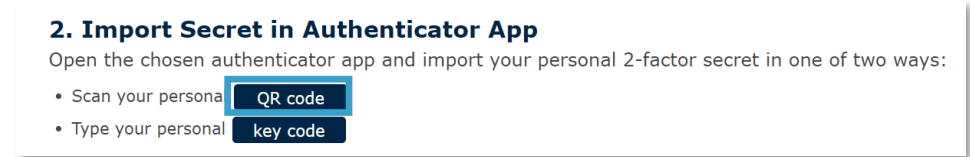
Access to AU ERDA

Since ERDA uses the central user database for user validation, all AU-employees can create an ERDA-account. AU users sign up to ERDA with the username and password used to log on to computer, email and internal websites.

Here, we walk through ERDA sign up as an AU-user and an external user.

| 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 AUTHENTI-CATION	Due to the risk of cyber-attack, we recommend securing your ERDA account with 2-factor authentication. 2-factor authentication adds a single-use code to login.

- Click the person icon at the bottom left corner of ERDA.
- Open ERDA and click **Setup** and on 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.

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

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.

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

- Click **Legitimisation Information** at the bottom right of Microsoft Authenticator og **Scan a QR-kode**.
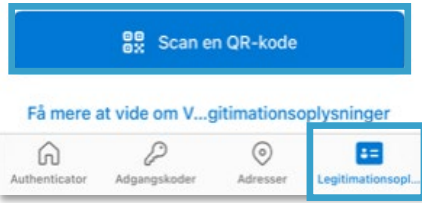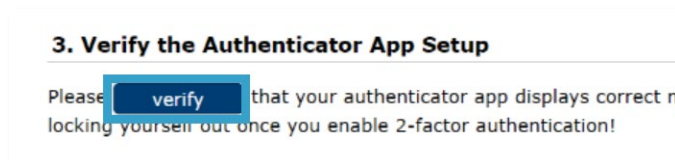
- Scan the QR code in ERDA: aim the camera on your device at the code. The app will scan the code automatically.
- Click **Done importing** in ERDA.

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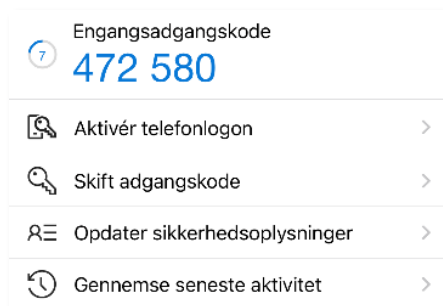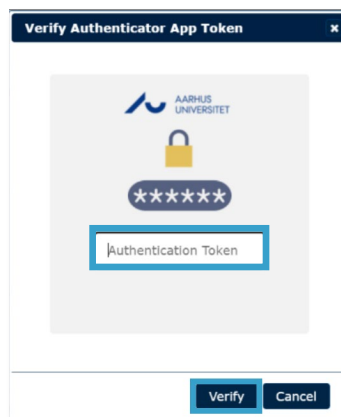

STEP 3: TEST THAT IT WORKS	Test that the 2-factor authentication is correctly set up. Click **verify** to open a pop-up window in ERDA.
	- Enter the code in the pop-up window and once again click **Verify**.
	Contact your local IT-support for help, if the authentication fails.

STEP 4: DEFINE AUTHENTI-CATION BREADTH	You must now define the breadth of 2-factor authentication. • Click the button under **Enable 2-FA for AU web login** You can now add 2-factor authentication for mounted access. If in doubt whether you will mount ERDA, we recommend activating authentication for all access. • Click **Save 2-Factor Auth Settings** to finish.
HELP	Find more guidance on the ERDA front page under **Support** and **About**. For help with 2-factor authentication, contact your local IT-support.

SIGN UP AS EXTERNAL PARTNER

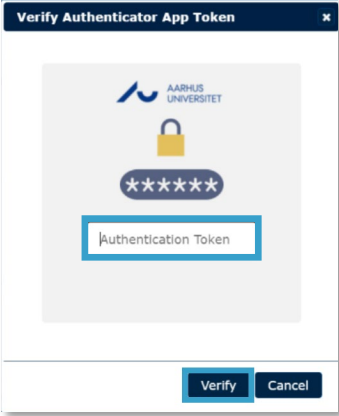|	
REGISTER	• Go to ERDA's front page. • Click the **External users** tab • Click **Sign up for ERDA** *without* an AU account? • Complete the form with your information. • Note that email address must be your work-email. • Note that your password must consist of at least 10 characters and contain upper and lower case letters, number, and special characters. • Under **Comment**, enter name and email of your AU-partner and the name of your project. • 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!**

Full name	Email address	Organization
Full name	username@organization.org	Organization or company

Country	Optional state code
	NA

Password	Verify password
Your password	Repeat password

Comment with reason why you should be granted a ERDA account:

Typically which collaboration, project or course you need the account for AND the name and email of your affiliated contact

I accept the ERDA terms and conditions 🔵

Send

You will receive an email with instructions when your request is processed.

If your request is denied, contact your AU-partner.

LOGIN	• Click on the link in the email from ERDA to access login. • Enter your email and your ERDA password. • Click **Yes**.
2-FACTOR AUTHENTI-CATION	Due to the threat of cyber-attack, we recommend securing your ERDA account with 2-factor authentication. 2-factor authentication adds a single-use numerical code to login. • In **ERDA Setup**, click the **2-Factor auth** banner. • Click **Okay, let's go**.
STEP 1: DOWNLOAD	Open **Microsoft Authenticator**, the AU-approved app for 2-factor authentication. Find the app in your app store, if it's not installed on your device.

APP	Click **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!
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 **Legitimisation Information** at the bottom right of Microsoft Authenticator og **Scan a QR-kode**. ⊞ Scan en QR-kode Få mere at vide om V...gitimationsoplysninger ⌂ Authenticator 🔑 Adgangskoder ◉ Adresser ▤ Legitimationsopl... • 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. ⑦ Engangsadgangskode **472 580** 🔍 Aktivér telefonlogon > 🔍 Skift adgangskode > 𐂎 Opdater sikkerhedsoplysninger > 🕙 Gennemse seneste aktivitet >
STEP 3: VERIFY THAT	Test that the 2-factor authentication is correctly set up. Click **verify** in ERDA.

IT WORKS	**3. Verify the Authenticator App Setup** Please [verify] that your authenticator app displays correct n~~~~ locking yourself out once you enable 2-factor authentication! - This opens a pop-up window in ERDA. - Enter the code from the app 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 the 2-factor authentication. - Select all six possibilities for maximum protection. - Click **Save 2-Factor Auth Settings**.
HELP	Find more guidance on the ERDA front page under **Support** and **About**. For help with 2-factor authentication, contact your local IT-support.

ERDA Overview

When you log on to ERDA, you will be taken to Home with your default apps: **Home**, **Files**, **Workgroups**, **Archives**, and the **Settings** and **Setup** menus.

Home

From **Home**, you can open your apps and select the ones you want on the front page. Click on an app to open it, and on **Add** to add or remove the apps you can see.

Files

Files is the main entrance to your research data in ERDA. Right click on a folder or file to see the most common actions.

- **Create File** opens an editor, where you can write a new file.
- **Upload File** opens an upload window. To add several files at once, use Add files…
- Click **Start upload**.

Edit files directly with **Edit** in the right-click menu.

Double-click a file to open it in the browser. If the browser cannot open it, it will be downloaded. Changes made to a downloaded file are **not** saved to ERDA. Remember to upload the file back to ERDA.

Workgroups

Use **Workgroups** to share files and collaborate in ERDA.

- Click **Request membership** ⊕ to request access to a group. The red version of the icon deletes your membership of the group.
- Click **Request ownership** ⚙ to request co-ownership of a group. The red version of the icon deletes your ownership of the group.
- Click **Edit** 🔧 to edit a group you own.
- Click **Create workgroup** at the bottom of the page to add a new group.

You can add websites to your workgroup to display it to the group members or the entire internet. See ERDA Data sharing.

Archives

Archives lets you create a frozen archive, i.e. a still image, of your research data in ERDA.

- **Add file/directory** to add files from ERDA to the archive.
- **Add upload** to add files from your PC to the archive.
- Double-click to pick a single file. Right-click and click **Select** to pick the entire folder.
- Indicate whether to make your frozen archive publicly available.
- Click **Save and Preview**.

Create Freeze Archive

Saved *preliminary* freeze archive with ID archive-C1LRj3 . You can continue inspecting and changing it until you're satisfied, then finalize it for actual persistent freezing.

⊞ View details

✎ Edit archive

⚠ IMPORTANT: you still have to explicitly finalize your archive before you get the additional data integrity/persistance guarantees like tape archiving.

✎ Finalize archive

- **Preview publishing** opens a preliminary view of the archive.
- **Edit archive** makes it possible to add files and edit the archive.
- **Finalize archive** permanently freezes the archive.

Archiving will **not** remove the files, just save a copy. You can continue to work on the files without changing the archived version.

- **View details** displays all the archive's details and links to associated files.

Settings and Setup

Use **Settings** to adjust ERDA's settings, i.e. change the look of the pages. You do not need to change the standard settings to use ERDA's basic functions.

Use **Setup** to change ERDA's advanced settings and i.e. set up backup to ERDA and configure effective access. Read more here: ERDA Setup.

Sara Marie Westh
Change photo

Home

Settings

Setup

Help

Sign Out
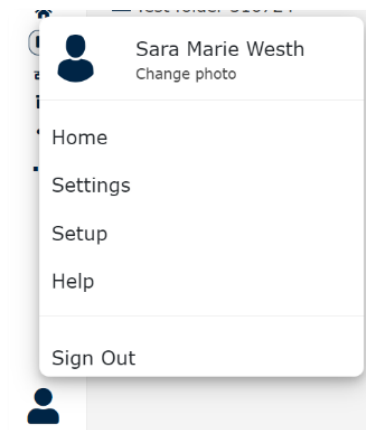
ERDA data sharing

ERDA supports workflows around research data sharing in several different ways.

- To share research data once or exchange data with peers without an ERDA-account, we recommend **Share Link**.
- To share research data permanently and transparently, we recommend **Workgroup Shared Folders**.
- To share research data broadly, add websites to the workgroup with **Workgroups websites**.

Share Links

- Right click on a folder or file in **Files**, choose **Share Link** and **Create**.
- Pick which combination of **Read-Only** and **Write-Only Access** to use. **Please note that when sharing single files, Read-Only Access is the sole possibility**.
- Click **OK**.

- Click **Edit and send share link** to send the invite via ERDA.

- Enter recipients' emails under **Recipients** and consider writing them a message.

- Click **Send invitation(s)**.

For information on more advanced use of **Share Links**, see [Effective access](#).

Workgroup Shared Folders

ERDA integrates project shares closely, making it easy to share files directly in **Files**.

All ERDA workgroups have a shared folder to which all members have access. The folder is marked with a small, blue folder-icon with a white link . The contents of this folder are automatically shared with the group-members.

For this reason, carefully assess the file structure of your workgroup, to ensure that its members only have access to research data with which they are allowed to work.

Workgroup websites

Workgroups have a simple, built-in infrastructure that supports basic websites added to the project. Via these websites, the project can be presented either to its members or to the entire internet.

When you create, or become co-owner of, a workgroup, you are given access to two new folders in the group. Both folders create websites containing the files placed in them.

- private_base - will create a website that can only be accessed by group members.
- public_base - will create a website accessible to the entire internet.

Use the folders to manage the contents of the website or open the online editor via **Edit-links** on the project page. Use **View-links** to inspect the websites.

Effective access

> To make working with advanced data access easier, we have made a tool that sets up the connection for you. Download the guide here: [link](#).

By setting up mounted access to ERDA, you can achieve more effective, transparent, and integrated access to your files than via the web interface. Mounted access makes it possible to transfer many and large files effectively and tie your ERDA files and folders to your machine.

Mounting uses a safe connection to ERDA, so the access is available so long as you are connected to the internet. It is not necessary to use VPN for mounted access outside AU.

[ERDA](#) guides you through mounting setup too. For more information, see **ERDA Setup**.

Mounted access via SFTP

SFTP is a secure and effective protocol for file-transfers. SFTP is built upon the security-infrastructure of the OpenSSH software and it is supported by a wide range of clients on the most popular platforms, i.e. Windows, Linux, and IOS.

SFTP setup in ERDA

- Open the **SFTP banner** in **ERDA Setup**.
- Configure how you want to identify yourself to the ERDA server: either copy and paste one or several SSH public keys or type in a password of your own choosing.
- Click **Save SFTP Settings**.

Please note that your login information – including your username – will be shown on the SFTP site.

SFTP with Windows

- Download og install WinFsp og SSHFS-Win.
- Open **Files** and click **Add Network Drive**.
- Enter \\sshfs\[username]@[project name]@io.erda.au.dk!2222 under **Folder**. You can copy both username and project name from the top of the ERDA setup page.
- Click **Finish**.
- Enter username and your chosen password when the system prompts you to log in.
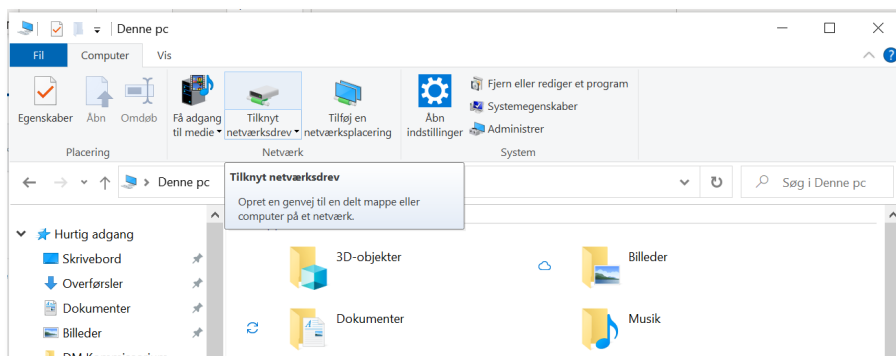
SFTP with MacOS

- Download and install the [macFUSE og SSHFS Stable Release](#) packages.
- Save your login details to your local ~/.ssh/config, to avoid having to enter them again:
    - Host io.erda.au.dk erda
    - Hostname io.erda.au.dk
    - VerifyHostKeyDNS ask
    - User [username]@[project name]
    - Port 2222
    - # Uncomment next line to use your private key in ~/.ssh/id_rsa
    - # IdentityFile ~/.ssh/id_rsa

You can now mount ERDA with the SSHFS-command.

SFTP with Linux

If you use Linux and SFTP is integrated into your file management system:

- Go to the **file manager** and click **ctrl+L**.
- Copy paste sftp://io.erda.au.dk:2222 into the field.
- Enter your username and chosen password when prompted by the system.

If you use Linux and SFTP is **not** integrated into your file management system.

- Download and install [SSHFS](#), including FUSE and OpenSSH via your preferred software/pack manager or downloads online.
- Save your login-details to your local ~/.ssh/config, to avoid entering them again:
    - Host io.erda.au.dk erda
    - Hostname io.erda.au.dk
    - VerifyHostKeyDNS ask
    - User [username]@[project name]
    - Port 2222
    - # Uncomment next line to use your private key in ~/.ssh/id_rsa
    - # IdentityFile ~/.ssh/id_rsa

You can now mount ERDA with the SSHFS-command.

Alternative clients

Aside from the above-mentioned clients, ERDA supports the following for mounted access:

- **WinSCP**. WinSCP is an FTP/FTPS/SFTP client for Windows. Its semi-automatic sync-function makes it easier to synchronise files between your machine and ERDA. See the [project webpage](#).

- **PuTTY SFTP** is an SSH client with a command-line SFTP client. For security reasons, you can only connect to our SFTP-service with version 0.67 or newer. See the project webpage.
- **SSHFS**. For brief instructions, see **ERDA Setup** under **SFTP**. Click **Show more SFTP client details…** at the bottom of the page. On the ERDA guidance portal, our coordinator for NAT, Jesper Lykkegaard Karlsen, walks through set up in Windows og MacOS respectively.

Mounted access via WebDAVS

WebDAV is a protocol for accessing external storage, that can be secured with TLS/SSL like a website. We refer to the secured version as WebDAVS. Newer versions of Microsoft Windows, MacOS, and Linux integrate WebDAVS directly.

> Unfortunately, Microsoft has introduced a c. 50MB limit for WebDAVS transfers. This means that you will get an error message if you attempt to transfer larger files.
>
> Because of this limit, we recommend using SFT instead of WebDAVS, if you need to work with larger datasets.

WebDAVS setup in ERDA

- Go to ERDA Setup and open **WebDAVS**.
- Pick a password for login.
- Click **Save WebDAVS Settings**.

NB: your login details – including your automatic username – will be displayed in the same place.

WebDAVS with Windows

- Open **Files** and click **Computer**.
- Click **Map network drive** or **Add a network location** at the top of the window. Note that Windows 7 only shows the second possibility if you click **Connect to a Web site…** Windows 8 and newer versions have a dedicated button.
- Pick a letter for your networkdrive (e.g. Z:)
- Copy-paste server URL from ERDA's WebDAVS page to **Folder**.
- Click **Finish**.

Windows Security will prompt you to logon to the external folder. Log on with your username and chosen password from ERDA's WebDAVS page and click **OK**.
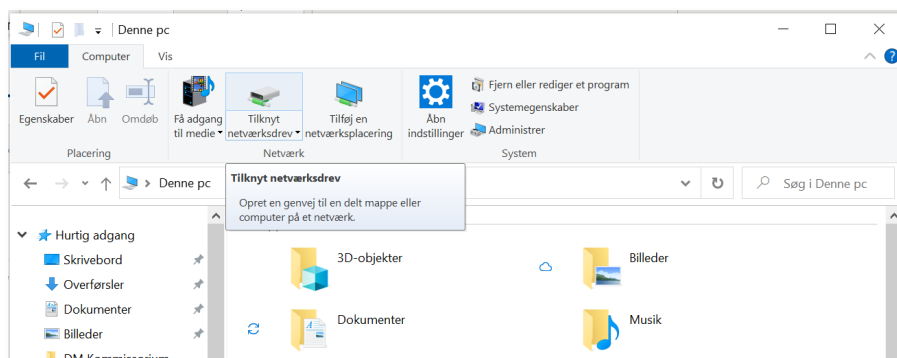
WebDAVS with MacOS

- Open **Finder**, click **Go** and choose **Connect to Server**.
- From the ERDA Setup page, copy-paste the Server URL into the pop-up window.
- Click **Connect**.
- Log in with your username and password.

If login is successful, you will find your ERDA folder under Files.

WebDAVS with Linux

- Open **Finder**, click **Go** and choose **Connect to Server**.
- Open **Files** (Nautilus, Konqueror, Dolphin, Thunar etc.).
- Click **Go** and **Open Location**.
- Enter server URL from the ERDA **WebDAVS** page (replace https with davs in the URL if it fails).
- Click **Connect**.
- Login with your automatic username and chosen password from ERDA.

NB: Nautilus and Thunar use the GNOME gvfs-library. Older versions of this library had a known error, which consistently caused uploads over 1GB to hang. If you experience this problem, upgrade to a more recent version of the library (e.g. 1.22.2) or use a different client.

WebDAVS/SFTP access to Share Links

To share links og exchange files outside ERDA, combine Share Links with read **and** write-access with effective access and tie share links to your machine as a network drive.

Use share links to share your own folders and group folders as a form of shared drive.

To set up effective access to share links, proceed as in the above, with this difference: use the 10-digit share link ID (e.g. gBf51LXf4T) as both username and password.

In all cases, carefully consider which files you give access to, and which people you give access to the files.

Backup to ERDA

> Only research data that can be open must be handled in ERDA. It is your responsibility to ensure that any backup you save to ERDA does not contain any other data categories.

There are four different ways to backup research data to ERDA: **Scheduled tasks**, **Data transfer**, **automatic backup**, and **server backup to ERDA with scripting**. We walk through all four below.

Scheduled task

ERDA can perform both recurring and one-time tasks with **Scheduled Tasks**. You can schedule e.g. a new backup archive or a specific folder to be created every day at a set time.

Start by adding Scheduled Tasks to your ERDA front page:

- Click **Add**
- Pick Scheduled Tasks
- Click **Save**

For an overview of available variables and commands, consult the two **Help** menus at the bottom of the page.

Monitor running and past Scheduled Tasks in **View Logs**.

Data transfer

If you work with larger datasets, you may need to im- and export research data effectively in ERDA. ERDA supports this workflow via various protocols (SFTP, RSYNC, HTTPS and WebDAVS).

Here, we walk through how to create an ssh-key, and how to use it to import files from an external server via SFTP-access.

- Go to **Home** and click **Data Transfer**.

On the transfers page you will see two headers: **Manage Data Transfers** and **Manage Transfer Keys**.

- **Manage Data Transfers** lets you set up and monitor transfers.
- **Manage Transfer Keys** lets you manage transfer keys

On the **Manage Data Transfers** page, by Login method, select **Login with key** to create an ssh-key.

- Enter your username
- Click **Generate Key**. You will see the public part of the key and brief instructions.
- Paste the public part of the key to the machine, you want to transfer data to or from.

The ssh-key's private part is saved only to an unreachable space in ERDA, as security against unauthorised access.

You can now configure background transfer of one or several files to or from ERDA. Configure the transfer to import the contents of the relevant folder on the remote server and save it to the ERDA data imports folder.

Click **Request transfer** to queue the transfer.

Monitor the transfer from the overview, via the status-buttons, or in the destination folder by clicking on local component.

Transfers can be combined in many ways, all of which follow the same overall method.

Click on **Status files** for more information, if the transfer fails.

Automatic backup to ERDA

With [Duplicati](#), you can automatically save a backup of your PC on ERDA.

Duplicati saves backup files in a special wrapped format, which lets you save special files and files with exotic names to ERDA. Duplicati also offers an easy way to encrypt your backup.

Two versions of Duplicati are available: a user-friendly graphic version, and a command-line version. The latter is recommended for backup of servers and NAS-solutions. We walk through the graphic version below.

Configuration on ERDA

- Go to **ERDA Setup** and click the **Duplicati** banner.
- Enter the name of your backup in the **Backup** field.

The rest of the fields are optional.

NB The protocol you enter in the **Protocol** field (e.g. SFTP), must be set up for login with password in ERDA. For more information, see [Effective access to ERDA](#).

- Click **Save Duplicati Settings**.
- At the bottom og the page, you will see links to a **.json** file for each of your backups. Download the file by right clicking on the link and picking **Save as**.

Loading Duplicati configurations

Download and install the latest 2.x version of [Duplicati](#). Chose the pack compatible with your system.

Upon installation, Duplicati will start up.

- Pick **Add backup**, **Import a file**, and click **Next**.
- Click **Browse** in the **Configuration file** field to find the saved .json file.
- Click **Import**.
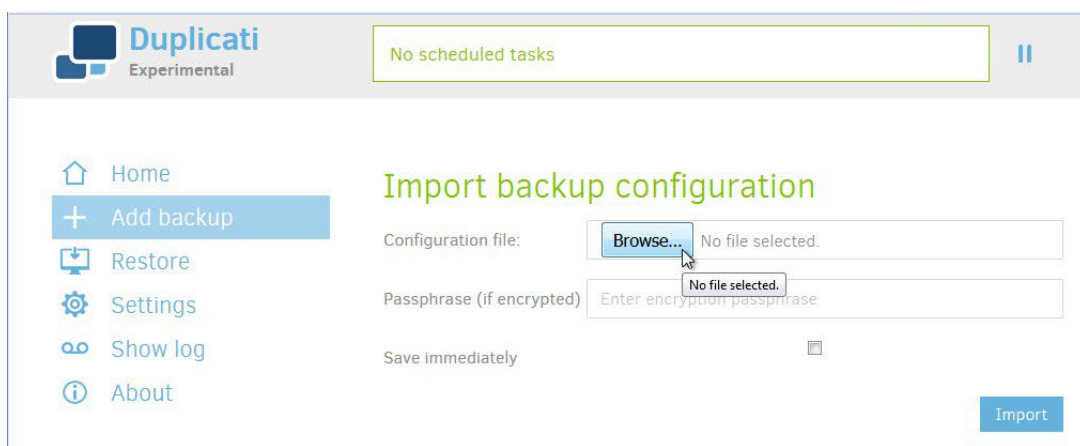
Complete the 5 phases of the Duplicati backup process outlined below.

1: General

Before clicking **Next**, decide whether to set up encryption.

- Determine whether your research data are subject to demands for encryption: AU policy on cryptography.
- Weigh your need for encryption against the strain the process places on your machine.

2: Destination

The ERDA settings will be pre-entered from the configuration file.

- Enter the password for your chosen protocol (your WebDAVS password as default).
- Click **Test connection** to ensure that connection and login are set up correctly.
- Click **Next**.

3: Source data

- Pick which folders to include in backup on ERDA.

Duplicati runs as your normal user and will not automatically have access to system files and facilities. Either exclude such folders from your backup or run Duplicati as privileged user.

- Click **Next**.

4: Schedule

Configure the automatic backup frequency.

- Leave the field under **Allow days** blank. This has the same effect as choosing all.
- Consider correcting **Keep backup** to e.g. 3 years.
- Click **Save** and **Next**.

5: Options

- Click **Continue without encryption** or **Cancel** to go back and set up encryption.
- Click **Run now** to begin backup.

Repeat the proces with **Add backup** for any other .json-files.

For more Duplicati guidance, see Duplicati's Getting Started guide.

Server Backup for ERDA with scripting

If you belong to a research group with its own NAS server, you can script creation of ERDA backup archives of its contents via a project.

- Pick your project (or create one - see Projects (VGrids)).
- Create a subfolder in one of your folders, e.g. "backup".

For security reasons, we recommend not saving your ERDA password on the machine performing backup. Therefore, use either

- SFTP/SSHFS with an ssh-key, (see Effective access) or
- Create a share link with read and write-access (see Share Links).

With share links, you can control access to the folder via WebDAVS/SFTP link-sharing, using the share link ID as username and password.

- Use a command to upload files from the storage server (e.g. sftp or lftp).
- Consider uploading ERDA as a network drive (see Effective access) and use rsync or similar to limit the upload to file changes.
- Set up a workflow rule in your group to integrate the creation of a backup archive in the backup process.

ERDA Workflows

- Open **ERDA Settings**.
- Under **Site Collaboration Links** pick **advanced** instead of **default** to access workflows.
- Go to **ERDA projects**. You will now see a Workflows-pillar.

- Click **Open link** and fill out the form with a new workflows-rule.

External collaboration

Research takes place across universities and most research projects will experience an ongoing need to exchange data with project partners. ERDA is designed to support collaboration, and for this reason, access to the system is based on a zero-trust security model with secure access for all users.

ERDA supports collaboration on research data, both as a course-aide and in projects between organisations.

Peers

To protect against unauthorised access to research data, ERDA separates access at user- and project-level. For this reason, external access to ERDA requires approval by an AU-contact. This process is integrated in **Peers**, where you can specify which external users need to access ERDA.

As an AU employee, there are two ways to invite external partners to become ERDA Peers:

1. Fill in the details of the external users under Peers and send them an invitation from ERDA. In this case, the external partner will be sent a link to a pre-filled sign-up form, to fill out email and password themselves.
2. The external users can sign up to ERDA after which you can approve their user creation. In this case, the external partner will be sent a link to a empty sign-up form, to fill out themselves.

Peers

| Show Peers | Requested Peers | Enter Peers | Import Peers |

You may enter your individual peers in the form fields below and assign a shared kind and account expiry time for all entries. Just leave the Action field to Add unless you want to Update or Remove existing peers. You are free to leave rows empty, but each field in a peer row MUST be filled for the row to be treated.

Label | Kind | Expire ⓘ
Peers name or label | Course | dd-mm-åååå

Action
Add

Full Name | Organization | Email | Country (ISO 3166) | State (if applicable)
Full Name | Organization | Email at organizatio | | 2-Letter state code

- Use **Show Peers** to manage your contacts and resend invitations.
- Use **Requested Peers** to approve external partners who have indicated you as their AU-contact.
- Use **Enter Peers** to manually type in external partners' details.
- Use **Import Peers** to import a CVS-formatted list of your external partners.
- **Label** lets you to keep track of your peers. Note that the field does not accept spaces.
- **Kind** lets you indicate what manner of collaboration your external partner is part of.

Expire sets an expiration date for peer access. The access is limited to a year by default. After the expiration date, approve the peer again or update their information.

Import share link

In a teaching situation, participants will often need to keep a copy of the material. Share files in ERDA via shared folders, to ensure that all participants work on the same copy.

- Create a folder for the relevant research data.
- Share the folder with a read-only share link.
- Share the URL or ID of the link with the participants.

The participants can now download a copy of the research data by importing the share link from the right-click menu in **Files**.

- In the right-click menu under **Import**, enter either the URL or ID of the share link.
- Click **OK**. This copies the contents of the share link to the user's folder.

Support, questions, and comments

If you encounter system errors or functions in SIF that do not operate as described, we would very much like to hear from you.

To ensure that our support is as effective as possible, please include information about your operating system and browser in your query. You can check which operating system and browser you're using at www.whatismybrowser.com or detectmybrowser.com. Screen shots are particularly useful in this context too, because they let us see exactly what you're seeing.

Contact us via sif-info.it@au.dk.