

ERDA

User guide

Aarhus University, spring 2024

Contents

Introduction	4
Usage requirements and rules.....	4
Access to AU ERDA.....	4
Registration.....	4
Login.....	5
Overview	5
Home.....	5
Files	6
Share Link and Workgroup Shared Folders.....	7
Share Links	7
Workgroup Shared Folders	8
Workgroups (VGrids)	9
Workgroups webpages	10
Archives.....	10
Settings and Setup	12
2-factor authentication.....	13
Logout	15
Advanced data access	15
WebDAVS.....	16
Windows file management.....	16
Adjust the size limit for Windows WebDAVS.....	17
Mac OSX file management.....	19
Linux file management	20
SFTP.....	21
WinSCP.....	21
PuTTY SFTP.....	22
Linux file management.....	22
SSHFS.....	22
WebDAVS/SFTP-access to Share Links.....	23
Automatic backup for ERDA.....	23
Server Backup for ERDA with scripting	28
Scheduled Tasks	29
Data Transfer	30
Courses and external collaborations	32

Peers.....	33
Import share link.....	34
Support, questions and comments.....	35

Introduction

ERDA or the Electronic Research Data Archive at Aarhus University (AU) is for AU employees, PhD students, and external collaboration partners. ERDA is a place where you can store, share, analyse and archive research data. ERDA provides secure, centralised storage space for your own and shared files, interactive analysis tools, and archiving facilities for data protection and publication. You can also use ERDA as a secure network drive regardless of where you are.

Usage requirements and rules

You only need internet access to use the basic functions in ERDA. If, on the other hand, you want to use the advanced functions, you may need to install some apps.

ERDA is limited by a few rules, and you can always find them here: <https://erda.au.dk/terms>.

The rules follow common sense, so for instance it is your own responsibility to only store data that you are entitled to store, and to keep your login secure and secret.

IMPORTANT! Read more about data replication and backup in our FAQ/OSS on [ERDA's front page](#), so you know about the data protection we offer and what is your own responsibility. This applies both to our terms of use and to complying with AU's [guidelines for data classification](#).

IMPORTANT! Uploading and storing data containing personal data is subject to strict requirements in the Danish Act on Processing of Personal Data (Persondataloven), cf. [GDPR at AU](#) and [the Danish Data Protection Agency's guidelines](#). Therefore, you **cannot** store such data on ERDA. If you need to store data containing personal data, we recommend ERDA's sister system [SIF](#), which has been approved for this purpose.

Access to AU ERDA

Everyone affiliated with AU has a login and username from the university – you use these details to log on to computers, email systems and internal pages, and to register on ERDA.

In these guidelines, we go through how to register on ERDA if you are registered at AU, but you can also find intros and more guides at <https://erda.au.dk>, where we also explain how to register as an external collaboration partner.

Registration

TIP: Follow our registration guide at <https://erda.au.dk>. We only cover the process for internal employees and students here.

Go to <https://erda.au.dk/>, click on **AU Users** and on **Sign up to ERDA using your AU account?**

Welcome to ERDA

AU Users	External Users	Advanced Access
Sign up to ERDA using your AU account? <input type="button" value="sign up"/>	I'm already signed up to ERDA with my AU account! <input type="button" value="log in"/>	

If you are already logged in to your AU account, the next step will happen automatically. Otherwise, you have to approve login via your **Microsoft Authenticator app**.



ERDA will now set you up as a user and open your front page. ERDA will also send you a welcome email with a link to the page, so if you are stuck you can get in that way.

Login

Once you have registered, you can always log in by going to <https://erda.au.dk> and approving the login with Microsoft Authenticator. Your browser will remember the login for some time, so you may not be asked to log in every time.

If you share your computer with other people, we recommend that you log out of ERDA after every session.

Overview

Opening ERDA will take you to Home where your apps are located: **Home**, **Files**, **Workgroups**, **Archives**, and **Setup** as default. We will describe these in more detail in the next section.

Home

From **Home**, you can open your apps and select the ones you want on the front page.

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: Easy data Analysis and Presentation ...**

Your apps & app-setup

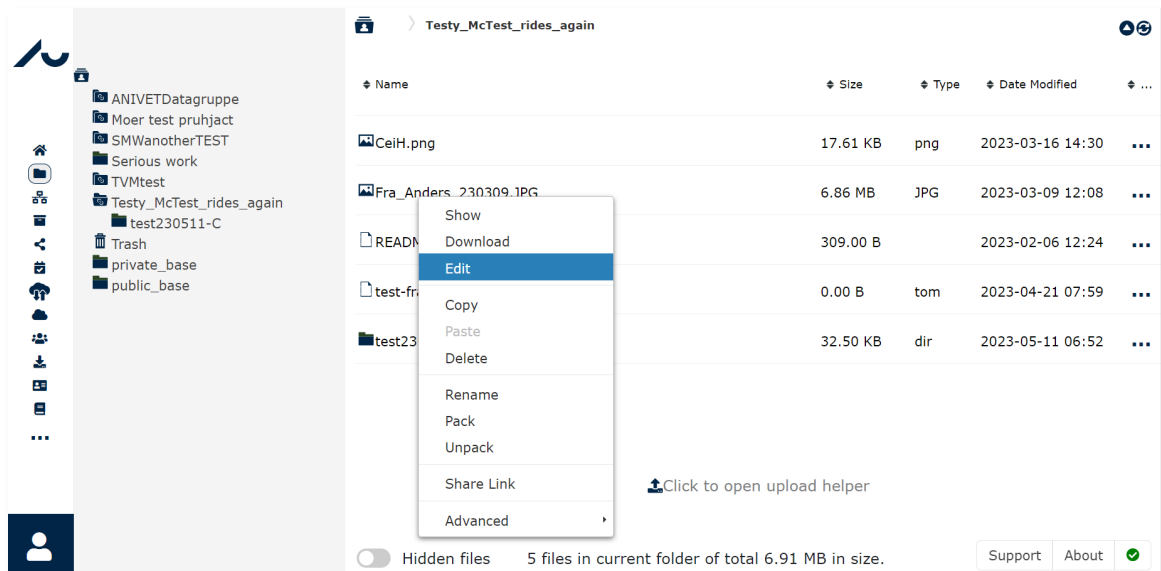


Click on an app to open it, and on **Add** to add or remove the apps you can see.

Files

Files is the main page of your data, where you can manage and open your own and shared files. The overview on the left links to subfolders, and the panel on the right shows everything in the folder you have open.

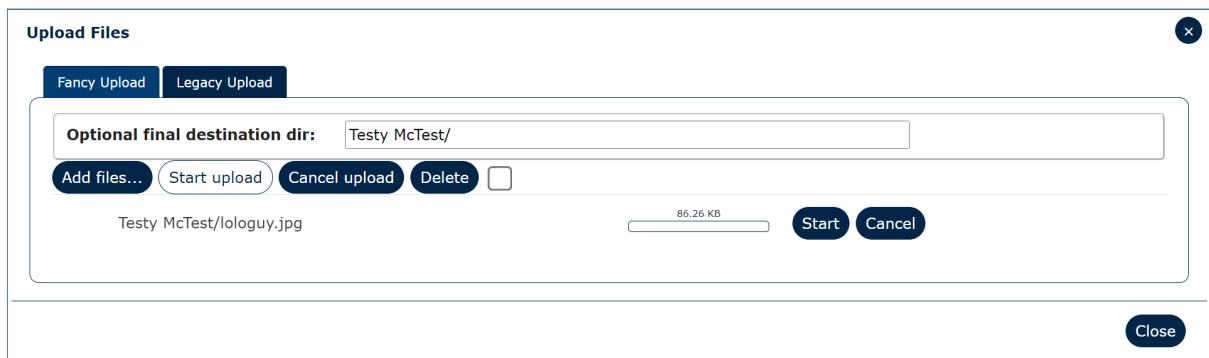
The bar at the top shows the path to the folder you have opened, and links to folders higher up the path.



Right-click on a folder or a file for a menu with the most common actions. For files, actions include **Download**, **Edit** and **Rename**; for folders, actions include **Upload**, **Create** or **Edit**. You can also display the folder's right-click menu by clicking in the empty field under the right-hand panel.

You can add files via **Create File** or upload using **Upload File**. Upload will open a drag and drop window. If you want to add several files at the same time, use **Add files**.

For example, you can choose **Create Folder**, name the folder *uploads* and click **OK**. Double-click on the new folder to open it, right-click in the folder and select **Upload File** and **Add Files...** NB: upload will not start on its own; click **Start upload**. Wait for the upload or click **Cancel** if you regret. Click **Close** to close the window and see the new files in your folder.



Double-click on a file to open it in your browser. If your browser cannot open the file, your computer will download the file so you can work on it locally. Remember to upload the file to ERDA when you are finished, otherwise your changes will not be reflected in the system.

You can edit text files directly using **Edit** in the right-click menu.

In the sections on **Advanced data access**, we show how you can easily work directly with your files in ERDA without downloading and uploading.

Share Link and Workgroup Shared Folders

Research collaboration often requires sharing data with others, and ERDA offers several options for this. If you need to share data once or exchange data with colleagues who do not have an ERDA account, **Share Link** is quickest and easiest option.

If, on the other hand, you need to share files more transparently and permanently, **Workgroup Shared Folders** will work better. This allows you to automatically and dynamically share folders with a group you define yourself and to fine-tune access control.

Share Links

In ERDA, you can share data simply and quickly with **Share Links**. Right-click on a folder or file in **Files**, select **Share Link** and **Create**. This will open a window where you must choose which combination of **Read Access** and **Write Access** you want to use. Tick the boxes to share data with read access, write access, or read and write access. Click **OK**

Create Share Link

You can explicitly share files and directories with anyone using share links. That is especially useful when sharing data with people who do not have an account here, so that basic Project sharing is impossible. Individual files can only be shared read-only, but folders can additionally be shared with read-write or write-only access to allow recipients of the share link to write and upload in the share.

Please be careful about giving write access to anyone you do not fully trust, and note that you can always delete share links again later to limit the risks of abuse.

File/folder to share:

Read Access **Write Access**

Ok **Cancel**

In this example, we have granted read access, so that our colleague can only read and download the file.

Click **Open share link** when the link is ready to see what it looks like for the recipients. Now you can either send the page address to your colleagues yourself or use the helper to email invitations.

Click **Edit and send share link** to open the helper. Enter the email addresses to which you want to send the invitation in **Recipients** and, if you wish, include a message to the recipients. Finally, click **Send invitation(s)**.

Edit Share Link

Here you can send invitations for your share link gAI0sH0VhS to one or more comma-separated recipients.

ID	Action	Path	Access	Created	Active	Owner	Invites	Expire	Single file
gAI0sH0VhS	Serious read work	/C=NA/ST=NA/L=NA/O=NA/OU=NA/CN=Sara Marie Westh/emailAddress=samawe@au.dk		Wed Jun 7 12:45:21 2023	Yes		mimsen_sarma@hotmail.com		False

Send Share Link Invitations

After creating a share link you can manually give the link to anyone you want to share the data with and/or use this form to send invitations on email. Please note that abuse of this service to send out spam mail is strictly prohibited and will be sanctioned.

Share Link ID:

Recipient(s):

Automatic Message:

Hi,
Sara Marie Westh (samawe@au.dk) has shared ERDA data with you on:
<https://anon.erda.au.dk/sharelink/gAI0sH0VhS>

--- Optional invitation message follows below ---

Optional Message:

Send invitation(s)

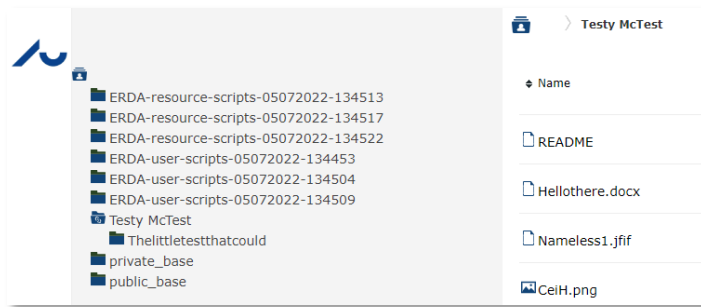
[Return to share link overview](#)

Later, if you want to invite more colleagues or see, change or delete share links, you can use the **Share Links** app. Open **Home** and click **Add** to add the app to your front page. Click **Save**. The **Share Links** app is now available on your **Home** page.

Find information about advanced **Share Links** under [WebDAVS/SFTP-access](#).

Workgroup Shared Folders

The other simple way to share files is through **Workgroup shared folders**, for example if you want to share files with a Workgroup group or a collaboration. ERDA integrates Workgroup shares closely, making it easy to share files directly in **Files**. All groups automatically have a shared folder with this icon: All files and folders you store here will automatically be shared with members of the group.



In our example, I own the Testy McTest Workgroup and can see the shared folder with the README file and the folder from the subWorkgroup. I have only shared the Testy McTest folder, so the Thelittlestthatcould folder has a standard folder icon.



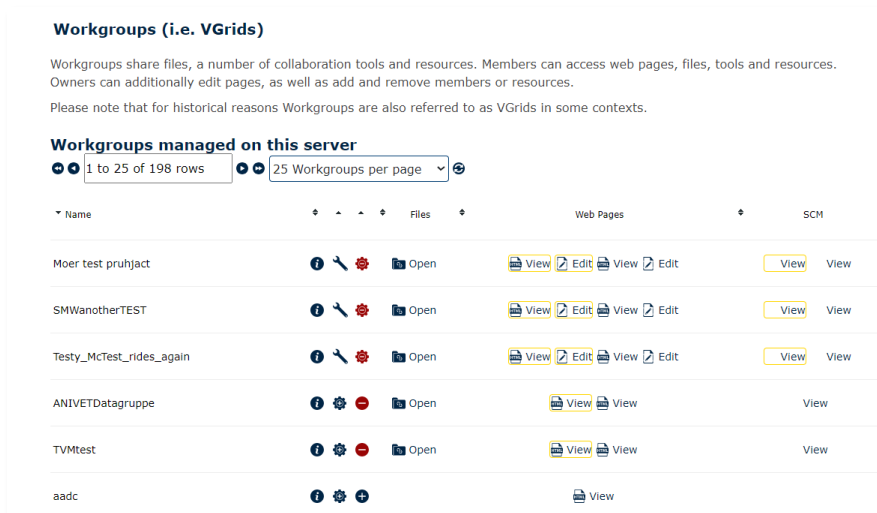
In the next section, we will go through how you register in a group.



Workgroups (VGrids)

Use **Workgroups** to share files with your colleagues.

TIP: Consult our short guide to **Workgroups** at <https://erda.au.dk>. The guide has an intro and a little more information about how to use the app.

On your Workgroups page, you can see all the Workgroups on the server. The Workgroups you are part of have some extra elements available, for example links to shared files and the group's webpages.



Click on the **request membership** icon  to get access to a group. Use the **request ownership** icon  if you want to be a co-owner of the group. When you click on the icon, a pop-up window will appear where you can explain to the group owner why you need access.

Users with special rights can also add new groups with the **Create Workgroup** button at the bottom of their **Workgroups** page.

Workgroups webpages

Workgroups has a simple infrastructure where you can link webpages so you can present your Workgroup either to the group members or the whole world.

When you create a group or become a co-owner of one, you will receive two new folders on ERDA:

- a) private_base
- b) public_base

Both folders will make webpages with the files you store in them. The ones you store in a) will only be visible to the group members, while the ones you store in b) will be available to the entire internet. You can use the folders to manage the content on the website, or to open the online editor via **Edit-Links** on the Workgroup page. You will also find **View-links** to the webpages here. Everyone can see the public webpages if they have the link.

Archives

Archives allows you to lock and archive a still of your files (frozen archives). This is a mandatory step if you need to submit a PhD dissertation and sometimes also when you send articles to conferences or journals. Once you have created some files, your archive list might look like this:

Frozen Archives

Frozen archives are write-once collections of files used e.g. in relation to conference paper submissions. Please note that local policies may prevent users from deleting frozen archives without explicit acceptance from the management.

Existing frozen archives

1 to 3 of 3 rows | 25 frozen archives per page

ID	Name	Created	Flavor	State	Files
archive-dRx7t6	Sara Marie Westh	Tue Jul 5 15:21:09 2022	freeze	FINAL	1
archive-ki63zz	backup-2022-07-05T152205.493590	Tue Jul 5 15:22:40 2022	backup	FINAL	1
archive-C1LRj3	Me	Fri Jul 15 13:04:43 2022	freeze	FINAL	1

Additional Frozen Archives

You can create frozen snapshots/archives of particular subsets of your data in order to make sure a verbatim copy is preserved. The freeze archive method includes support for persistent publishing, so that you can e.g. reference your data in publications. Backup archives can be used as a basic backup mechanism, so that you can manually recover from any erroneous file removals.

Choose one of the archive methods below to make a manual archive:

- Create a new freeze archive
- Create a new backup archive

You can see an archive by clicking on , changing unfinished archives with and, if you have access to it, deleting your files with .

Click on **Create a new frozen archive** to add a new archive. As an example, below we have created a new archive named *Article Data* and completed the form.

Freeze Archive

Please enter your archive details below and select any files to be included in the archive.

Name:

Author(s):

Description:
 Archive with article metadata and an ERDA file

Apart from this free text field, archives get a few fields like date and owner assigned automatically.

Freeze Archive Files:

Make Dataset Publicly Available @yes no

You can add ERDA files with **Add file/directory** and files from your PC with **Add upload**. **Add file** will open a window where you can select the files you want add. Double-click to select a single file or right-click and choose **Select** for the entire folder. **Add upload** will open an upload window, just like with **Files**. Add files, select whether the archive should be publicly available, and click **Save and Preview**.

If you have selected **Make Dataset Publicly Available**, you can see a preview with **Preview publishing**. Use **Edit archive** to add and change files. Select **Finalize archive** to freeze the archive permanently and indicate that it is ready to be archived on tape. Your data will not be secure until you have clicked **Finalize archive**, and it will then be stored for at least ten years.

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.

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

NB: archiving will *not* remove the ERDA files you have selected. It will just save a copy. Therefore, you can continue to work on the files without it changing the archived version.

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

Show Freeze Archive Details

1 to 1 of 1 rows 25 frozen files per page Loaded cached archive - update pending

Name	Action	Date	Size in bytes
Testy McTest/thanos-snap-gif.gif		2022-07-15 13:04:43	1038408

ID archive-C1LRj3
Name Me
Flavor freeze
Description Frozen archive
Published No
State PENDING
Creator /C=NA/ST=NA/L=NA/O=NA/OU=NA/CN=Sara Marie Westh/emailAddress=samawe@au.dk
Created Fri Jul 15 13:04:43 2022
On disk 2022-07-15 13:04:43

Show archive with file checksums - might take quite a while to calculate:

You can continue inspecting and changing your archive until you're satisfied, then finalize it for actual persistent freezing.

Settings and Setup

You can adjust your ERDA settings on the **Settings** and **Setup** pages. Among other things, you can change the appearance and behaviour of the pages and set up advanced access methods such as SFTP/WebDAVS clients or map remote directories as a network drive on your PC.

Find more information about the **SFTP/WebDAVS** tabs and how to use them in the sections on Advanced data access.

You do not need to change the default settings to use the basic functions, so leave them as they are if you are in doubt.

Settings

Select your ERDA settings

Please note that if you want to set multiple values (e.g. addresses) in the same field, you must write each value on a separate line but without blank lines.

Email
List of E-mail addresses

1	samawe@au.dk
---	--------------

Language
Your preferred interface language
English

User Interface
Your preferred web interface
V3

Default Page
Your preferred page opened on login
Home

Site Base Menu
Which base menu to use.
default

Site User Menu
Additional menu items.

- sharelinks
- seafile
- crontab
- transfers
- cloud

Site Collaboration Links
Which group collaboration components to use.
advanced

Save General Settings

You can select the page you use most as your **Default Page**, so you start on it when you log in.

Change Site Collaboration Links from **default** to **advanced** to see more functions on your Workgroups page.

Setup gives you access to some slightly more advanced functions, which we will go through below.

2-factor authentication

There is an ever-increasing number of automated attacks and phishing attempts online, where hackers try to guess passwords or extract information from people. We therefore recommend that you make your login extra secure.

All ERDA services offer 2-factor authentication (2FA), which is precisely the kind of extra security we recommend. 2FA adds an extra step to your login, so you need to use something you know (name and code) as well as something you have. On ERDA, this is a single-use code of six numbers, a *token*. ERDA uses the TOTP standard for tokens, and you need to install an app that generates them on your mobile or tablet.

To set up 2FA on ERDA, open **2-Factor auth** under **Setup**. Click **OK, let's go** and install an app for TOTP authentication. You can find the apps where you usually download them from.

Setup

SFTP WebDAVS FTPS Duplicati **2-Factor Auth**

2-Factor Authentication

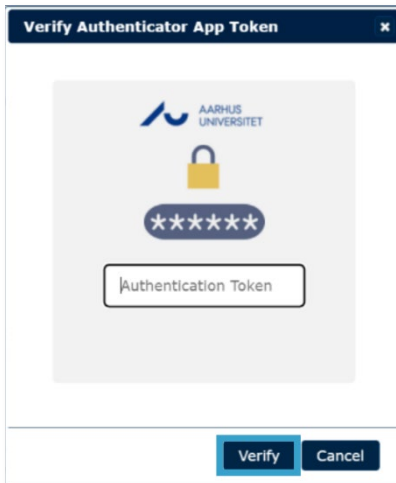
We allow 2-factor authentication on ERDA for greater password login security. In short it means that you enter a generated single-use token from e.g. your phone or tablet along with your usual login. This combination makes account abuse much harder, because even if your password gets stolen, it can't be used without your device.

Preparing and enabling 2-factor authentication for your login is done in four steps.

Okay, let's go!

Click **I've got it installed**. Now you can import your personal token by scanning the QR code or entering the text code. If your device has a camera, it is easiest to scan. In the example below, we have used Microsoft Authenticator, which is AU's general app for 2-factor authentication. We have also selected **Scan a QR code**.

Click **QR Code** in ERDA and aim the camera on your device at the code. The app will usually open a window with your token. Click **Done importing** in ERDA, and enter the code in the pop-up window. Click **Verify** to check that your app is working properly. Tokens change every 30 seconds, so if the authentication fails because it takes too long, just try again.



Once your token has been approved, the guide will continue to the final step where you select the security level of your 2FA.

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.

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](#)

The latter is usually more cumbersome but may be needed if your app or smart device doesn't support scanning QR codes. Most apps automatically add service and account info on QR code scanning, but otherwise you can manually enter it.

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!

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 ERDA logins are security-enhanced with a request for your current token from your authenticator app.

SECURITY NOTE: please immediately contact the 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 AU OpenID web login

Add an extra layer of security to your AU OpenID web logins through a personal auth token generator on your phone or tablet.



Enable 2-FA for Non-AU OpenID web login

Add an extra layer of security to your Non-AU OpenID web logins through a personal auth token generator on your phone or tablet.



[Save 2-Factor Auth Settings](#)

You can choose to enable 2FA for both your AU and non-AU web logins. If you select these options, four new points will appear. Select all of them for maximum protection.

Click **Save 2-Factor Auth Settings** to finish. The next time you log on to ERDA, you will be asked to log in with 2FA after you have entered your username and password.

Logout

When you have finished working in ERDA, we recommend that you log out. Click **Sign Out** at the bottom of the user menu and **Yes** to log out. It is even more important that you log out if you share your computer with others.

Advanced data access

In addition to the web interface, there are other ways in which you can work with your files in ERDA – ways that give you more efficient, transparent and integrated access. With advanced data access, you can transfer many and large files efficiently and map your ERDA files onto your PC as a network drive, so you can work on them as if they were local files. All ERDA accesses use a secure connection, so that they are always available if you are online. This means that you do *not* need to use the VPN to gain access outside AU.

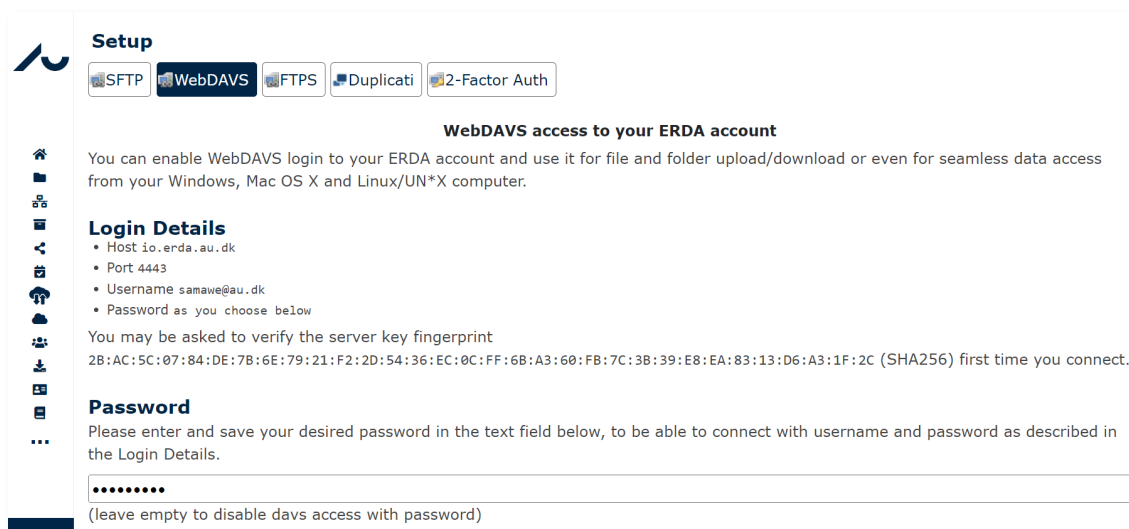
TIP: Consult our intro at <https://erda.au.dk> to see how to set up ERDA as a network drive using SSHFS or WebDAVS. We also provide more information on the platforms below.

WebDAVS

We don't recommend using WebDAVS for file transfers: this protocol is slow, strains the system, and in order to use it to transfer larger files, you must first change your computer's setup.

WebDAVS is a protocol to access remote storage via an add-on to the http protocol, and it can be secured with TLS/SSL like webpages. We call the secured version WebDAVS. Newer versions of Microsoft Windows, Mac OSX and Linux integrate WebDAVS, so you can safely access the remote storage without installing new programs. It is relatively easy to use WebDAVS, but it has some limitations: it is not particularly efficient if you are working with large amounts of data, nor is it robust in terms of network outages. We recommend an [SFTP-based option](#) if you want capacity and stability.

Open **WebDAVS** under ERDA **Setup** and configure how you want to identify yourself on our server. Choose a password for login and click **Save WebDAVS Settings**. **NB:** your login details – including your automatic username – will be displayed in the same place.



The screenshot shows the 'Setup' page for WebDAVS access to an ERDA account. At the top, there are navigation tabs for SFTP, WebDAVS (which is selected), FTPS, Duplicati, and 2-Factor Auth. Below the tabs, the heading is 'WebDAVS access to your ERDA account'. The main text explains that WebDAVS login can be used for file and folder upload/download or for seamless data access from Windows, Mac OS X, and Linux/UNIX computers. Under 'Login Details', the following information is listed: Host io.erda.au.dk, Port 4443, Username samawe@au.dk, and Password as you choose below. A server key fingerprint is also provided: 2B:AC:5C:07:84:DE:7B:6E:79:21:F2:2D:54:36:EC:0C:FF:6B:A3:60:FB:7C:3B:39:E8:EA:83:13:D6:A3:1F:2C (SHA256) first time you connect. The 'Password' section asks the user to enter a password in a text field, with a note to leave it empty to disable access. The password field contains several dots, indicating it is masked.

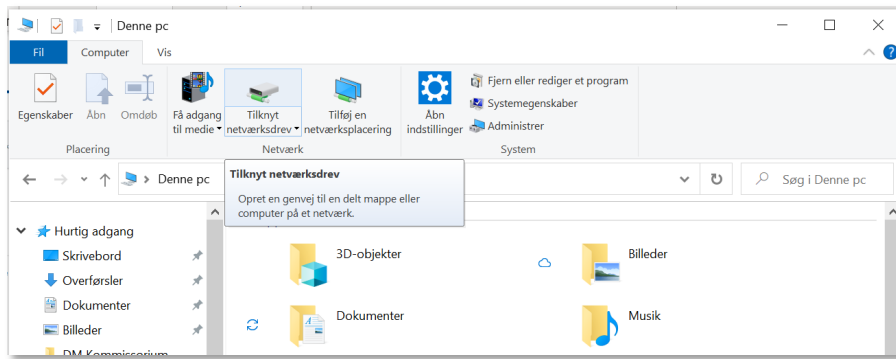
You can find the URL you need to establish the connection by combining **Host** and **Port**. In our example, it is <https://io.erda.au.dk:4443>. The automatic username is the email you use to log in.

In the below paragraphs we will walk through the different ways you can connect to your ERDA folders via WebDAVS, once you have created the initial setup in ERDA.

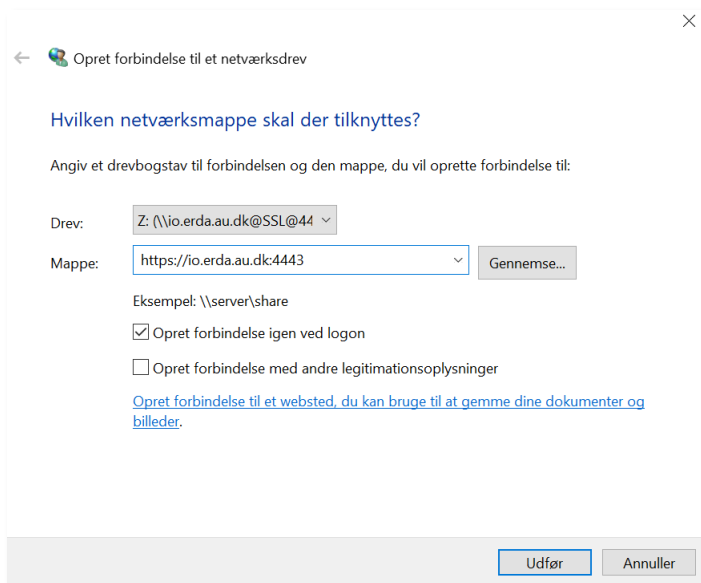
Windows file management

In Windows, you can open WebDAVS remote folders from Files. The appearance changes slightly between the different versions, and you can also use other commercial solutions. Here we show how to use **Tilknyt netværksdrev** in Windows 10.

Click on **Computer** and **Tilknyt netværksdrev** to start the guide.



Choose a letter for your network drive (e.g. Z:), copy paste the server URL from ERDA and click **Udfør**.



Log in using your username and the password you selected in the **WebDAVS** tab and click **OK**.

If your login is successful, you will see your ERDA files under the drive name you selected.

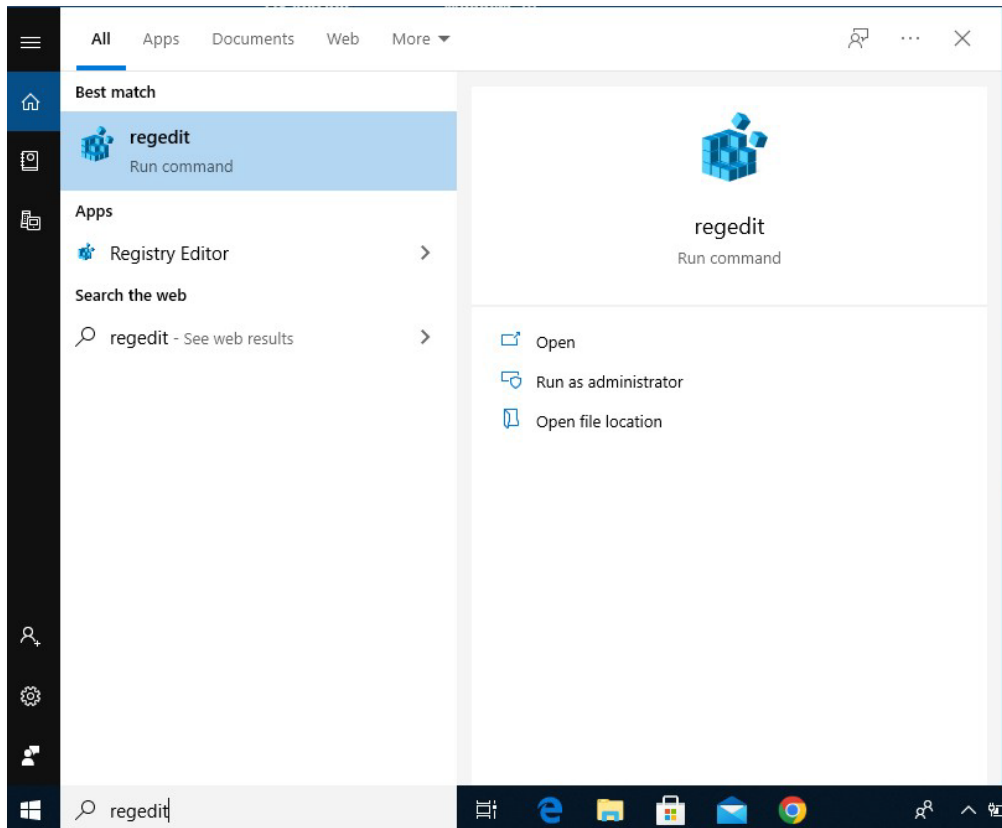
As long as you are online, you can work on the files in the same way as those on your PC. The next time you start your device, you only need to open the network drive. When you have finished working on the files, right-click on the drive and select **Disconnect** to close the connection.

Adjust the size limit for Windows WebDAVS

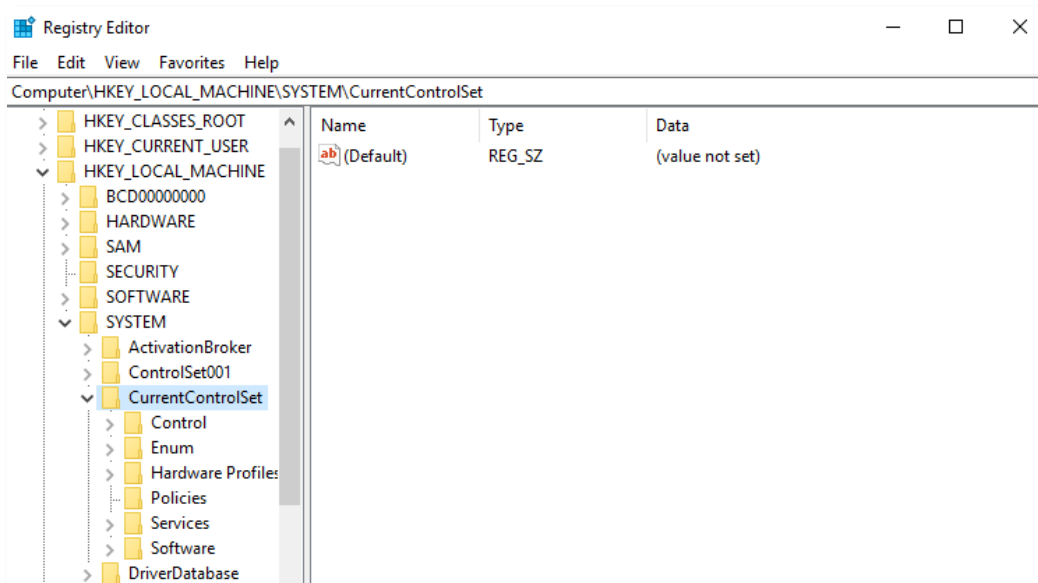
Unfortunately, Microsoft has set a low limit on the size of the files you can download through WebDAVS. This means that you will receive an error message if you try to download files of around 50MB or more.

You can increase the limit to 4GB through the **Registry Editor**. We will go through how you do this, but the solution is also described here: [FIX: Error 0x800700DF The file size exceeds the limit allowed and cannot be saved in SharePoint & WebDAV. - wintips.org - Windows Tips & How-tos.](https://www.wintips.org/windows-tips-how-tos/fix-error-0x800700df-the-file-size-exceeds-the-limit-allowed-and-cannot-be-saved-in-sharepoint-webdav/)

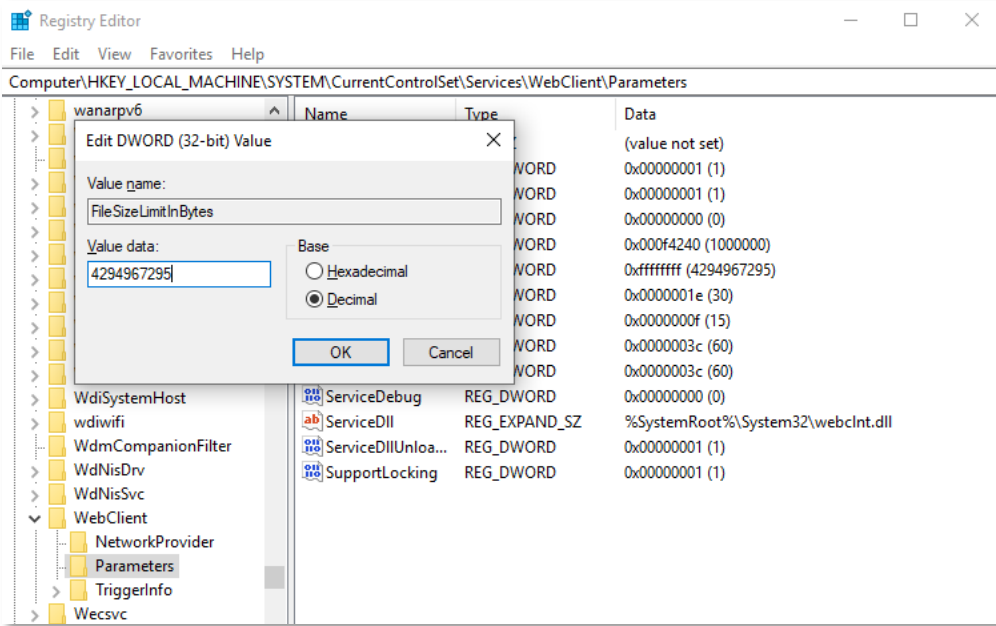
Search for *Regedit* on your computer and run the command.



Select the **HKEY_LOCAL_MACHINE**, folder, open **SYSTEM**, and open **CurrentControlSet**.



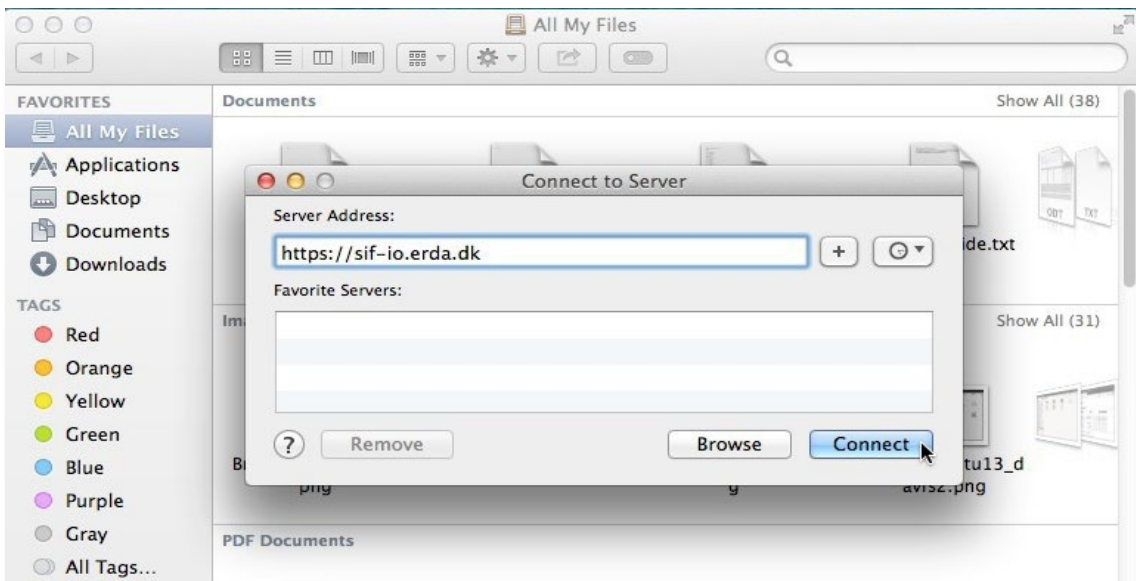
Open **Services**, **WebClient** and **Parameters**. This will take you to **FilesizeLimitInBytes**, where you can change the value to, for example, 4294967295 in Decimal base. You can now transfer files of up to 4GB.



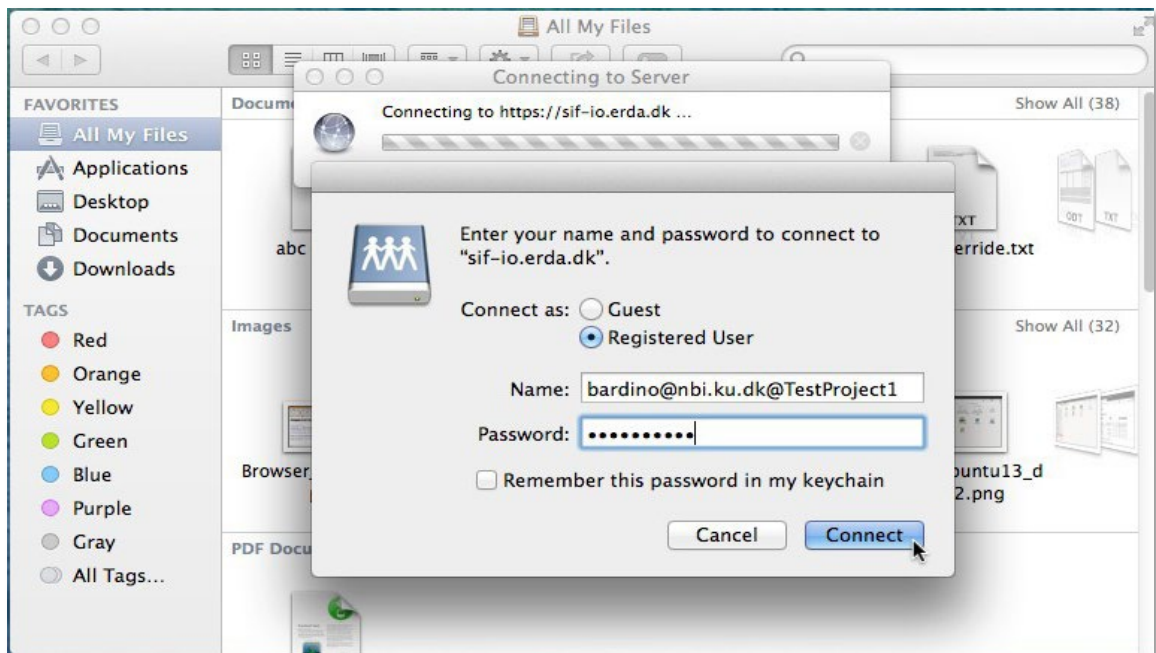
If you work with large amounts of data, we recommend that you use [SSHFS](#) instead of WebDAVS.

Mac OSX file management

On Mac OSX, use Finder to open WebDAVS folders. Select **Connect to Server** under **Go** and enter the server URL from ERDA's **WebDAVS** tab under Server Address. Click **Connect**.



Log in with the username and code you selected on the **WebDAVS** tab. In the example below, we used the automatic username [bardino@nbi.ku.dk@TestProject1](#).

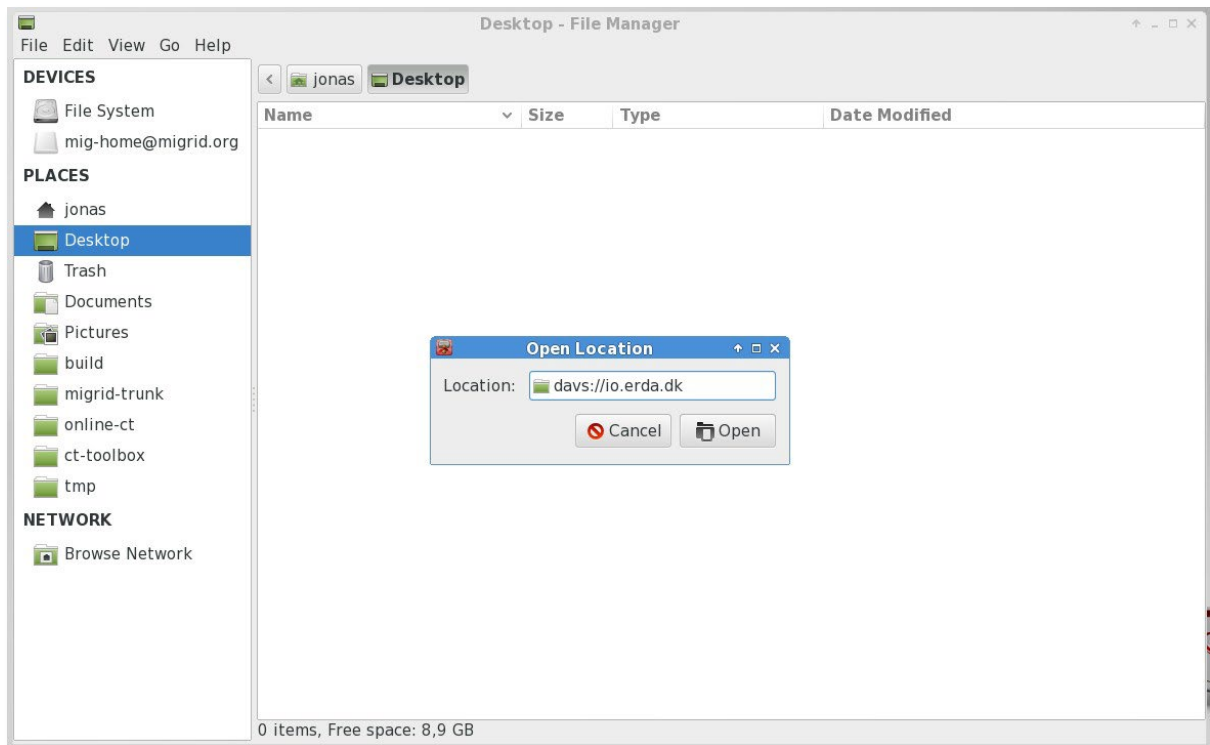


If your login is successful, you will see your SIF folder on your device.

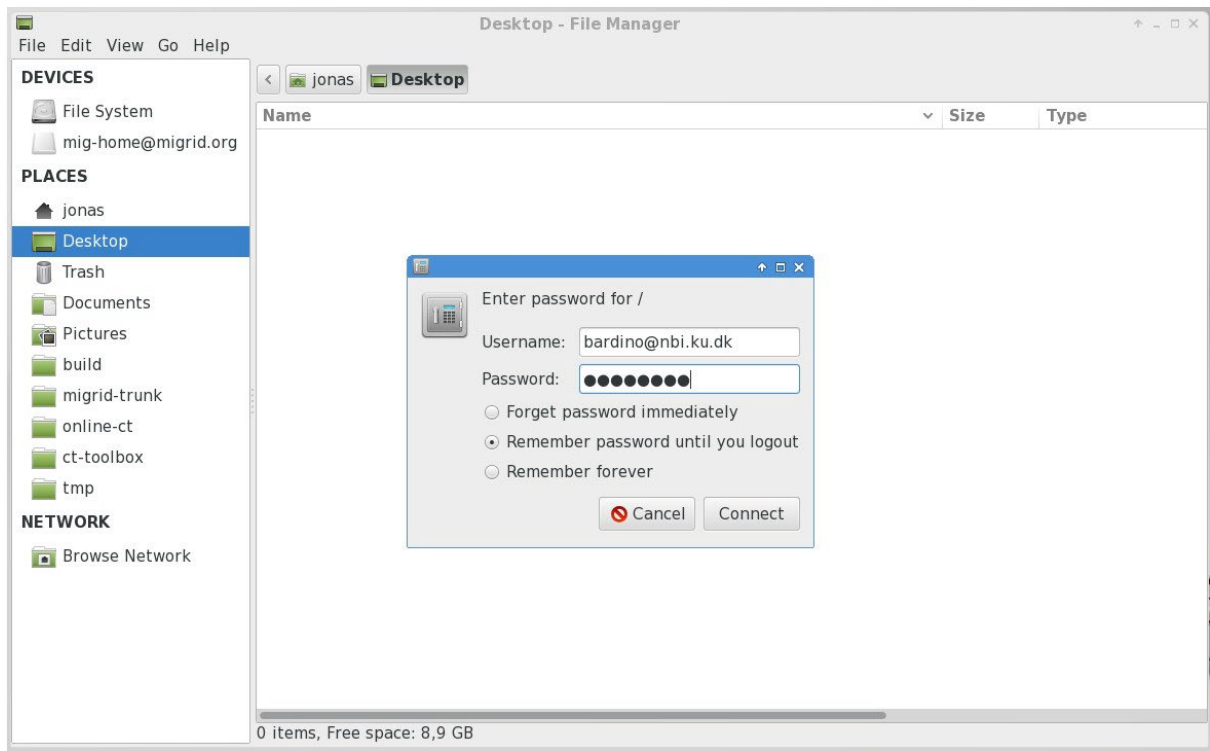
Linux file management

On most modern Linux distributions, you can open WebDAVS folders with file manager, regardless of whether it is Nautilus, Konqueror, Dolphin, Thunar or a fifth. Click **Go** and select **Open Location**.

Enter the server URL from **WebDAVS** (if it doesn't work, replace https with davs in the URL) and click **Connect**. We used XFCE with Thunar, and therefore davs as the prefix in the server URL instead of https.



Log in with the username and password from the **WebDAVS** tab. In the example below, we used the automatic username [bardino@nbi.ku.dk@TestProject1](#).



If you manage to login, you will see the remote content in your system.

NB: Nautilus/Thunar use the GNOME gvfs library, which had an error in older versions. The error consistently caused files of over 1GB to get stuck during upload. If you experience this problem, upgrade to a newer version of gvfs (e.g. 1.22.2) or use another client.

SFTP

SFTP is a secure and efficient protocol for file transfers, a little like the old FTP protocol, but with built-in security. SFTP builds on [the OpenSSH](#) security infrastructure and is supported by a number of clients on the popular platforms. Some of them integrate the functionality in their file management, so you do not need to download apps.

Open the **SFTP** tab under **Setup** and configure how you want to identify yourself on our server. Either copy-paste one or more SSH public keys¹ or choose a password and click **Save SFTP Settings**. **NB:** your login details – including your username – will be displayed in the same place.

You can use one of the clients below, which we know all work with ERDA, but other clients should also work.

WinSCP

WinSCP is another FTP/SFTP client for Windows. WinSCP is available in a **portable** version that can run anywhere without installation and without administrator access. WinSCP is also has a **semi-**

¹ Read more about SSH public keys here: [Git - Generating Your SSH Public Key \(git-scm.com\)](#).

automatic sync function that makes it easier to synchronise files between your device and ERDA.

The first time you connect, you will be asked to verify the ERDA server. Use the details from your **SFTP Setup** page in ERDA. Click **OK**. Now your ERDA files should be visible in the panel on the right.

Find more information on the Workgroup's own website: <https://winscp.net/>

PuTTY SFTP

PuTTY is an SSH client developed for Windows, but it is now also available on other platforms. It includes an SFTP client command line that can be used with ERDA.

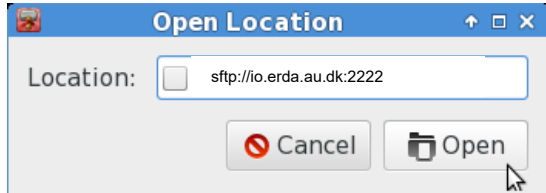
NB: for security reasons, you *must* use version 0.67 or later versions to connect to our SFTP service. Older versions (at least until 0.64) will refuse to connect, with the error message "Couldn't agree a key exchange algorithm: available...". PuTTY [Change Log](#) lists several security fixes, which is a sufficient reason to upgrade to version 0.68 or later.

Find more information on the Workgroup's own website: www.chiark.greenend.org.uk/~sgtatham/putty/

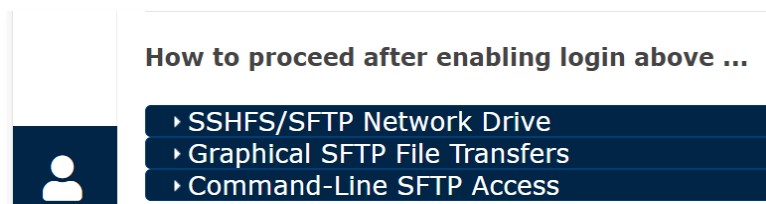
Linux file management

On most modern Linux distributions, you can access SFTP remote folders with the file Manager. The procedure is similar to WebDAVS, but you need to change the URL to point to SFTP.

Enter server details from **SFTP** under setup and click **Connect**. Replace sftp with ssh in the address if it fails. In our example, you need to type in sftp://io.erda.au.dk:2222, since we use port 2222.



The rest of the setup is like for WebDAVS, but with login details from your SFTP Setup. You can find further details about the different protocols as well as a how-to guide at the bottom of the ERDA Setup page, under the SFTP heading:



SSHFS

On Mac OSX and Linux you can map remote directories locally with SSHFS, so you can use the content as if it were a local folder, and now Windows also has a well-functioning client. SSHFS uses an SSH/SFTP connection and has inherited its capacity and robustness. You can use it directly with ERDA SFTP.

Install SSHFS on Windows by downloading and running **WinFsp** and **SSHFS-Win** from Win-SSHFS. Now your ordinary file management can support **map drive** via SFTP – more or less as described under [WebDAVS for Windows](#), but without the difficult additional system adjustments.

A short guide with a practical example and a video is available on the Win-SSHFS page, and there you can see that you need to use the form `\\sshfs\BRUGERNAVN@SERVER` in connection with map drive. Write USER NAME and SERVER as described under [SFTP](#), with the login you chose in ERDA.

On Mac OSX, you can install SSHFS by downloading and opening **FUSE For OS X** and **SSHFS** packages from **OSXFuse SSHFS** or through the **MacPorts/Brew** commands. With FUSE, you can also use MacFusion, which integrates your SSHFS as an image instead of using terminal commands.

On Linux, you must install SSHFS via **Software Center** or the **APT/YUM** commands. Here, the name of the package is `sshfs`. In addition to the example from the ERDA **SFTP** tab, there are several guides online to help you if you get stuck. You can also use Linux's built-in SFTP support from Filhåndteringen if you do not want to install sshfs and familiarise yourself with how to use it from the command line.

WebDAVS/SFTP-access to Share Links

Provided they have read- and write- access, you can combine ERDA Share Links with efficient file access from WebDAVS and SFTP. With these, you can map share links, provided the link has both read **and** write access, to your PC as a network drive. In this way, you can exchange files with collaboration partners who *do not* have an ERDA account.

You can also share a folder as a type of shared drive with share links if you want to avoid logging on to ERDA. In this way, you can share your own folders and folders from a group.

Previously, we went through how you map folders from different platforms, and here the procedure is the same. The only difference is that you must use the share link ID of 10 characters both as your username and code. You can share the share link with ID gBf51LXf4T by connecting to WebDAVS/SFTP with gBf51LXf4T as both username and code.

Automatic backup for ERDA

You can combine Avanceret datatilgang with Duplicati, a free and open backup program to automatically save backups of your PC on ERDA. Duplicati saves backup files in a special format, so you can use it to save special files and files with names that ERDA does not accept. This is also an easy way to encrypt your backup, so that no one else can read it, even if they gain access without authorisation.

Duplicati is available in both a user-friendly image version and a command line version, which is better if you need to backup servers and certain NAS solutions. Below is a description of the graphical solution.

You need to go through two steps to set up Duplicati: 1) configure on ERDA through **Duplicati Setup** and 2) upload the resulting configurations in Duplicati onto your PC.

Go to ERDA **Setup** and click on the **Duplicati** tab.

Setup

SFTP
 WebDAVS
 FTPS
 Duplicati
 2-Factor Auth

Duplicati Backup to ERDA

You can install the Duplicati client on your local machine and use it to backup arbitrary data to ERDA. We recommend the most recent version of Duplicati to be able to import the generated configurations from here directly.

Configure Backup Sets

You can define the backup sets here and then afterwards just download and import the configuration file in your Duplicati client, to set up everything for ERDA backup use.

Backups

List of backup set IDs.

1

Protocol

Which protocol to use for communicating with the server.

SFTP

Username

Username for given protocol when communicating with the server.

samawe@au.dk

Schedule

Optional scheduling of automatic runs this often.

Daily

Save Duplicati Settings

Import Backup Sets

Your saved ERDA Duplicati backup settings are available for download below:

Enter the name of your backup in the **Backup** field, e.g. the name of the PC or folder you want to back up.

The remaining fields are optional. Remember that SFTP, or the alternative you choose in the **Protocol** field, must be set up for login with a password in **ERDA Setup**. We have previously looked at how you set up passwords for the various protocols.

Click **Save Duplicati Settings**. At the bottom, there are links to a **.json** file for each backup name you chose. Download the file by right-clicking on the link and selecting **Save as**.

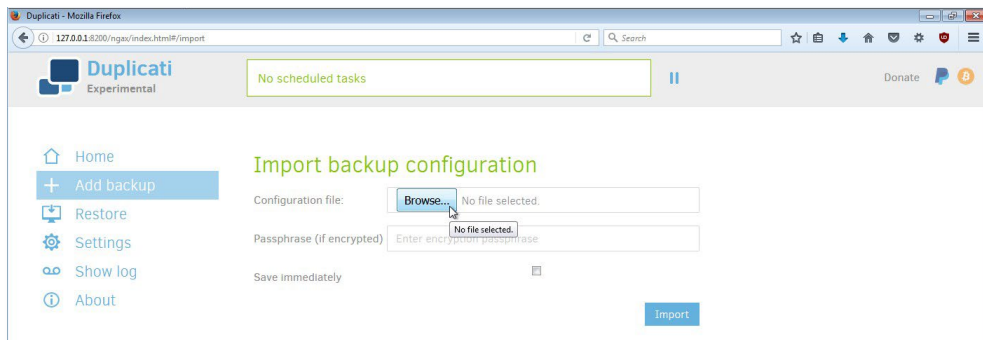
To complete the second step of the setup, you must import the **.json** file in Duplicati. Download and install the latest 2.x version from [Duplicati](#). This has pre-packed versions for a wide range of popular platforms. In the example below, we use a file ending with **-x86.msi**, which is suitable for 32-bit Windows. If you are using 64-bit Windows, you must download the file ending with **-x64.msi**, and **.dmg** if you are a Mac user.



Install the package by double-clicking on the file and following the guide. On Windows, Update should have the necessary .Net 4.5+ library, but on other platforms you may need to install the corresponding Mono 3.0+ libraries.²

When you have installed Duplicati, the program will start up on its own and display the overview page. You can always open Duplicati by clicking on the icon in the bottom right-hand corner and selecting Open.

Select **Add backup** in the Duplicati menu, click **Import a file**, and **Next**. In the **Configuration file** field, select **Browse** to find the saved .json file. Click **Import**.



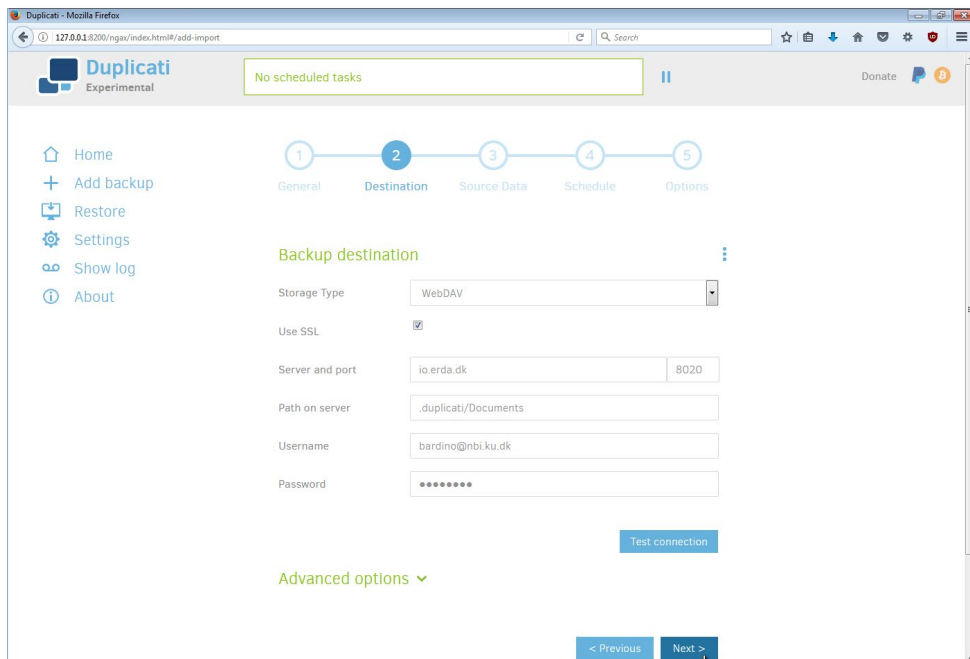
Before clicking **Next**, you can choose to set up encryption. Here, we show how it looks without encryption.

You need to weigh your need for encryption against the impact encrypting and decrypting backup data has on your PC.

On the next page of the **Duplicati** guide, the settings from ERDA have been prefilled-in from the configuration file. The only exception is your password, which you must enter yourself with the protocol you have selected. With the standard settings, you have to use your ERDA WebDAVS code.

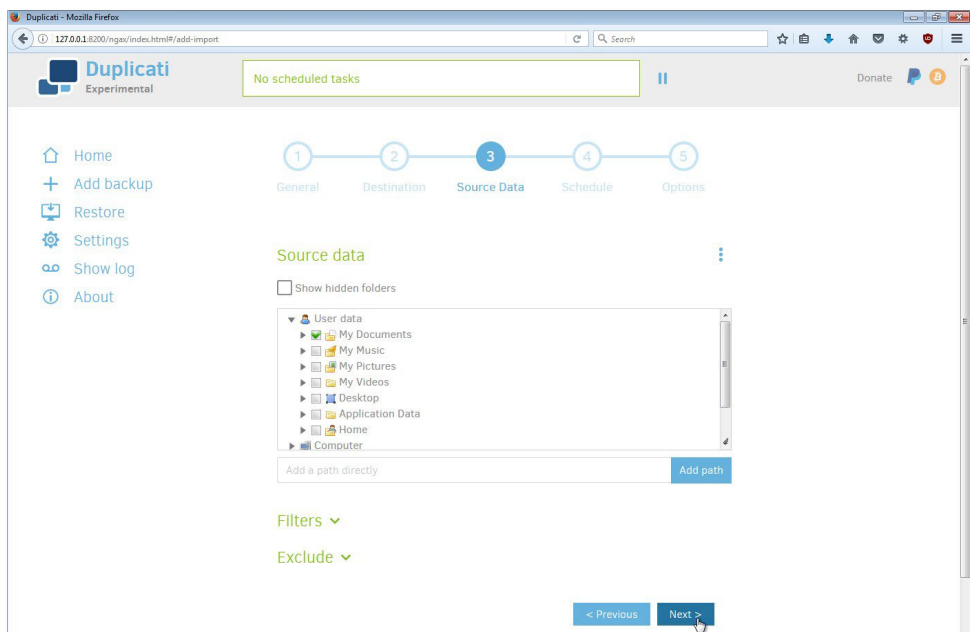
To double-check, click **Test connection** to see whether the connection and login are set up properly before you click **Next**.

² If you receive security warnings from Mono, find help at <https://github.com/duplicati/duplicati/wiki/SSL-TLS-support-in-Mono>.

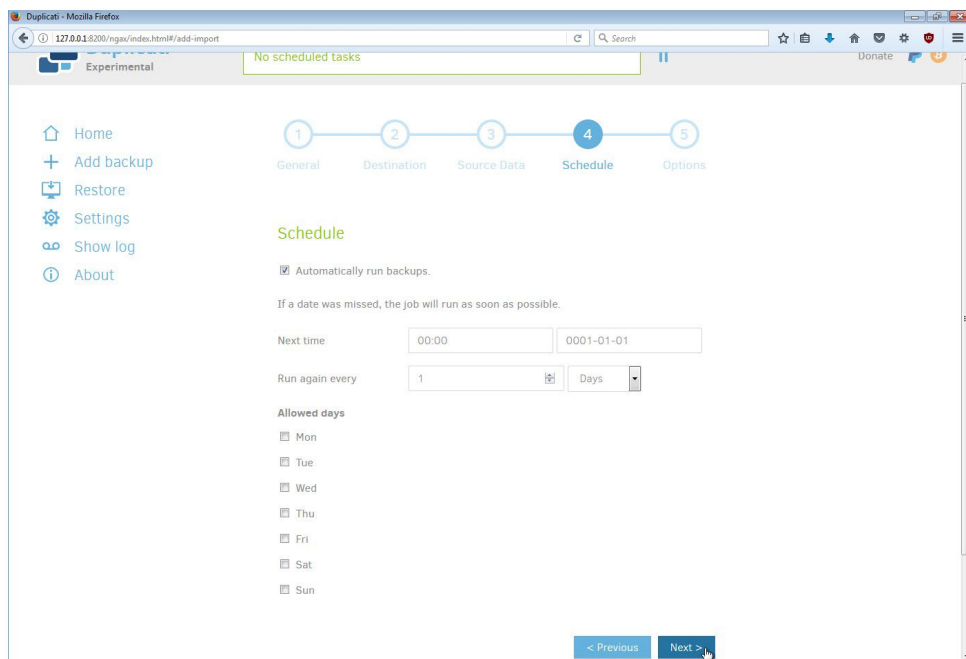


Select the folders you want to include in the backup on ERDA and click **Next**.

Duplicati runs as your ordinary user by default, so it does not automatically have access to all system files and facilities to shadow-copy open files. Therefore, you may get warnings or error messages if, for example, you try to backup folders outside your user area or application data in use. You can either not include such folders in your backup or run Duplicati as a privileged user.



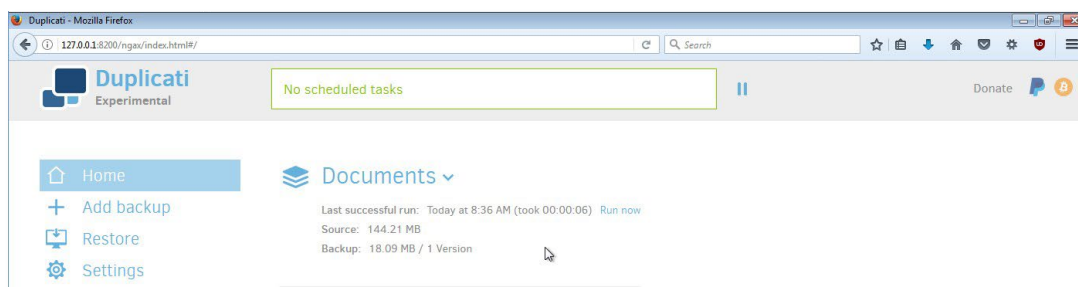
Now you can set the automatic backup frequency and click **Next**. You do not have to select anything under **Allow days**, because not selecting anything has the same effect as selecting all.



If necessary, you can change **Keep backup** to e.g. 3 years or similar. Click **Save**.

If you did not select encryption, you will now be asked whether you are sure. Click either **Continue without encryption** or **Cancel** to go back and set up the encryption.

The backup is now ready to run. Click **Run now**. When it is finished, you will see a status like this:

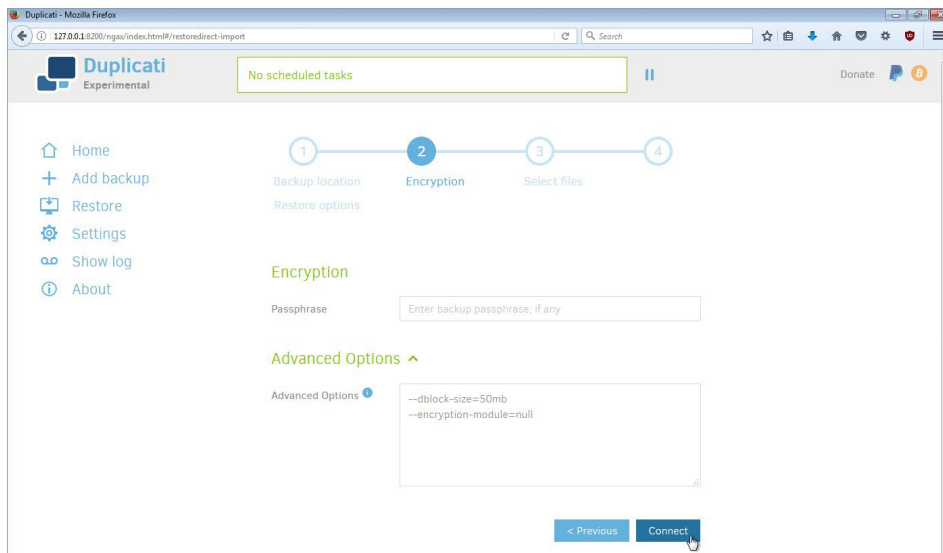


Repeat the process with **Add backup** in Duplicati if you created other .json files.

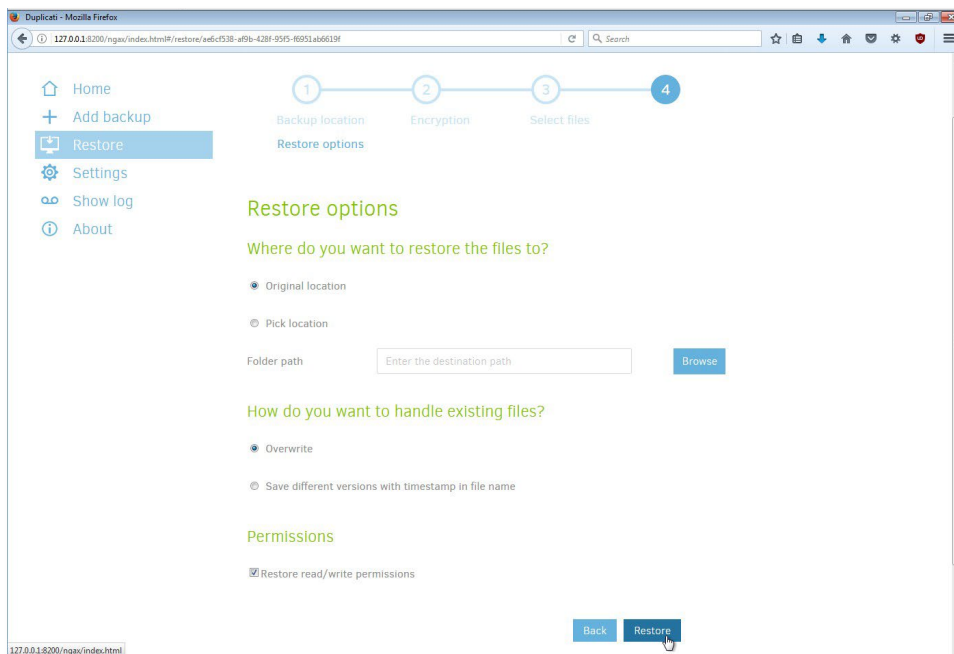
Once the backup is finished, you can restore files and folders with **Restore** from the Duplicati menu or by opening the backup status and selecting **Restore files...** Duplicati will then guide you through the process.

If you lose your PC or get a new one, you will have to download the .json files and import them to restore the Duplicati setup. Select the .json file you downloaded and fill in the form again with the password for the protocol you selected on **ERDA Setup**.

Click **Connect** if you did not encrypt your backup. If you did encrypt it, you must first enter your passphrase and change --encryption-module=null to --encryption-module=aes under **Advanced options**.



Duplicati will now download information about the saved backup from ERDA. Indicate where the local Duplicati setup is to be stored and click **Restore**.



You can now restore data from your backup on ERDA.

Find more guides for Duplicati at <https://www.duplicati.com/articles/Getting-Started/>

Server Backup for ERDA with scripting

Some research groups have their own NAS/server for their data. If you want to back up a NAS/server on ERDA without Duplicati, you have other options for scripting the creation of ERDA backup archives.

The easiest way is through a Workgroup group. Upload a read+write share link and set up a workflow rule for the group which creates a backup archive when you upload a special cursor file.

Select a group (if you do not have one yet, follow our guide under [Workgroups \(VGrids\)](#)). Create a subfolder in one of your folders, e.g. *backup*.

For security reasons, you may want to avoid saving your ERDA password on the PC that runs backup. To do so, you can either use SFTP/SSHFS with an ssh key or create a share link with read **and** write access, as described under [Share Links](#). If you use share links, you can access the folder via WebDAVS/SFTP/FTP access to link sharing, i.e. with the share link ID as your username and code. This restricts access to the subfolder and reduces the risk of misuse.

You can now use a command like *sftp* or *lftp* to upload files from the storage server. You can even upload ERDA as a network drive with, for example *sshfs* and use *rsync* or similar if you only want to upload file changes.

Now we could open ERDA Archives in a web browser and set up a backup archive manually, but most server administrators prefer to integrate this step into the backup process. Set up a workflow rule in your group to integrate the step.

Open ERDA **Settings**. In **Site Collaboration Links**, select *advanced* instead of *default* to get access to workflows. In the Workgroup overview, you can now see a **Workflows** column. Click the *Open* link. Fill in the form with a new workflow rule.

In practice, you create a backup archive of the subfolder every time you upload or store an X.create-backup file in your backup folder.

You can now upload a snapshot of your data to *[mappenavn]/backup/snapshot-[dato]* from the storage server and then upload a file to *[mappenavn]/backup/snapshot-[dato].create-backup*. Now you have automatically created a *snapshot-[dato]* backup archive. You will be able to see it both in your workflows log and on the Archives page.

Alternatively, you can use **Scheduled Tasks** in ERDA to plan when the backup folder is to be backed up. The next section is about Scheduled Tasks.

Scheduled Tasks

ERDA can perform tasks on your behalf using **Scheduled Tasks**. The **Scheduled Tasks** app is not automatically on your front page, so click **Add**, select the app and click **Save**.

With **Scheduled Tasks**, you can plan both regular tasks and tasks that only need to be completed once.

Schedule Tasks

Manage Tasks | View Logs

Manage Scheduled Tasks

You can schedule ERDA commands to run on your behalf at given times. In that way you can automate many of the routine tasks that you would in practice be able to do manually, but which would be tedious and inconvenient to repeat every time. This includes tasks like regular backup or archiving, which typically makes most sense to run e.g. every night or once a week.

Information about any scheduled actions you configure automatically gets logged and you can use View Logs above to inspect them.

Please note that for security reasons you can **ONLY** schedule runs of a limited set of commands, namely a selection of the most useful actions you would be able to interactively run.

The fold-outs at the bottom contain additional help on the available commands and the format in use.

All timestamps implicitly use the site timezone where the date and time is currently 2024-02-06 09:20:54.

Cron Jobs: Repeating Command Schedule

Each line here follows the standard UNIX crontab format with five time fields specifying when to run, followed by the command to run.

```

1  ### Cron Jobs: Regularly Running Tasks
2  # This is a standard crontab specification describing actions to run on your
3  # behalf at given times. Lines starting with a '#' are comments, only used for
4  # explaining things. All other lines represent a scheduled task.
5
6  # Each task to run has to be defined through a single line indicating with
7  # different fields when the task will be run and what command to run for the
8  # task.
9
10 # To define the time you can provide concrete values for minute (m), hour (h),
11 # day of month (dom), month (mon), and day of week (dow) or use '*' in these
12 # fields (for 'any').
13
14 # For example, if you have a Documents folder and want to create a backup of it
15 # at 5 a.m every week, you can do so by adding a rule like:
16 # 0 5 * * * 1 pack Documents Documents-backup.zip
17 # somewhere below this help text. Just leave out the leading '# '.
18 #
19 # m h dom mon dow  command
20

```

At Jobs: One-time Command Schedule

For one-time commands you can use the following field instead. Each line consists of a time stamp in ISO format followed by the command to run at that particular time.

In the example above, we have scheduled ERDA to set up a new backup archive of our *uploads* folder every day at 16:38. We can either manually store in this, or we can use Server Backup for ERDA with scripting to upload data on an ongoing basis. The Createbackup command uses a name with three automatic variables such as *+SHCEDDAY+* to name the archive after the run date.

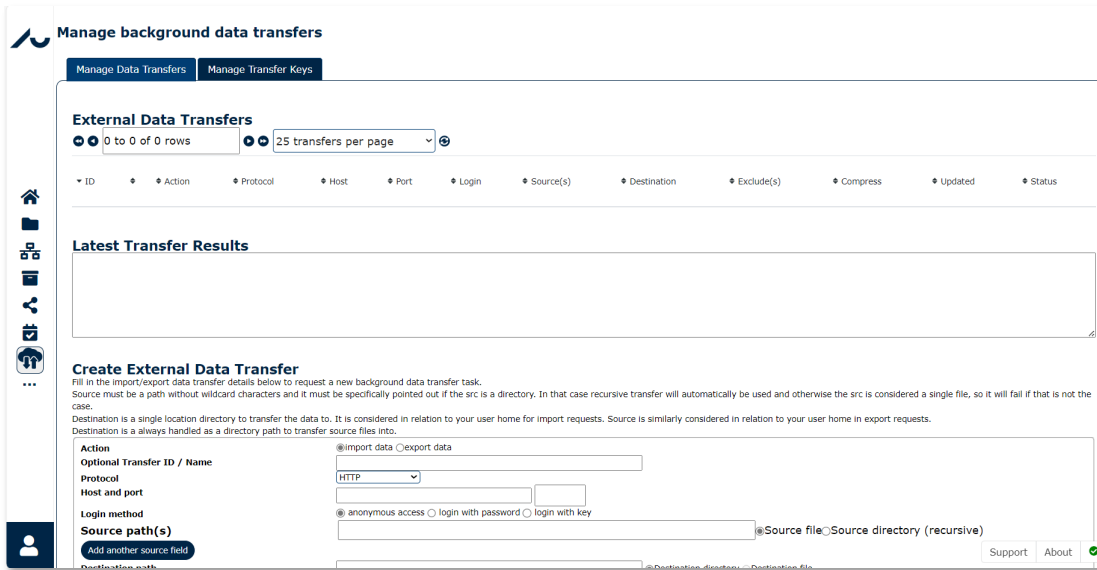
You can follow Scheduled Tasks runs in **View Logs**. In the log from the first run, you will see that the backup archive has automatically been given a name based on the current date. Read more about available variables and commands at the bottom of **Manage Tasks** under **Schedule Tasks**.

Data Transfer

If you use other storage systems or measurement instruments online, it may be useful to be able to import or export data from ERDA efficiently. Users who are used to handling large datasets may need to download such systems and instruments, regardless of whether they are dedicated Linux/UNIX servers or imaging sites such as SLS, ESRF, where you first record data and then have remote access.

ERDA supports the import and export of low-level data in the background via various efficient transfer protocols such as SFTP/RSYNC/HTTPS and WebDAVS.

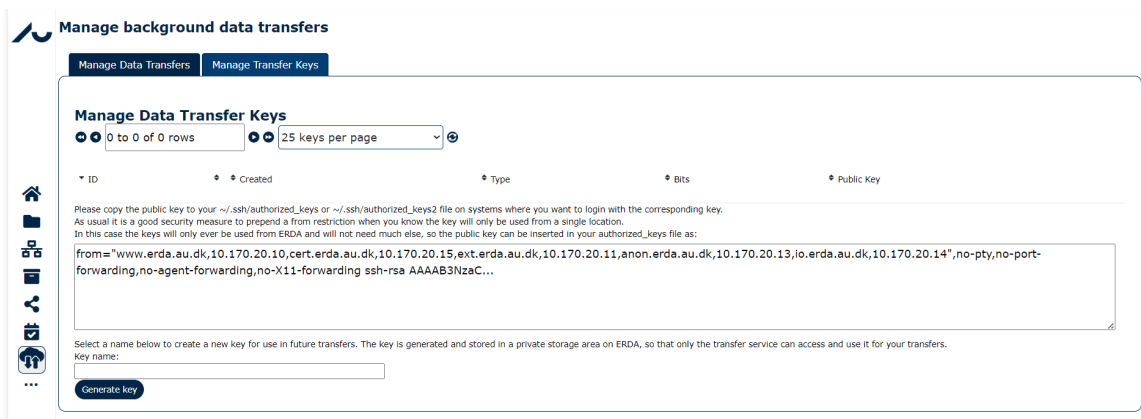
Go to **Home** and click on **Data Transfer** to open the data transfer page.



There are two tabs on the transfer page. Use the first, **Manage Data Transfers**, to set up and monitor transfers, and the second, **Manage Transfer Keys**, to handle transfer keys (you can use digital keys instead of a password to secure remote login). Here we go through how to create an ssh key and use it to import from a server to which you have SFTP access.

If you already have access with login, you do not need to create an ssh key, but you can choose **Login with password** instead of **Login with key** when you set up the transfer.

In the example below, we show how to create a key when you have clicked on **Manage Transfer Keys**. You can decide the name of the key, and this name will only be used to select the key in the transfer.



Enter the name and click on **Generate Key**. Now you can see the public part of the key and brief instructions. In short, you must insert the key where you want to use it to login.

The private part of the ssh key will **only** be stored in an inaccessible location on ERDA, so that no one else has access to the key.

Manage background data transfers

Generated new key with name `my_key` and associated public key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDSHdwMzLIEC+6Voz/+x+IxmoeuAEYedK6YlmesNwt1osqar4T3kymxzXCIFTikmX4yDD/B6qd5beOQCotzIR3lWkkAospi+LUFgIvwCEDhyCZp16kZvroRyze2uS2o6vg
YrwwlWlV0zoz3vOMsyAn+huFqQDkKdHu6oQrNSFK8DcoEhmyPOZayrCOVeX/9r606cjmrgW80qn/7BRe+oKumDsErEd1skFyrMYDjJmAH5bl/JshqGYynshuNqgM7WEM2r/kN2LUUJItNAkF6kXOCuEPm4GH
wLZmeol+SuMy/vlSqL2qoG1e1xpxmAyixdvZKsALwJmcOmzpsgug/1_my_key
```

Please copy it to your `~/.ssh/authorized_keys` or `~/.ssh/authorized_keys2` file on the host(s) where you want to use this key for background transfer login. As usual it is a good security measure to prevent a restriction when you know the key will only be used from a single location. In this case the keys will only ever be used from ERDA and will not need much else, so the public key can be inserted in your `authorized_keys` file as:

```
from="www.erd-test.au.dk,10.170.20.30,cert.erd-test.au.dk,10.170.20.35,ext.erd-test.au.dk,10.170.20.31,anon.erd-test.au.dk,10.170.20.33,jo.erd-test.au.dk,10.170.20.34",no-pty,no-
port-forwarding,no-agent-forwarding,no-X11-forwarding,ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDSHdwMzLIEC+6Voz/+x+IxmoeuAEYedK6YlmesNwt1osqar4T3kymxzXCIFTikmX4yDD/B6qd5beOQCotzIR3lWkkAospi+LUFgIvwCEDhyCZp16kZvroRyze2uS2o6vg
YrwwlWlV0zoz3vOMsyAn+huFqQDkKdHu6oQrNSFK8DcoEhmyPOZayrCOVeX/9r606cjmrgW80qn/7BRe+oKumDsErEd1skFyrMYDjJmAH5bl/JshqGYynshuNqgM7WEM2r/kN2LUUJItNAkF6kXOCuEP
m4GHwLZmeol+SuMy/vlSqL2qoG1e1xpxmAyixdvZKsALwJmcOmzpsgug/1_my_key
```

[Return to data transfers overview](#)

Insert the public key on the PC you want to transfer to or from by following its guide. You can now set up the background transfer to or from your ERDA folder. Configure the transfer to import the content of the `build/circular` folder onto the remote server and store it in the ERDA `dataimports/folder`.

Latest Transfer Results



Create External Data Transfer

Fill in the import/export data transfer details below to request a new background data transfer task. Source must be a path without wildcard characters and it must be specifically pointed out if the src is a directory. In that case recursive transfer will automatically be used and otherwise the src is considered a single file, so it will fail if that is not the case. Destination is a single location directory to transfer the data to. It is considered in relation to your user home for import requests. Source is similarly considered in relation to your user home in export requests. Destination is always handled as a directory path to transfer source files into.

Action	@import data @export data
Optional Transfer ID / Name	test_name_too
Protocol	SFTP
Host and port	marge.escl.nbi.dk 22
Login method	<input type="radio"/> anonymous access <input type="radio"/> login with password <input checked="" type="radio"/> login with key
Username	Sara_Marie
Key	my_key
Source path(s)	build/circular/ <input type="checkbox"/> Source file <input checked="" type="checkbox"/> Source directory (recursive)
Destination path	dataimports/ <input type="checkbox"/> Destination directory <input type="checkbox"/> Destination file
Exclude path(s)	
Enable compression (leave unset except for slow sites)	<input type="checkbox"/>
Optional notify on completion (e.g. email address)	email: SETTINGS
<input type="button" value="Request transfer"/> <input type="button" value="Clear"/>	<input type="button" value="Support"/> <input type="button" value="About"/>

Click *Request Transfer* to queue the transfer. You can follow the transfer in the overview and via the status buttons on the right. You can also follow the transfer in the destination folder by clicking on the **local component** icon.

There are many other ways in which you can combine transfers, and they generally follow the same method.

Click on the **status files** icon for more information if the transfer fails. It can be tricky to locate errors in connection with login and transfers, so contact us if you need help.

Courses and external collaborations

You can use ERDA as support for courses and in collaboration across organisations, both in Denmark and abroad. ERDA's tools make it easy to work with data in depth and to combine theory and practice, so you can present data and increase people's understanding by working directly with the data.

Peers

Research rarely takes place at a single university, and in most Workgroups there is an ongoing need to exchange data between institutions, with companies and across national borders. ERDA is designed to perform this task, so access to the system is not restricted by the outdated mindset that you have to be physically present at AU or use a VPN. Instead, we use a zero-trust security model³ with strictly secured access for all users.

Of course, we cannot let just anyone have access to arbitrary data. Therefore, ERDA separates access at user and Workgroup level. External access requires that an AU employee vouches for the user, and this requires formal approval in agreement with the management. We have formalised this process through **Peers**. Through Peers, you can specify the external users you are going to work with or give them access in connection with courses or workshops.

There are two ways to do this:

1. You can fill in the details of the external users and send them an invitation
2. The external users can sign up and then you can approve the creation of their account

External users must go through a separate login, in which they fill in a registration form, use their email as their username and select a code. If you use method 1., the form is prefilled-in, except for the password, but in method 2. the user has to fill in the form and write the name and AU email address of the employee who is to approve the account.

In the example below, we show how to invite an external colleague to a collaboration.

The screenshot shows the 'Peers' management interface. At the top, there are four tabs: 'Show Peers', 'Requested Peers', 'Enter Peers', and 'Import Peers'. Below the tabs is a text box explaining the form: '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.' Below this is a form with the following fields: 'Label' (input field with placeholder 'Peers name or label'), 'Kind' (dropdown menu with 'Course' selected), and 'Expire' (input field with placeholder 'dd-mm-aaaa'). Below these is an 'Action' dropdown menu with 'Add' selected. Below the action menu is a table with the following columns: 'Full Name', 'Organization', 'Email', 'Country (ISO 3166)', and 'State (if applicable)'. Each row has input fields for these fields, with 'Email' pre-filled as 'Email at organization' and 'Country' and 'State' as dropdown menus.

If you select *Invite on email*, the system automatically sends an email to the user with a link to a prefilled-in registration form. Here they have to choose a code, accept the user rules, and click *Send*. In other words, peers do not need AU ID in order to log in.

NB: *Label* is a name you choose yourself to keep track of your peers. You cannot use spaces or special characters here, but you can use "-" and "_" to separate words.

The administrators will now create the user and send them a welcome email with login details.

³ See more at <https://www.nist.gov/publications/zero-trust-architecture>.

As an employee, you can use **Show Peers** to manage external contacts and send them an invitation, if you did not do so during the registration.

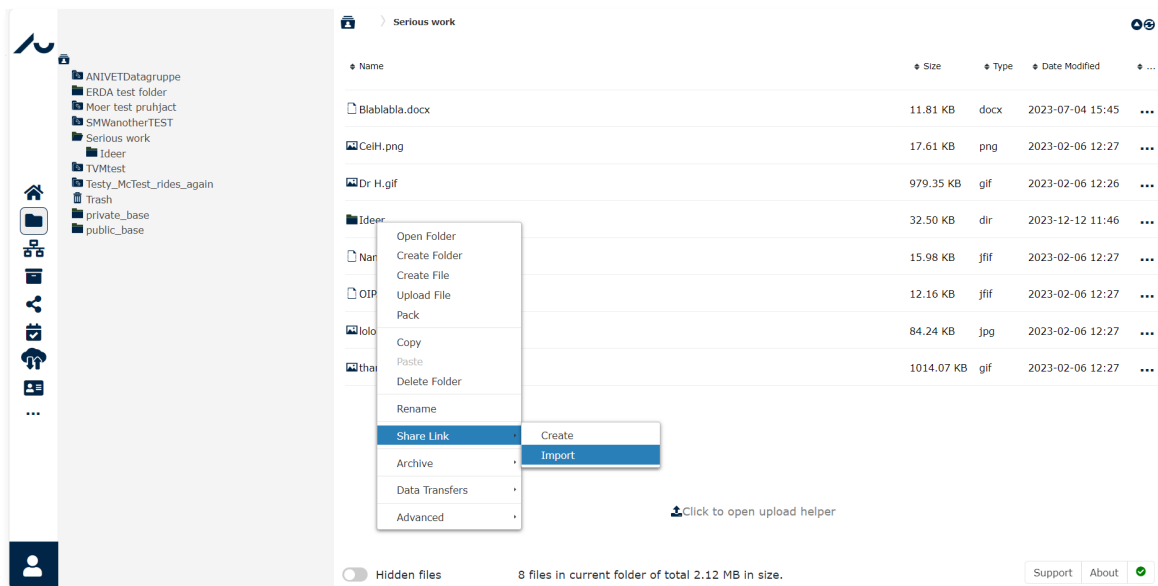
The ERDA administrators use **Expire** to set an expiry date for peer access. Access is always limited to one year at a time to reduce the number of inactive accounts, but it can be renewed without your approval if **Expire** is far enough into the future. When **Expire** expires, you will have to make a new Peer approval or update.

If you want to change **Expire**, you can either do so under **Enter Peers** or **Import Peers**. You have to enter the same ID values again, select **Update** in the **Action** menu and set a new **Expire**.

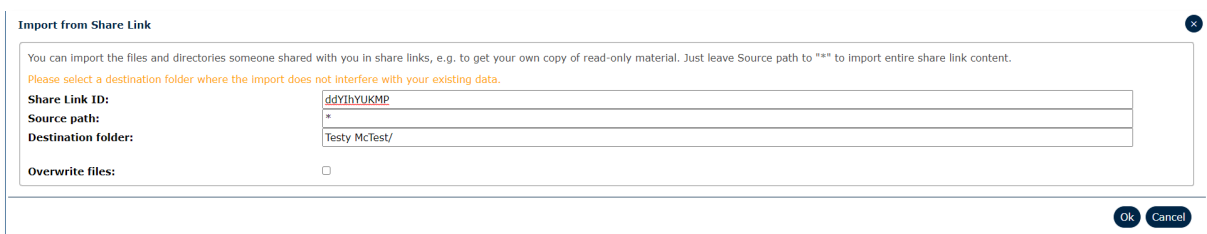
Import share link

In a Workgroup, the easiest way to share data is via shared folders, because then there is *one* copy that everyone can work in.

In teaching situations, participants often need a copy of the material to work with. A common way to produce such material in ERDA is to create a folder with data and a **read-only share link**. Now you can give the participants the link or its ID, so they can download a copy of the data by importing the share link from the right-click menu in their ERDA **Files**.



Enter either the Share Link or the entire URL under **Import**. In our example, we use ID ddYIhYUKMP.



Click **OK** to copy the content of the share link to your folder, so you can use it for exercises etc.

Support, questions and comments

If you have any ideas for how we can make the user experience on ERDA better or if you have any questions about the system, we would very much like to hear from you. This also applies if something does not work as intended or as described in this guide.

It would be a great help if you could include information about your operating system and browser in your inquiry. If you are unsure about the browser and system you use, check by visiting either <https://www.whatismybrowser.com/> or <https://detectmybrowser.com/>. Send us the line under "Your web browser is:" in the top blue field, or the line that begins with "You're using". Screenshots are also very useful when we're trying to help, because then we can see exactly what you see.

Contact us: erda-info.it@au.dk

Yours sincerely, the team behind ERDA AU and AskOS