

User Training Guide

ERDC's Education Data Enclave

Please read this document carefully before you start working in the Education Data Enclave (EDE).
[Save this guide to help you use the EDE in the future.](#)

About the Education Data Enclave	1
Security Guidelines	1
Privacy Statement.....	3
System Requirements	3
Signing In to Your Account.....	4
Applications	13
File System.....	14
Import Requests	15
Export Requests.....	15
Leaving the Education Data Enclave	17
Data Enclave Help Portal.....	18

Have Questions?

Contact NORC Data Enclave Helpdesk

DataEnclaveHelp.norc.org

Mon-Friday: 9am-5pm, Central

About the Education Data Enclave

The ERDC Education Data Enclave (EDE), a subnet of the NORC Data Enclave®, is a secure virtual desktop environment co-managed by the Washington State Education Research & Data Center and NORC at the University of Chicago.

The EDE is an extension of your research workspace. It is configured to provide you with the tools you need to analyze data, collaborate with your team, and prepare output. The EDE offers resources to users on a **virtual desktop**.

Security Guidelines

The EDE is a closed environment which helps prevent accidental disclosure by separating the confidential data from potential sources of disclosure. This means:

- You **cannot** access the internet from within the EDE. The Microsoft Edge and Firefox browsers in the EDE can only be used to submit [Export Requests](#) through the DEER portal and to preview HTML documents.
- You cannot move data, files, or screenshots between your **local desktop** and the **EDE virtual desktop**.

Each EDE user is provided a set of credentials that allows access to the EDE environment. This is your personal passport to the EDE, so you should keep your login information safe and confidential. All EDE users are responsible for maintaining the environment's security by following the EDE User Best Practices in the box below.

EDE User Best Practices

To keep the EDE secure, all users must follow three best practices when accessing and working in the virtual environment:

1. Do **not** share your password, username, or SecurID token with anyone else.
2. Do **not** allow anyone who is not an authorized user to view the EDE virtual desktop. This includes but is not limited to looking over your shoulder while you are logged in or screen sharing through video conferencing software.
3. Do **not** use screen-capture software and devices on your local desktop while you are working in the EDE.

Taking Screenshots for Troubleshooting Purposes

When you run into issues in the DE, you may need to take screenshots of error messages, etc., and share them with the Helpdesk. You must use a screenshot tool **inside** the DE in order to capture these screenshots, as external screen capture software and devices are disallowed. Please follow the below instructions for taking and sharing screenshots of the DE.

1. Inside the DE, open the app "Snipping Tool"
 - a. You can access the Snipping Tool in the Start Menu under "Windows Accessories" or by searching "snipping".



Figure 1: Snipping Tool icon

2. Capture your screenshot using the Snipping Tool. If required, take multiple screenshots to capture the entirety of an error message and the context that led to that error message.
3. Save the screenshot(s) to your H: drive (e.g. H:\Screenshots) with a descriptive filename.
4. Contact the Helpdesk with the filename and its location within your H: drive.

Privacy Statement

ERDC data collection, use, and disclosure is based on legal authority. The ERDC collects, uses, and discloses information responsibly and ethically, avoiding discrimination, deception, or harm.

Federal law (specifically, the Federal Educational Rights and Privacy Act of 1974, also known as "FERPA") safeguards the confidentiality of individual student information. This law requires that educational institutions and state agencies maintain the confidentiality and privacy of personally identifiable information in student records. The U.S. Department of Education has created extensive regulations regarding implementation of FERPA under Title 34, Part 99 of the Code of Federal Regulations.

In some instances, data may also be protected by the Parts B and C of the federal Individuals with Disabilities Education Act, also known as "IDEA". Federal regulations regarding implementation of IDEA can be found in Title 34, Part 300 and Title 34, Part 303 of the Code of Federal Regulations. IDEA incorporates all the provisions of FERPA and adds eight additional requirements to safeguard privacy.

Workforce-related data are also protected and secured by federal law, such as Section 303 of the Social Security Act, for which the U.S. Department of Labor has promulgated Title 20, Part

603 of the Code of Federal Regulations. Furthermore, the federal Workforce Innovation and Opportunity Act of 2014 prohibits the disclosure information collected under the auspices of the workforce development system that would “constitute a clearly unwarranted invasion of personal privacy.

System Requirements

Please carefully read through the below system requirements and ensure that you have all of the required hardware and software for accessing and using the Data Enclave:

- **Computer with Bluetooth** enabled
 - Windows 11 devices are officially supported
 - Other OSs may work but are not officially supported
- Recommended browser: Microsoft Edge
 - Also compatible: Google Chrome, Mozilla Firefox
- **Citrix Workspace**, the Virtual Desktop Infrastructure (VDI) client, must be installed on your computer.
 - Download the latest version for your computer here:
<https://www.citrix.com/downloads/workspaceapp/>
- A compatible **mobile device**
 - Android device, OS version 14 or higher
 - iOS device, OS version 17 or higher
- **Microsoft Authenticator** must be installed on your mobile device
 - Download Microsoft Authenticator app from the Google Play Store (Android) or the App Store (iOS)

If you do not have one of the above devices, or if your OS version does not meet these requirements, please reach out to DataEnclaveHelp@norc.org.

Signing In to Your Account

Introduction to Passkeys

The Data Enclave leverages passkeys for multi-factor authentication (MFA) for signing in to the Data Enclave and affiliated sites. Our passkey MFA may have stricter system requirements than what you may have used for other online services. Please review the system requirements for setting up passkey MFA below.

Set up your Passkey

Before you Begin

Please ensure you have the following information and devices ready before moving on to the next section.

- Your Data Enclave account username
- Your Data Enclave account password
- Computer with Bluetooth enabled and Citrix Workspace installed
- A compatible Android or iOS device with Microsoft Authenticator installed

Sign in to Microsoft My Sign-ins Site

1. Navigate to <https://mysignins.microsoft.com/> in your computer's browser of choice. You should be brought to the below screen:

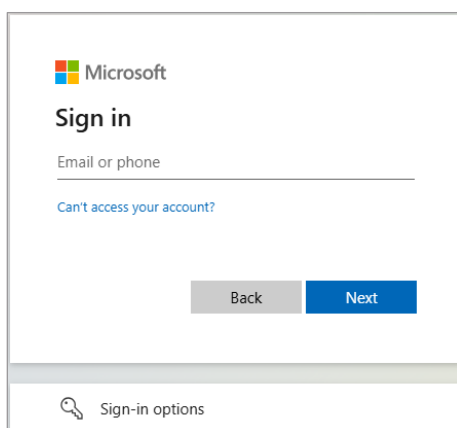


Figure: Microsoft MySign-Ins login screen

2. Enter your username **followed by @de4.norc.org**, then click "Next"
 - a. For example: lastname-firstname@de4.norc.org
3. Enter your password, then click "Sign in"
4. You will now be prompted to set up push-notification MFA in Microsoft Authenticator for this account
 - a. NOTE: If you have already set this up, skip to Step 11
5. You should see a screen that says "Let's keep your account secure"
6. Click "Next" until you reach this screen:

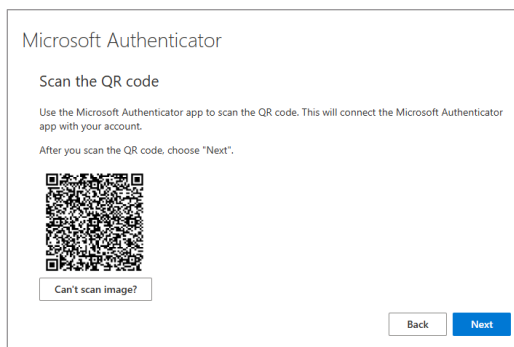


Figure: Screen to scan QR code

7. Open Microsoft Authenticator and scan the QR code using the in-app camera

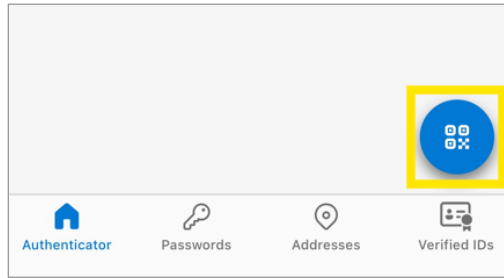


Figure: In-app button used to scan QR code

8. You should be prompted to enter a number into Microsoft Authenticator
9. Once you enter the number in the Microsoft Authenticator app, click "Next" on your computer screen until you reach the below screen:

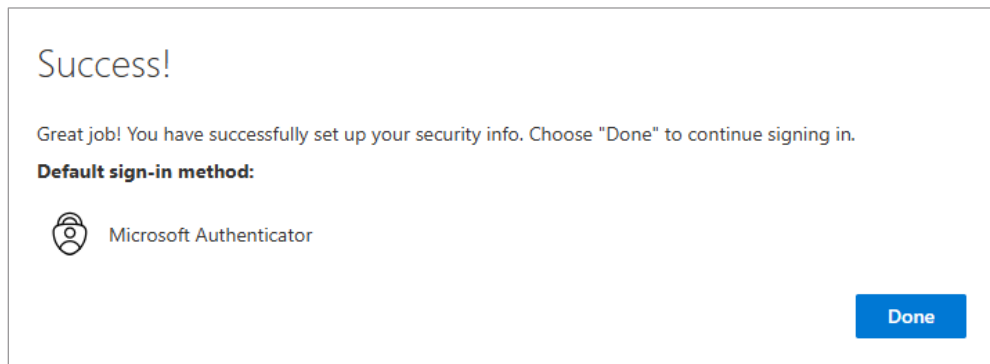


Figure: Confirmation screen your push-notification MFA has been set up successfully

10. Click "Done"
11. You should be brought to the Microsoft My Sign-Ins site. Click "Security info" in the left pane as shown below to view your available sign-in methods

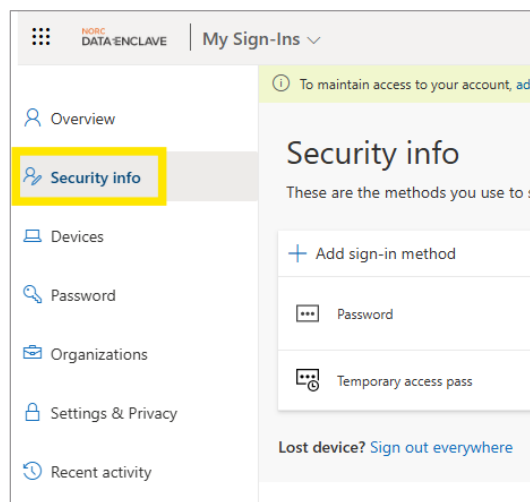


Figure: Microsoft MySign-Ins site Security Info page

12. Once you see the Security info page on your computer screen, proceed to the next section

Set up Passkey via Microsoft Authenticator

1. On the Security info page, click “+ Add sign-in method”, then select “Passkey in Microsoft Authenticator”

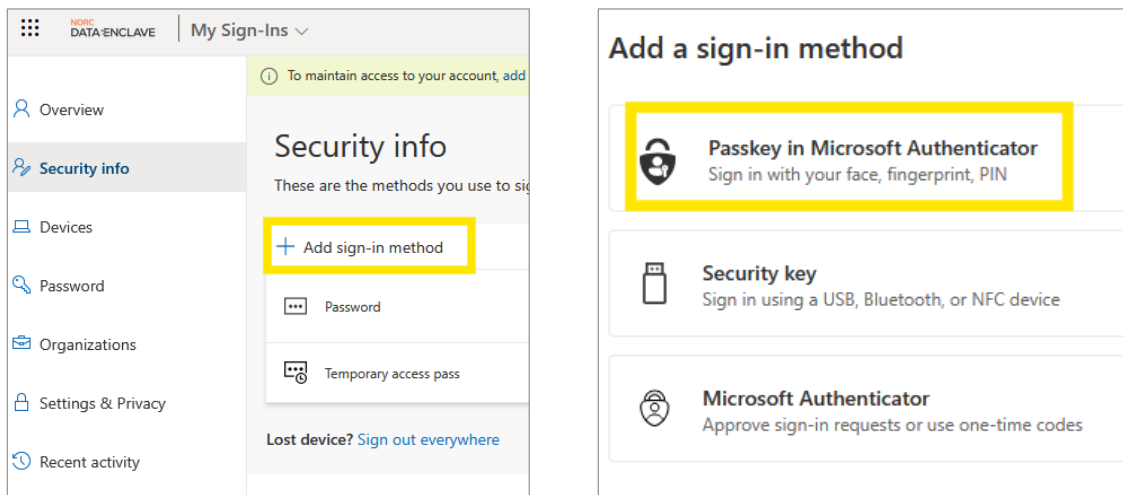


Figure: Options to add a new sign-in method under Security info

2. Click “Next” **once**. You should see the “Complete the setup in Microsoft Authenticator” screen below. Pause at this screen and move to your mobile device. **Do not click ‘Next’ yet**

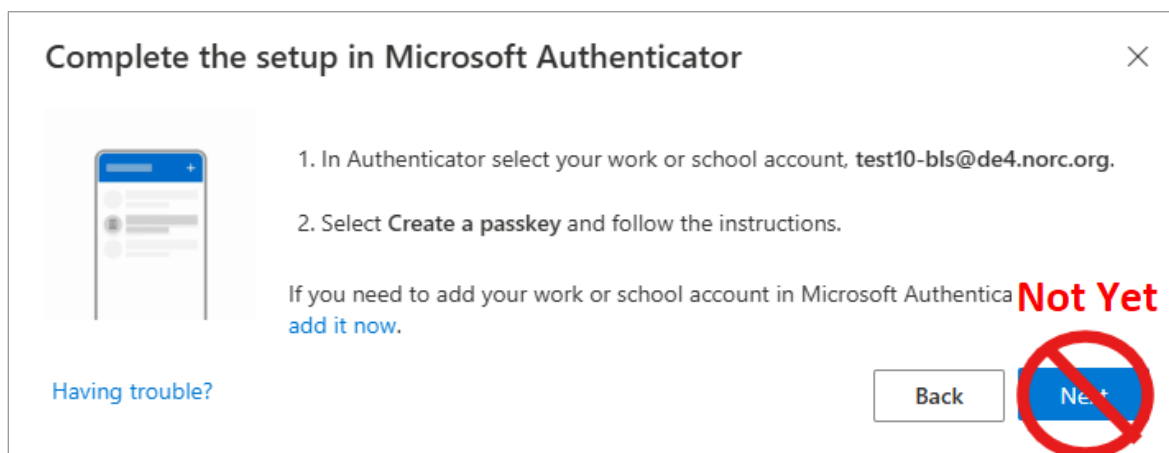


Figure: Screen indicating to complete your passkey setup on your mobile device

3. On your mobile device, open the Microsoft Authenticator app and tap on your account username

4. Under 'Other Ways to Sign In', tap 'Create a passkey'
5. You should be brought to a page that says 'Let's create your passkey'. Select 'Sign in'

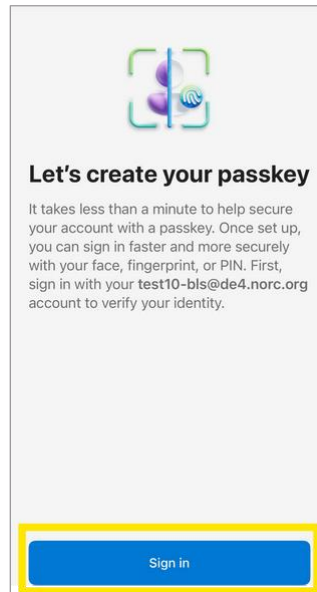


Figure: Screen for signing in to create a passkey for your account

6. Follow all prompts to sign in to your account
 - a. You may be asked to re-enter your password
 - b. You may be asked to confirm your sign in via the push-notification MFA established earlier
 - c. If asked to enter an "email or phone", enter your full username (e.g. lastname-firstname@de4.norc.org)
7. You **may** be prompted to allow Passkeys on your mobile device. Please allow for passkeys for Microsoft Authenticator
8. You **may** be asked to register your device. Select 'Register', then select 'Done'

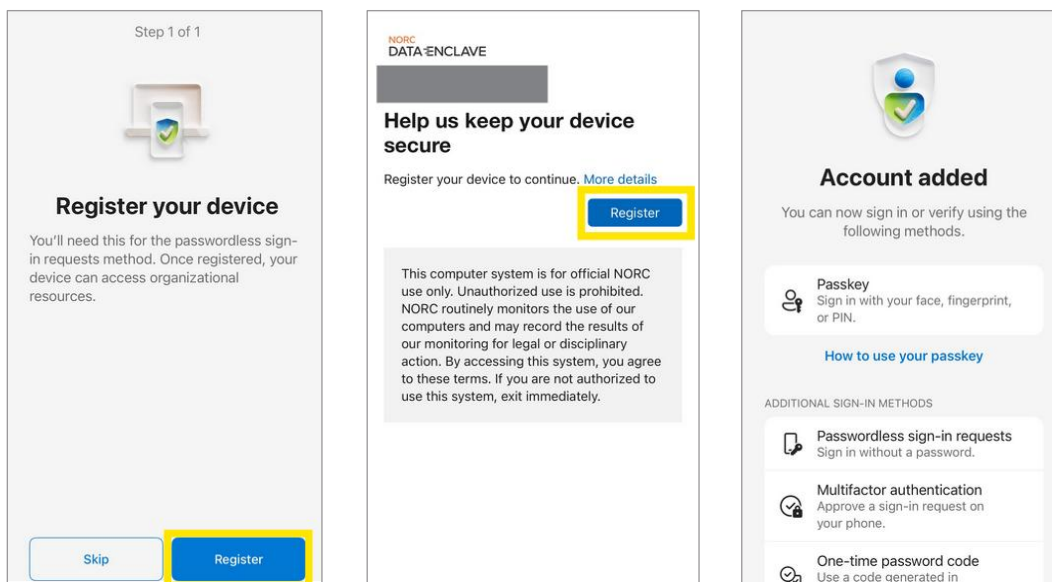


Figure: Screens for registering your phone device if prompted

9. You should see a screen that says “Passkey created”. Tap “Done”
10. You should be returned to the Microsoft Authenticator app home screen
11. Back in your computer’s browser, click “Next”

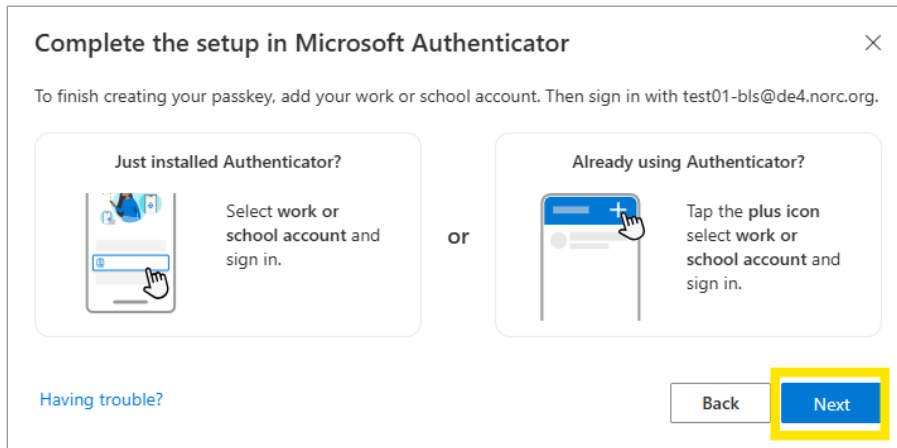


Figure: Screen indicating to complete passkey setup on your phone

12. You should see “Passkey created” on your computer screen. Click “Done”
13. If successful, you should now see a Passkey listed as a sign-in method on your Security info page. Proceed to the next section to test logging in with your passkey

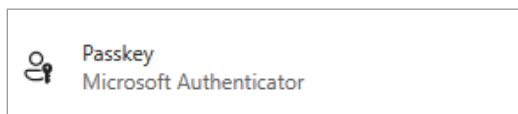


Figure: Confirmation your passkey has been successfully set up through the Microsoft MySign-ins site

Logging in With Your Passkey

1. Go to the Data Enclave login site (DataEnclave.norc.org)
2. Enter your username (with @de4.norc.org) and click “Next”
 - a. Or select your account from the “Pick an account” screen
 - b. You may need to select or enter your username more than once

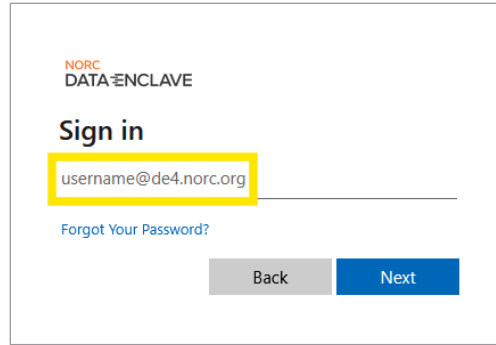


Figure: Enter your username screen

3. You may be prompted for something other than your passkey:
 - a. Click “Other ways to sign in”, then “Face, fingerprint, PIN, or security key”
4. You will be prompted to sign in with your passkey. Select “iPhone, iPad, or Android device”, then “Next”

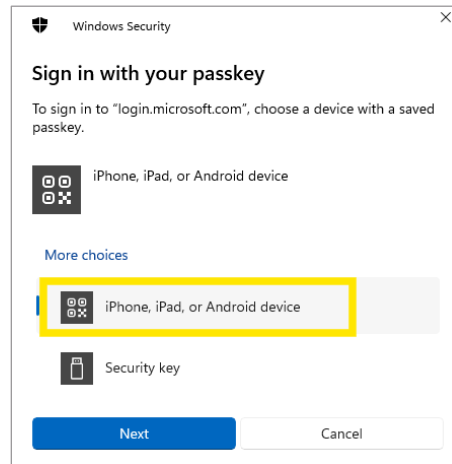


Figure: Screen to select “iPhone, iPad, or Android device”

5. In the Microsoft Authenticator app, tap the blue button in the lower righthand corner (that resembles a simplified QR code) to open the in-app camera

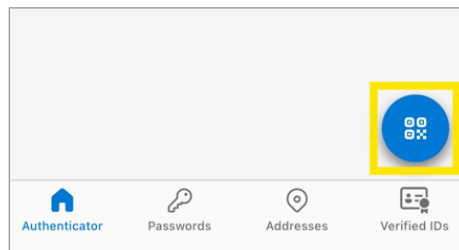


Figure: MS Authenticator - “Blue button resembling a QR code”

6. Scan the QR code on your computer screen using the in-app camera, then follow any on-device prompts as needed to continue

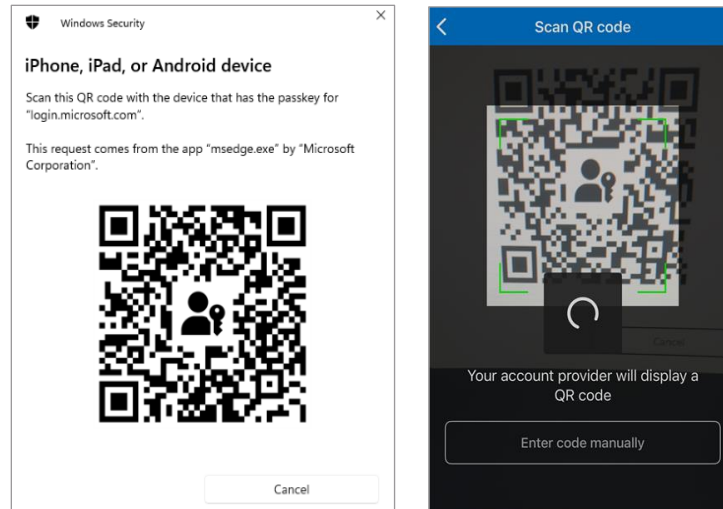


Figure: Scan QR code using the Microsoft Authenticator app

7. If the QR code scan was successful, you should receive the below 'Device connected!' message on your computer screen:

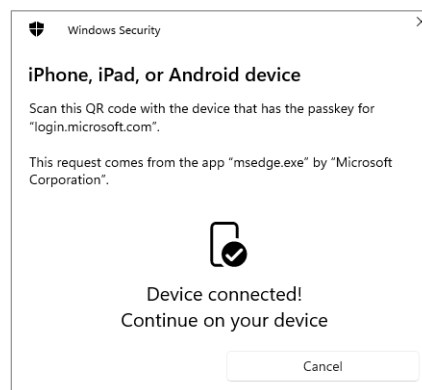


Figure: Confirmation message your passkey was used successfully

8. You may be prompted to "Download" Citrix Workspace, even if you already have it installed. The site should automatically detect Citrix Workspace and move on after a few seconds. If it doesn't, you can click the "Detect again" or "Already installed" links below the "Download" button to proceed.
 - a. Please install Citrix Workspace now if you have not already done so:
<https://www.citrix.com/downloads/workspaceapp/>
9. When you reach this page with the blue "ERDC Desktops" icon, you have successfully logged into your account. Click on "ERDC Desktops" to launch your virtual desktop session.

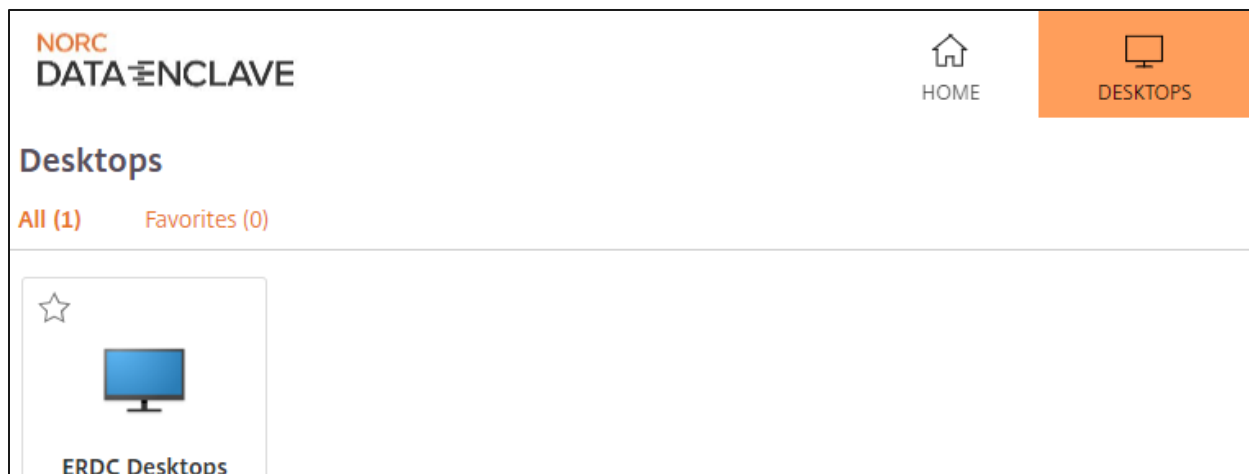


Figure: Click on the ERDC Desktops icon to launch the virtual desktop

When to Ask for Login Help

- **No need to contact the Helpdesk** after *three consecutive* failed login attempts. Your account will be locked and automatically unlocked after **30 minutes**.
- Email the **Helpdesk (DataEnclaveHelp@norc.org)** or **submit a ticket in the Data Enclave Help Portal** if:
 - You are presented with errors using or setting up your passkey.
 - You installed the Citrix Workspace App but fail to launch the EDE virtual desktop.
 - Your credentials are rejected after three consecutive login attempts after your account has been automatically unlocked. You may be using incorrect login information, or your account may be suspended.

Change Your Password

At the top of your EDE virtual desktop, you can see a pull-down toolbar with a downward pointing arrow:



Figure: Pull-down tab

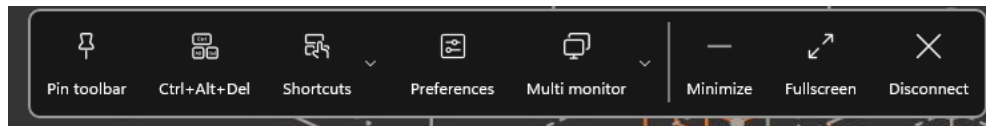


Figure: Pull-down toolbar

In the pull-down toolbar, click the Ctrl+Alt+Del button. Then select the **Change a password** option.

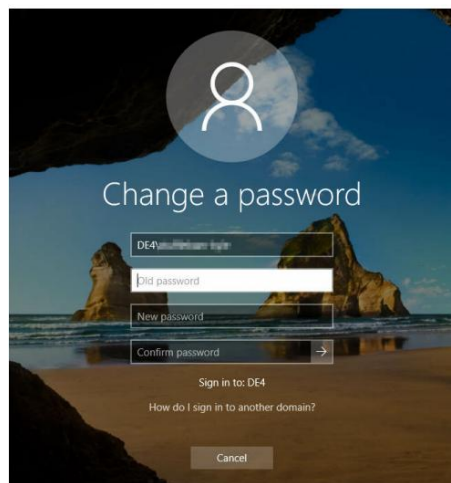


Figure: "Change a password" screen

Password Requirements

8 characters minimum and at least:

- 1 uppercase letter
- 1 lowercase letter
- 1 number
- 1 symbol

Your password cannot include any part of your **username** or a previous password that you have used in the Date Enclave.

Applications

1. Click the Start button to open the Start Menu.
2. By default, applications are organized alphabetically.
3. You can also search for an application by opening the Start Menu, then immediately typing the name of the app you are looking for. Alternatively, you can search by clicking the Search button next to the Start button.
4. To create a shortcut to a frequently used application, right-click the icon for the app, and select "Pin to Start" or "More >" and then "Pin to taskbar"



Figure: Start button (left) and Search button (right)

Statistical Applications

All users have access to Stata, Stat/Transfer, R, RStudio, and Python (Jupyter Notebook, Spyder). **Data Enclave’s internal repository contains most common packages, including a routinely updated Comprehensive R Archive Network (CRAN) mirror.** NORC reviews applications and the package repository for updates on a regular schedule.

Table: Statistical Applications in the DE

Application	Description	How to install packages
STATA	General purpose statistical software application	Enter the 'net' command and click more to reveal all directories Additional Stata resources can be found in K:\Datasets\Common\02 Stata Resources
STAT/Transfer	Utility program that converts datasets from one format to another (for example, SPSS to Stata, or SAS to Excel)	N/A
R	Programming language for statistical computing and graphics supported by the R Foundation for Statistical Computing.	Select "Package" in the toolbar, then "Install packages(s)". Additional R resources can be found in K:\Datasets\Common\03 R Resources
Rstudio	Integrated development environment (IDE) for R	Select "Packages" on the right-hand side, then click the "Install" button. Search for the package name in the pop-up "Install Packages" window, then click "Install"

Jupyter Lab and Jupyter Notebook	Jupyter supports execution of Python code in 'notebooks', which can help with creating clear and understandable steps in code	Open "Python Command Prompt" and enter 'pip install name of package'. Be sure to also include 'import package' statements to your code as needed
Spyder	Open-source, cross-platform IDE for scientific programming in the Python language	Open "Python Command Prompt" and enter 'pip install name of package'. Be sure to also include 'import package' statements to your code as needed.

File System

You have access to two network drives in **File Explorer**: 

- **DOCUMENTS (H:\ drive):** Your personal workspace with 50 GB of available storage.
- **ERDC_RESEARCH (K:\ drive):** Shared data drive.
 - **K:\Datasets:** Data storage area.
 - **K:\Datasets\Common:** Reserved for read-only updates and announcements available to all researchers.
 - **K:\Datasets\<project folder name>:** Reserved for customized datasets for your project. All researchers on your project share *read* access to this project datasets folder that contains the ERDC-provided read-only data files.
 - **K:\Research:** Research project folder.
 - **K:\Research\<project folder name>:** All researchers on your project share *write* access to this project research folder to collaborate on work products.
 - **K:\Home:** Links to your H:\ drive.

Import Requests

To initiate an **Import Request**:

1. Fill out all required fields on the **Import Request form**:

<https://accellion.norc.org/form/import-request>

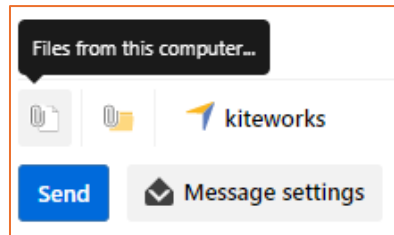
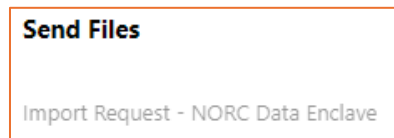
- Sign into Accellion kiteworks with your EDE **username** and **password**.

2. Attach Files from your computer. Before the upload:

- **Importing multiple files:** Group the files into as few zipped files as possible.
- **Encryption:** If your file(s) contains sensitive or confidential information (e.g., Personally Identifiable Information), the files must be encrypted.

3. Click **Send**.

- **NOTE:** Do not change any Message settings.



NORC will email you when your file has been imported into the EDE.

Export Requests

The **Data Enclave External Review (DEER)** portal within the EDE enables researchers to save outputs for statistical disclosure control review and release. The Export Process must be used to export data and documents from the Enclave to your local computer. The ERDC will review for FERPA compliance (including cell sizes) and then approve or deny the export request. This process may also involve the ERDC sending your draft materials to data contributors for their review and feedback. If you are exporting a report or other deliverable (e.g., research reports, scholarly journal publications, presentations, and/or data dashboards), then you must submit all draft materials that use the data requested in this form to ERDC for review before any materials are shared with anyone not listed in the data-use agreement and before any materials are published.

The screenshot shows a web interface for 'Export Request History'. On the left is a 'Filters' sidebar with a 'Request Status' section containing checkboxes and counts for Open (1), Pending (4), External Client Review (0), Approved (2), Rejected (0), Completed - Approved (0), and Completed - Rejected (0). The main area has a search bar and a table with columns for Date, File, and Status. A '+ NEW EXPORT REQUEST' button is in the top right.

Date	File	Status
11/22/24, 12:09 PM	Test Export Submission.xlsx	Pending
11/21/24, 2:37 PM	Test Export Submission.xlsx	Approved
11/20/24, 9:21 PM	Test Export Submission.xlsx	Open
11/20/24, 9:18 PM	Test Export Submission.xlsx	Pending
11/20/24, 9:13 PM	Test Export Submission.xlsx	Pending

Figure: EDE desktop – DEER portal’s “Export Request History” screen

1. To access DEER, launch **Microsoft Edge in the EDE**. You can also access DEER in **Firefox in the EDE** by typing in this URL: <https://deer.de4.norc.org/norc-deer>.
2. Upload the file that you would like to export out of the EDE. If you have more than multiple, please zip them using **7-Zip File Manager available in the applications section**.
3. To help expedite the review process, please include details about the file:
 - A brief description of the output (e.g., simple regression, box-and-whiskers plot)
 - Whether this is a new request or one that builds on a prior request
 - A list of the key variables
 - Whether or not the variables are continuous
4. Click **Submit**. Your request will be added to the review queue.
5. NORC will notify the **ERDC reviewer** to conduct disclosure review.
 - If the file is **approved**, NORC will send you an email with an *Accellion kiteworks link* so that you can download your file outside of the EDE.
 - If the file is **rejected**, NORC will prompt you to check the reviewer's comments in DEER. Once the appropriate edits are made, you can submit a new request.

Export Request Best Practices

All users should follow these best practices when preparing an export request:

1. ERDC does **not** typically approve requests to export record-level data from the enclave to your local computer. If you expect to request an export of record-level data, then please notify the ERDC before you submit your export request.
2. Due to FERPA compliance requirements, unredacted aggregate data (i.e., data with cell values less than 10) will **not** be approved for export from the enclave to your local computer.
3. Word documents, Excel spreadsheets, text files, and statistical software files can be exported through the DEER portal. Make sure to describe the files that you want to export, as outlined in Step 3 above.

For more information on the disclosure review process and how to prepare analytic output for review, see K:\Datasets\Common\01 Security and Confidentiality Training

Leaving the Education Data Enclave

Save your work (including outputs, programs, or other documents) and **Sign Out** after each EDE session. Any unsaved files may be lost if not properly saved. It is also good practice to save in progress work routinely during a session.

Sign Out

- Open the Start Menu. Click on your profile icon on the left side, then click “Sign out”.

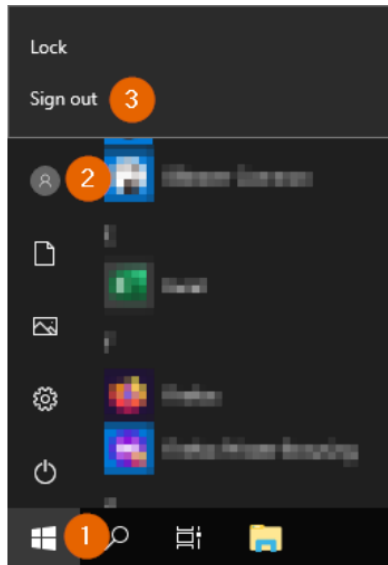


Figure: Click the buttons in the order shown to “Sign out”

System Maintenance

System maintenance that impacts user access to EDE desktops and applications will take place on the **first Monday of each month** from **1 am to 4 am (Central Time)**.

- What to expect:** During this time, all existing user sessions will be terminated.
- What to do:** Please make sure to save your files and **Sign Out** before the maintenance window.

Disconnect

- If you need to run a program overnight, you can use the **Disconnect** option in the pull-down toolbar rather than signing out at the end of the session.
- NOTE:** If your session is inactive for 72 hours, it will be terminated.
- Make sure to log back on so that it remains active. Make sure to save your outputs so they are not lost due to a terminated session.

Data Enclave Help Portal

This self-service portal will be available to all Data Enclave users to request support from the Data Enclave Helpdesk, check on status of support requests, and update any existing support tickets. You will now receive updates on your tickets as emails directly from our ticketing system.

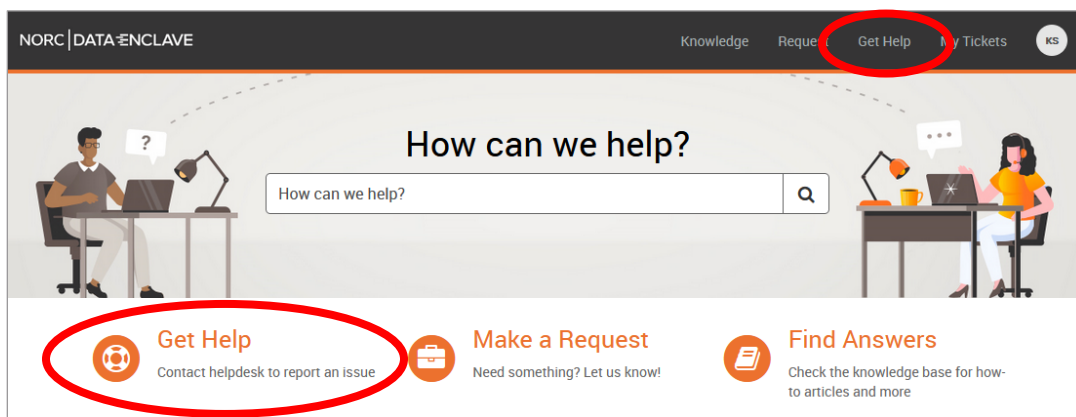
You can access the Data Enclave Help Portal by using this link: DataEnclaveHelp.norc.org. Please login to the Data Enclave Help Portal using the same login method as for the Data Enclave itself (login via passkey).

If you run into any issues setting up a passkey for your Help Portal access, or run into any access issues in general, please reach out to DataEnclaveHelp@norc.org for assistance.

Getting help when something goes wrong

To report an issue:

Select "Get Help" from the homepage, or from the ribbon at the top-right of the window



Complete the form to report an issue. Please ensure you provide all relevant information, including:

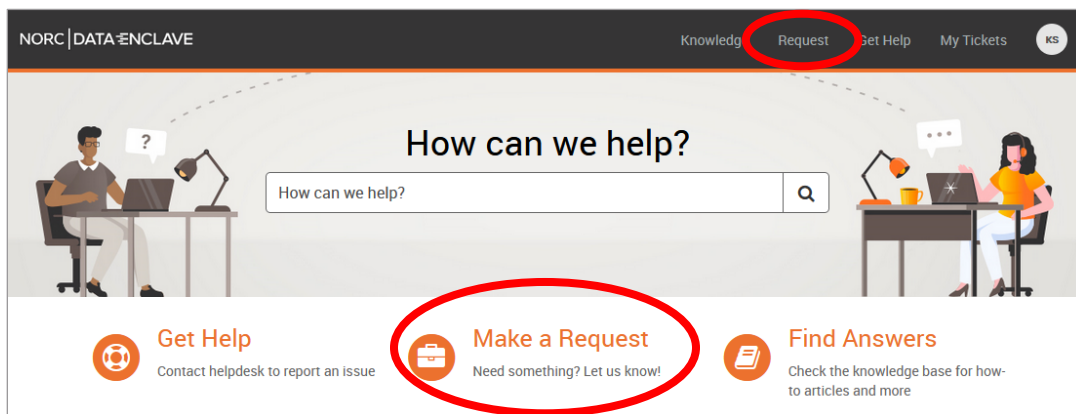
- Your Data Enclave username
- The name of the application or process where the issue exists
- A screenshot or description of any error messages received

Making Requests

Data Enclave users can make requests, including access to data, new software, or file imports, etc.

To make a request:

Select "Make a Request" from the homepage, or "Request" from the ribbon at the top-right of the window.



Complete the form to create a request. Please include all relevant information, including:

- Your Data Enclave username
- The name of your project or team
- A summary of your request
- Any other relevant details for your request

Accessing Your Tickets

In the Data Enclave Help Portal, users can view open tickets and ticket history.

To see your tickets, select "My Tickets" from the homepage.

