

Configuring your authentication access for Diamond based applications

Step-by-step guidance for new users, including Multi-Factor Authentication (MFA) setup and changing your MFA token

Introduction

Diamond has changed the way we authenticate staff and facility users when they access systems at services at Diamond. This includes systems such as the user administration system (UAS), ISPyB and the Diamond publications database.

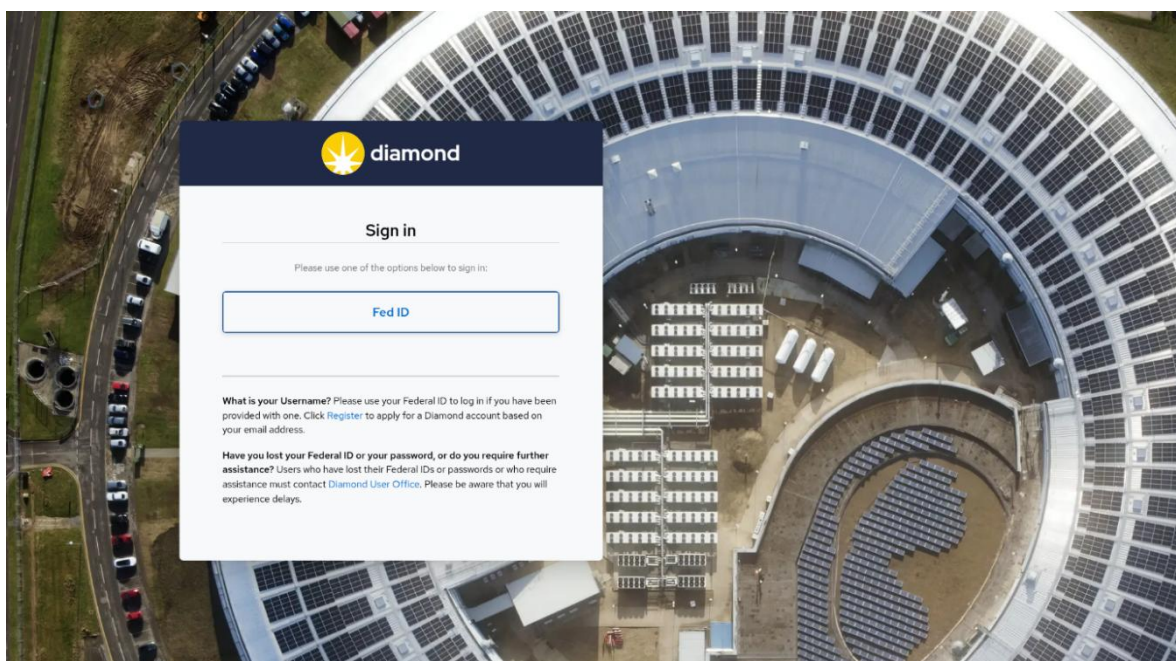
This guide provides instructions for the new authentication system (Keycloak). It provides first-time users step by step guidance on how to sign in and secure their account with Multi-Factor Authentication (MFA) using an Authenticator App. You'll also find steps for changing your MFA token (the device you use to produce a MFA generated code, for example your phone) in the future.

Before You Begin

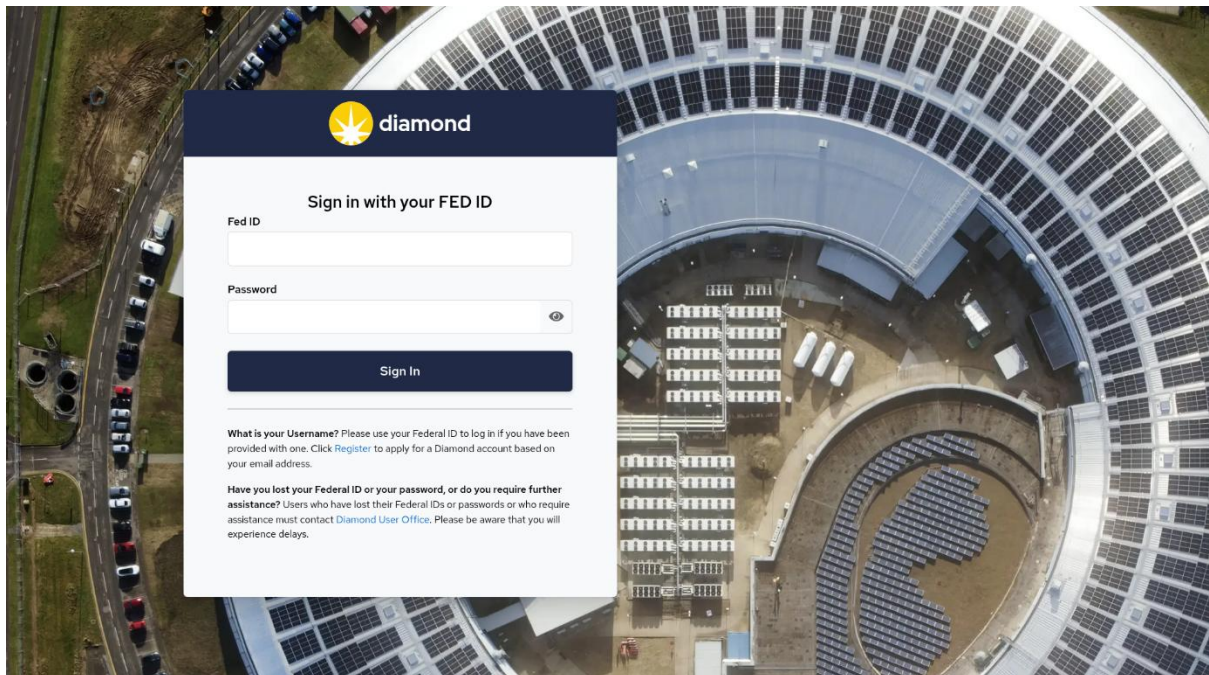
- Have your mobile device ready with an Authenticator App installed (e.g., Google Authenticator, Microsoft Authenticator, or similar).
- Ensure you have your username and password for Diamond's Systems (UAS or Synchweb, for example).

Part 1: First-Time Sign-In to the Keycloak

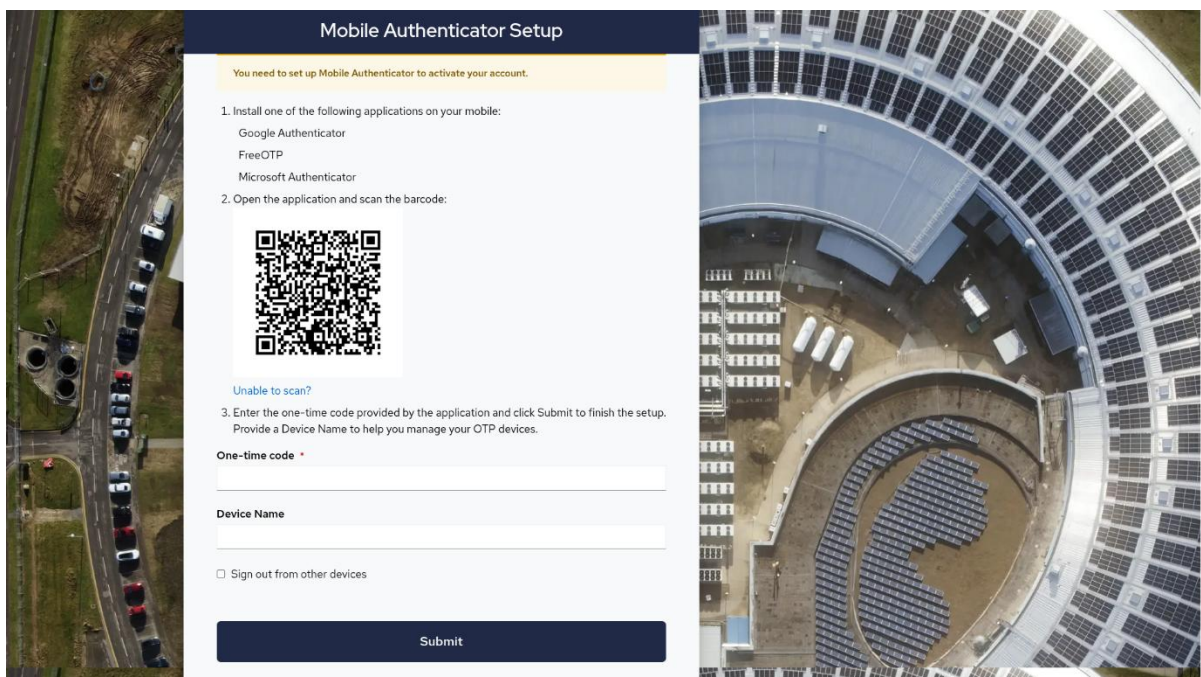
1. Enter the URL for the application you are trying to access.
2. You will be prompted to sign in with your FedID.



3. When you click FedID you will be prompted for your credentials.
4. Type in your username and password, then click 'Sign in'.
5. Begin MFA Setup

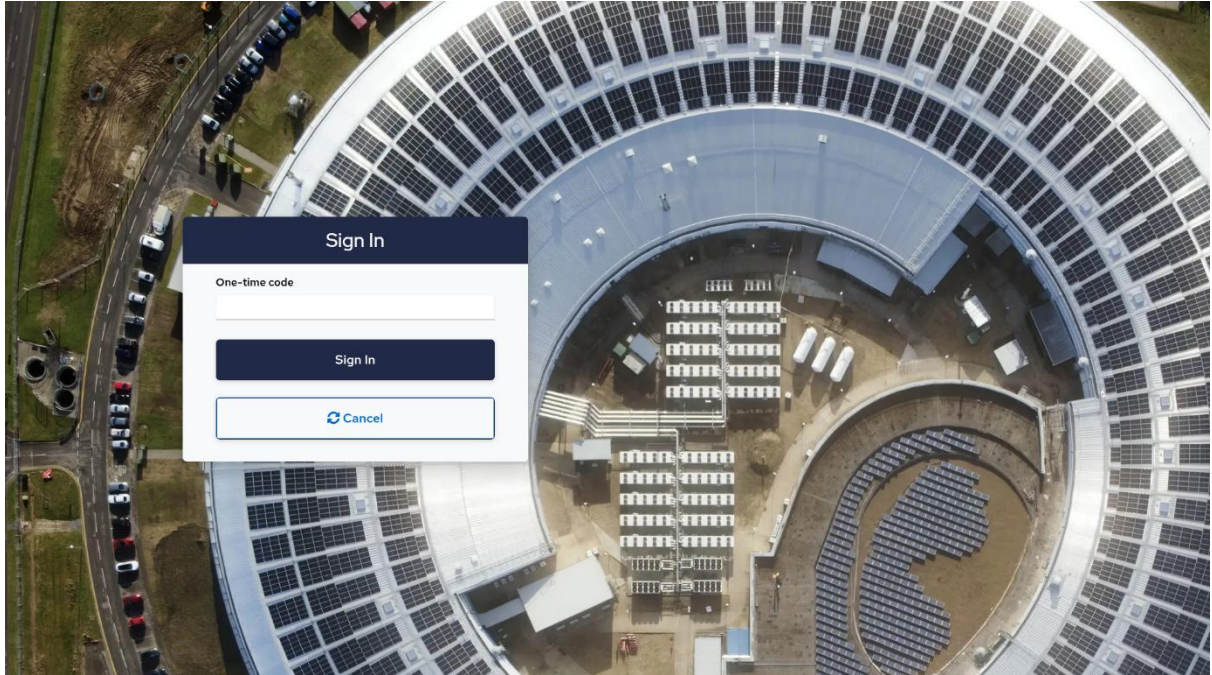


6. Upon first sign-in, you'll be prompted to set up Multi-Factor Authentication.



7. Open your Authenticator App on your mobile device and use it to scan the QR code displayed on the screen.
8. If you cannot scan the QR code, click on the "Unable to scan?" link to get a manual code you can enter in your app.
9. Enter a Device Name for your future reference

10. Once the Authenticator App generates a code, enter it into the field on the keycloak setup page and click 'Submit'.
11. If the code is accepted, your MFA setup is complete. You will be redirected to the application you are trying to access.
12. Future sign-ins on Diamond systems will be through this system and you will be prompted for a one time passcode

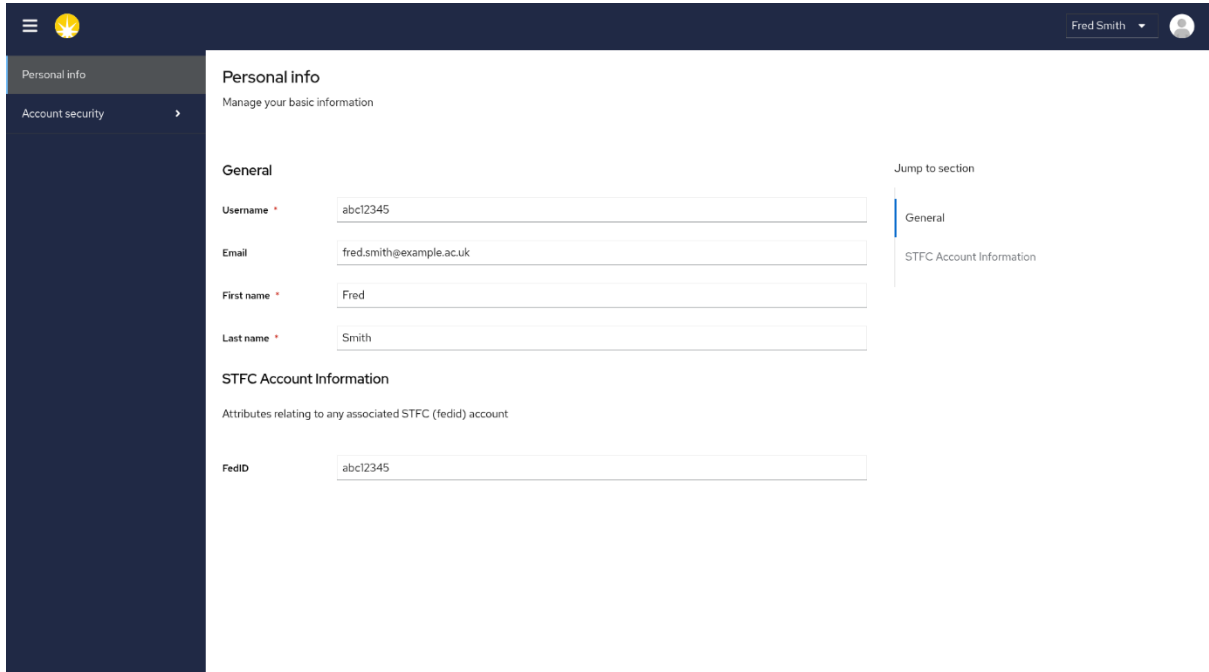


Instructions for changing your MFA Token are available on the following pages.

Part 2: Changing Your MFA Token

If you need to change your MFA token (e.g. you have a new phone), follow these steps:

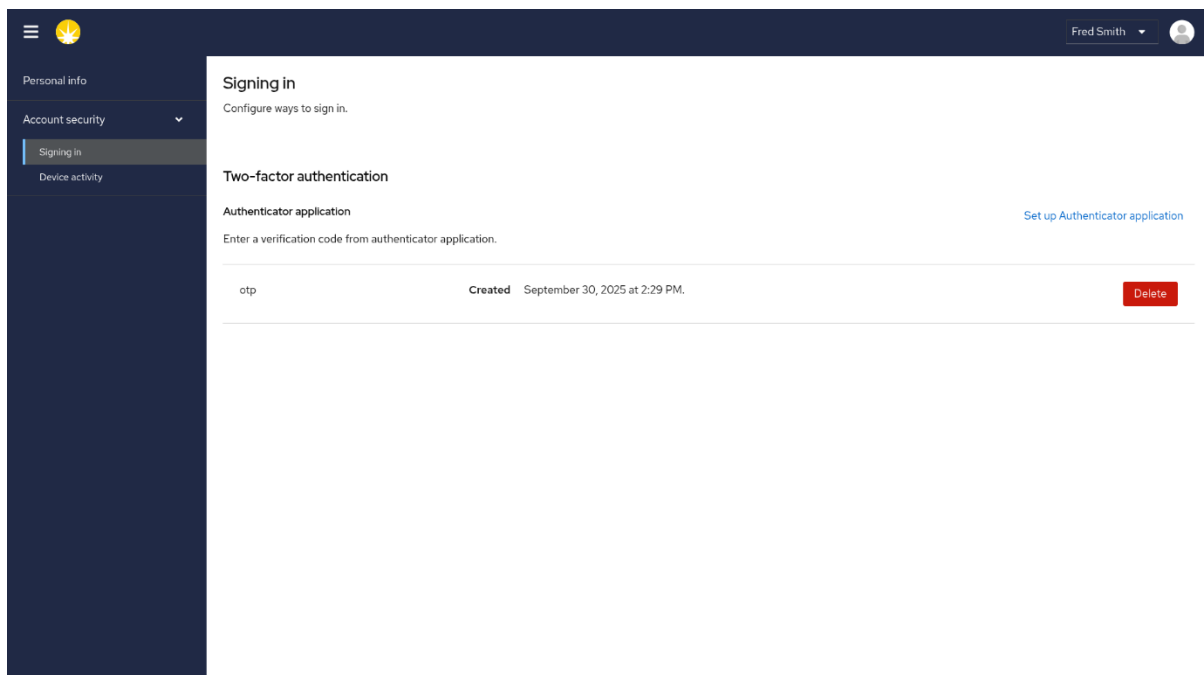
1. Log onto the [authenticator home page](https://identity.diamond.ac.uk/realms/dls/account) (<https://identity.diamond.ac.uk/realms/dls/account>) and sign in with your



The screenshot shows the 'Personal info' page. The left sidebar has 'Personal info' selected. The main content area is titled 'Personal info' and 'Manage your basic information'. It contains two sections: 'General' and 'STFC Account Information'. The 'General' section has input fields for Username (abc12345), Email (fred.smith@example.ac.uk), First name (Fred), and Last name (Smith). The 'STFC Account Information' section has a FedID field (abc12345). A 'Jump to section' sidebar on the right lists 'General' and 'STFC Account Information'.

username, password, and current MFA code.

2. Navigate to 'Account Security'
3. Remove Your Old MFA Device
4. Select the option to remove or reset your current MFA device or token. Confirm the action if prompted.



The screenshot shows the 'Signing in' page. The left sidebar has 'Account security' selected, and 'Signing in' is highlighted. The main content area is titled 'Signing in' and 'Configure ways to sign in.'. It contains a 'Two-factor authentication' section with an 'Authenticator application' table. The table has one entry: 'otp', 'Created September 30, 2025 at 2:29 PM.', and a 'Delete' button. A 'Set up Authenticator application' link is also visible.

5. Set Up a New MFA Device

6. Follow the same setup instructions as in Part 1 to register your new Authenticator App.

Support and Further Assistance

If you encounter any issues during sign-in or MFA setup, please contact the User Office (useroffice@diamond.ac.uk) or, for Diamond Staff, Diamond's Scientific Computing Helpdesk (schelpdesk@diamond.ac.uk) for help and support resources.

Notes

- Remember to keep your mobile device secure, as it is now required for logging in.
- Do not share your MFA codes with anyone.
- Contact the User Office team (useroffice@diamond.ac.uk) if you lose access to your authenticator app or device.