2024-03-19

Multi-factor Authentication (MFA)

Multi-factor authentication, also known as two-step verification, means that as an extra security, you use two different verification steps for access to certain services, such as SharePoint, email, Teams, etc. After step one of specifying your username and password, you must give additional approval in the next step. This second step is done through your mobile phone and the Microsoft Authenticator app.

Why is MFA required?

MFA is a requirement from the Swedish Civil Contingencies Agency (MSB) according to the (2020:07) regulation.

MFA allows students to prove that they are who they claim to be. As you must actively approve your login as a next step you efficiently prevent unauthorised log-ins. If an unauthorised person manages to get hold of your account details, they cannot access your MDU account/service/application as you must perform step two of the login procedure yourself.

As a student with an MDU email address, you are included in this requirement and will automatically be activated for MFA, then you have 14 days during which you can register for MFA.

To register for MFA, students need an iPhone with support for iOS 15.0 or later or an Android with an operating system 8.0 or later. The Microsoft Authenticator app is available for Android and iOS. Make sure that you keep yourself up to date with the latest version of Android or iOS for the best authentication experience.

Please note that there are other apps with a similar name and icon, so make sure that you install the Microsoft Authenticator from Microsoft Corporation.

Activate MFA for the first time

Start by installing the Microsoft Authenticator app on your mobile phone. You can find the app in Play Store/App Store.

Please note that only Microsoft Authenticator is approved by MDU to be used as an authentication app. Make sure when installing the app that it is the correct one.

- Start Microsoft Authenticator and approve the terms and conditions.
- Start by selecting **Add an account**.
- Select **Work or School account**.

- Click on **Scan the QR code** and allow access to the camera as well as allowing notifications and alerts from the app.

Then go to the Microsoft page for managing the MFA app, preferably from a computer: https://mysignins.microsoft.com/security-info

- Click on **Next** in the following boxes until a page with a QR code appears.
- Now use your phone to scan the QR code through the Microsoft Authenticator app.
- Then click on **Next**.
- You will now be asked to verify this, match the numbers from the screen and enter the numbers into the app.
- Click on **Next** and now you have successfully added the two-step verification. You can now close the window.

Approve the login

Important Never authorise a login you are not expecting. If you are unsure, it's better to deny a login.

When you log in with your MDU account, as a next step you will need to approve the login in the Microsoft Authenticator on your mobile device.

- Log in to your MDU account on a computer or mobile device.
- A confirmation prompt will appear.
- In that prompt, there will be a number, which you must enter into Microsoft Authenticator on your mobile device that you registered your MFA on.
- You can also take the opportunity to check the box labelled **Don't ask again for 14 days**. Then the login on the specific device you are using will be valid for 14 days.
- Once you have entered the number into Microsoft Authenticator, press **Yes**.

Add a new device to an existing MFA

For example, start the Google Chrome browser on your computer.

- In the address field you must enter https://mysignins.microsoft.com/security-info
- Log in with your MDU email address and password, approve the login in Microsoft Authenticator on the mobile device that you have already configured the MFA on.
- Click on **Security information** in the left field, then on **Add a sign-in method.**
- Select the **Authentication app** and then click on **Add.**
- Find the device you want to add to MFA and install the Microsoft Authenticator app from the device's app store. Start Microsoft Authenticator and approve the terms and conditions.

Please note that only Microsoft Authenticator is approved by MDU to be used as an authentication app. Make sure when installing the app that it is the correct one.

- Start the Microsoft Authenticator app on your mobile device.

- On your mobile device, select **Scan a QR code**.
- On your mobile device, authorise the access request to the camera.
- On the computer, click on **Next** when asked to download Microsoft Authenticator.
- On the computer, click on **Next** when asked to configure your account.
- Aim your mobile device camera towards your computer screen and scan the QR code.
- On the computer, click on **Next** when you have scanned the QR code.
- On your mobile device, enter the number that is shown on your computer.
- Click on **Yes.**

Remove a device in MFA

For instance, start the Google Chrome browser on your computer.

- In the address field write https://mysignins.microsoft.com/security-info
- Log in with your MDU email address and password, approve the login in the MFA app on the device that you have already configured the MFA on.
- Click on Remove the device to be removed.

Lost/damaged mobile device

If you don't have access to your MFA-registered mobile device, you can reset your MFA by following the procedure outlined under the heading **Remove a device in MFA**, in a computer lab at MDU campus.

If you're unable to come to campus, you must contact the student centre to get assistance with resetting your MFA. To allow the student centre to assist you in resetting your device, you need to connect via Zoom and verify your identity.