2024-05-13

Mälardalens universitet

Multi-factor Authentication (MFA)

Multi-factor Authentication (MFA) also known as two-step verification, means that you will use two different verification steps to access your Microsoft account. This means that in one step you specify your username and password and in the next step you approve the login with an app in your mobile device.

System requirements for MFA

As a student, with an MDU email address, you will be activated for MFA and within 14 days you must verify your identity with MFA.

To verify yourself you need an iPhone with iOS 15.0 or later or an Android with an operating system 8.0 or later as well as the Microsoft Authenticator application that you download from the corresponding app library.

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.

Please note: You must not reinstall Microsoft Authenticator on your mobile device if you notice an error with MFA. Please contact the Student Centre instead for help to restore/activate MFA on your mobile device if there is a problem/error. For the Student Centre to be able to help you to restore/activate your device you need to provide your personal identity number to verify yourself.

Activate MFA for the first time

Start by downloading and installing the Microsoft Authenticator app on your mobile phone. It’s important that all the steps are followed.

1. Start Microsoft Authenticator on your mobile device and approve the terms and conditions and allow notifications. If you do not allow notifications on the mobile device, MFA activation may be denied.
2. Select Add an account.
3. Select Work or School account.
4. Click on Scan the QR code and allow access to the camera as well as allowing notifications and messages from the app.
5. Open a web browser and write the address to Microsoft’s page for managing the MFA application, https://mysignins.microsoft.com/security-info. It’s better if you do this from a computer.
6. Login with your MDU email address and password.
7. You should now see a guide, click on Next until you come to a page with a QR code.
8. Use your mobile device to scan the QR code through Microsoft Authenticator.
9. Click next on your computer.
10. Enter the numbers shown on your computer in your mobile device.

11. Click on Next and now you have added the mobile device as an authentication method for MFA.

Approve the login

When you log in with your MDU account, as a next step you will need to approve the login in the Microsoft Authenticator app on your mobile device. Never authorise a login you are not expecting. If you are unsure it's better to deny a login.

1. Log in to your MDU account on a computer or mobile device.
2. A check box for approval will be displayed with numbers.
3. Enter the numbers in the Microsoft Authenticator app on the mobile device that you have registered MFA.
4. You can check the box ”Don't ask again for 14 days” and the login on the particular device will be valid for 14 days.
5. When you have entered the numbers in Microsoft Authenticator, press Yes.

Add a new mobile device

There are two sub-headings you can choose from, for steps you follow if, for example, you want to add additional mobile devices for MFA or if you need to replace a lost/broken device for MFA.

Add additional mobile devices

1. Start a web browser on a computer.
2. In the address box please enter https://mysignins.microsoft.com/security-info
3. Login with your MDU email address and password and approve the login in the Microsoft Authenticator app on the device that you have configured MFA on.
4. Click on Security information in the left field, then on Add a sign-in method.
5. Select the Authentication app and then click on Add.
6. A guide will be shown on the computer.
7. Download and start Microsoft Authenticator on your mobile device and approve the terms and conditions and allow notifications. If you do not allow notifications on the mobile device, MFA activation may be denied.
8. Select Add an account.
9. Select Work or School account.
10. Click on Scan the QR code and allow access to the camera as well as allowing notifications and messages from the app.
11. On the computer, click Next until a page with a QR code is shown.
12. Use your mobile device to scan the QR code through Microsoft Authenticator.
13. Click next on your computer.
14. Enter the numbers shown on your computer on your mobile device.
15. Click on Next and now you have added the mobile device as an authentication method for MFA.

Add a new mobile device if you have a lost/broken device

Please note: If you use a computer in the Library or a computer room on campus you will not need to approve the login through Microsoft Authenticator on your lost/broken mobile device. If you are unable to get to a computer room/Library on campus, you will need to contact the Student Centre who will help remove the MFA on the lost/broken device and add the new mobile device. For the Student Centre to be able to help you to restore your device you need to provide your personal identity number to verify yourself.

1. Start a web browser on a computer in a computer room on the MDU campus.
2. In the address box please enter https://mysignins.microsoft.com/security-info
3. Login with your MDU email address and password.
4. Click on Security information in the left field, then on Add a sign-in method.
5. Select the Authentication app and then click on Add.
6. A guide will be shown on the computer.
7. Download and start Microsoft Authenticator on your mobile device and approve the terms and conditions and allow notifications. If you do not allow notifications on the mobile device, MFA activation may be denied.
8. Select Add an account.
9. Select Work or School account.
10. Click on Scan the QR code and allow access to the camera as well as allowing notifications and messages from the app.
11. On the computer, click Next until a page with a QR code is shown.
12. Use your mobile device to scan the QR code through Microsoft Authenticator.
13. Click next on your computer.
14. Enter the numbers shown on your computer on your mobile device.
15. Click on Next and now you have added the mobile device as an authentication method for MFA.

Remove a device in MFA

This step is performed if you want to remove MFA from a mobile device when you have acquired a new mobile device. If you have a lost/broken mobile device on which you have activated MFA and you want to remove it, you will have to follow the steps above first (see "Add a new mobile device when you have a lost/broken device", after that you can remove the lost/broken device).

1. Start a web browser on a computer.
2. In the address box please enter https://mysignins.microsoft.com/security-info
3. Login with your MDU email address and password, approve the login in the Microsoft Authenticator app on the device that you have already configured MFA on.

Click on Remove beside the device that you want to remove.