

Multifaktorautentisering (MFA)

Multifaktorautentisering (MFA), även känd som tvåstegsverifiering, innebär att du använder dig av två olika verifieringssteg för att få tillgång till ditt Microsoft-konto. Det innebär att du i steg ett anger ditt användarnamn och lösenord och i nästa steg godkänner inloggningen med en app i din mobila enhet.

Systemkrav för MFA

Som student, med en MDU e-postadress, blir du aktiverad för MFA och ska inom 14 dagar autentisera dig med MFA.

För att autentisera dig behöver du en iPhone med iOS 15.0 eller senare eller en Android med operativsystem 8.0 eller senare, samt applikationen Microsoft Authenticator som du laddar ned från respektive tillverkares bibliotek där appar finns.

Det finns även andra applikationer med liknande namn och ikon, så försäkra dig om att det är Microsoft Authenticator av Microsoft Corporation som du installerar.

Observera! Du ska inte ominstallera Microsoft Authenticator på din mobila enhet om du uppmärksammar ett fel med MFA. Kontakta i stället studenttorget för hjälp att återställa/aktivera MFA på din mobila enhet om ett fel uppstår. För att studenttorget ska kunna hjälpa dig att återställa/aktivera din enhet behöver du bistå med ditt personnummer för att kunna verifiera dig.

Aktivera MFA för första gången

Börja med att ladda ner och installera applikationen Microsoft Authenticator på din mobila enhet. Det är viktigt att alla steg utförs.

1. Starta Microsoft Authenticator på din mobila enhet och godkänn villkoren, samt tillåt aviseringar. Om du inte tillåter aviseringar på mobila enheten så kan aktivering av MFA nekas.
2. Välj Lägg till ett konto.
3. Välj Arbete eller skolkonto.
4. Klicka på Skanna QR-koden och ge åtkomst till kameran samt tillåt aviseringar och meddelanden från applikationen.
5. Starta en webbläsare och skriv adressen till Microsofts sida för hantering av MFA-applikationen, <https://mysignins.microsoft.com/security-info>. Detta gör du med fördel från en dator.
6. Logga in med din MDU e-postadress och lösenord.
7. En guide borde nu visas, klicka på Nästa tills en sida med en QR-kod visas.
8. Använd nu din mobila enhet för att skanna QR-koden genom Microsoft Authenticator.
9. På datorn klickar du sedan på Nästa.
10. På din mobila enhet, skriv in siffrorna som visas på datorn.

11. Klicka på Nästa och nu har du lagt till den mobila enheten som en autentiseringsmetod för MFA.

Godkänn inloggningen

När du loggar in med ditt MDU-konto ska du som nästa steg godkänna inloggningen i Microsoft Authenticator på din mobila enhet. Godkänn aldrig en inloggning som du inte förväntar dig. Om du är osäker är det bättre att neka inloggningen.

1. Logga in på ditt MDU-konto på en dator eller mobil enhet.
2. En ruta för godkännande kommer visa sig med siffror.
3. Skriv siffrorna i Microsoft Authenticator appen på den mobila enhet som du registrerat MFA på.
4. Du kan bocka i rutan "Don't ask again for 14 days" och inloggningen på den specifika enheten kommer att vara giltig i 14 dagar.
5. När du har skrivit in siffrorna i Microsoft Authenticator, tryck Ja.

Lägg till en ny mobil enhet

Här finns två underrubriker du får välja mellan, för steg du följer om man exempelvis vill lägga till ytterligare mobila enheter för MFA eller om man behöver ersätta en förlorad/trasig enhet för MFA.

Lägg till ytterligare mobila enheter

1. Starta en webbläsare på en dator.
2. I adressfältet skriver du <https://mysignins.microsoft.com/security-info>
3. Logga in med din MDU e-postadress och lösenord, godkänn inloggningen i Microsoft Authenticator på den mobila enhet som du har konfigurerat MFA på.
4. Klicka på Säkerhetsinformation i vänstra fältet och sedan på Lägg till inloggningsmetod.
5. Välj Autentiseringsapp och klicka sedan på Lägg till.
6. Ladda ner och starta Microsoft Authenticator på din nya mobila enhet och godkänn villkoren, samt tillåt aviseringar. Om du inte tillåter aviseringar på mobila enheten så kan aktivering av MFA nekas.
7. Välj Lägg till ett konto.
8. Välj Arbete eller skolkonto.
9. Klicka på Skanna QR-koden och ge åtkomst till kameran samt tillåt aviseringar och meddelanden från applikationen.
10. På datorn, klicka Nästa tills en sida med en QR-kod visas.
11. Använd nu din mobila enhet för att skanna QR-koden genom Microsoft Authenticator.
12. På datorn klickar du sedan på Nästa.
13. På din mobila enhet, skriv in siffrorna som visas på datorn.
14. Klicka på Nästa och nu har du lagt till den mobila enheten som en autentiseringsmetod för MFA.

Lägg till en ny mobil enhet när du har en förlorad/trasig enhet

Observera! Om du använder en dator i biblioteket eller en datorsal på campus, så kommer du inte behöva godkänna inloggningen via Microsoft Authenticator på din trasiga/förlorade mobila enhet. Har du inte möjlighet att ta dig till en datorsal/biblioteket på campus behöver du kontakta studenttorget som hjälper till med att ta bort MFA på den förlorade/trasiga enheten och lägga till den nya mobila enheten. För att studenttorget ska kunna hjälpa dig att återställa din enhet behöver du bistå med ditt personnummer för att kunna verifiera dig.

1. Starta en webbläsare på en dator i en datorsal på MDU campus.
2. I adressfältet skriver du <https://mysignins.microsoft.com/security-info>
3. Logga in med din MDU e-postadress och lösenord.
4. Klicka på Säkerhetsinformation i vänstra fältet och sedan på Lägg till inloggningsmetod.
5. Välj Autentiseringsapp och klicka sedan på Lägg till.
6. En guide kommer nu visas på datorn.
7. Ladda ner och starta Microsoft Authenticator på din nya mobila enhet och godkänn villkoren, samt tillåt aviseringar. Om du inte tillåter aviseringar på mobila enheten så kan aktivering av MFA nekas.
8. Välj Lägg till ett konto.
9. Välj Arbete eller skolkonto.
10. Klicka på Skanna QR-koden och ge åtkomst till kameran samt tillåt aviseringar och meddelanden från applikationen.
11. På datorn, klicka Nästa tills en sida med en QR-kod visas.
12. Använd nu din mobila enhet för att skanna QR-koden genom Microsoft Authenticator.
13. På datorn klickar du sedan på Nästa.
14. På din mobila enhet, skriv in siffrorna som visas på datorn.
15. Klicka på Nästa och nu har du lagt till den mobila enheten som en autentiseringsmetod för MFA.

Ta bort en enhet i MFA

Detta steg utförs om du vill ta bort MFA från en mobil enhet när du har införskaffat en ny mobil enhet. Har du en förlorad/trasig mobil enhet som du har aktiverat MFA på som du vill ta bort, så får du följa stegen ovan först (se "Lägg till en ny mobil enhet när du har en förlorad/trasig enhet", efter det kan du ta bort den förlorade/trasiga enheten).

1. Starta en webbläsare på en dator.
2. I adressfältet skriver du <https://mysignins.microsoft.com/security-info>
3. Logga in med din MDU-e-postadress och lösenord och godkänn inloggning i Microsoft Authenticator på den enhet där du redan konfigurerat MFA.
4. Tryck på Ta bort bredvid enheten som du vill ta bort.