



## Hvorfor Office 365 MFA – 2 faktor autentisering

Kombinasjonen av bare brukernavn og passord gir ikke god nok beskyttelse for pålogging i Office 365. Hovedtyngden av bekreftede data-innbrudd i de senere årene skyldes svake, standard eller stjålne passord. Resultatet kan være tap av kritisk informasjon, kompromitterte tjenester, ødelagt rykte – og ikke minst gigantiske utgifter. Angrepene kommer som regel utenfra og foretas ved hjelp av sosial manipulering, phishing og skadelig programvare. Med multifaktor-autentisering (MFA) gjør du det betydelig vanskeligere for en angriper å komme seg inn i kontoen din, for så i neste omgang å kartlegge svake punkter i kommunen og legge ut på en angrepskjede.

Office 365 MFA benyttes for å gi brukere multifaktor eller 2-faktor autentisering på Office 365-tjenestene. Office 365 MFA er inkludert i Office365-abonnementene til kunder.

Office 365 MFA vil, når det er aktivert, beskytte alle Office 365-tjenester som kunden har – Outlook, Teams, Skype for Business, OneDrive etc.

Brukere av Office 365 MFA må ha tilgang til en smarttelefon da selve 2faktor-løsningen anbefales brukt med en app som lastes ned på smarttelefonen. Denne appen finnes både for Android og IOS(IPhone). Appen heter Authenticator og bruker vil måtte godkjenne med denne appen hver gang en prøver å logge inn på en Office365 applikasjonen. Feide pålogging benytter samme app. Det er også mulig å sette opp løsningen slik at det sendes en SMS til bruker med kode som må tastes inn for å autentisere bruker mot Office365.

### 1. Brukerveiledning for installasjon og oppsett

(Ved bytte av mobiltelefon gå til: [2. Brukerveiledning ved bytte av mobiltelefon](#))


Du trenger PC/Mac og Mobil for å sette opp løsningen.

1. Last ned på mobilen og installer **Microsoft Authenticator appen** fra Google Play eller Apple App store. Tillat varslings. Når ferdig installert, ikke legg til konto enda.



2. Åpne en **nettleser lokalt** på PC eller Mac (ikke 3-1 ....) og gå inn på <https://aka.ms/mfasetup>

3. **Logg på** med din jobb e-postadresse og passord eller velg en konto hvis du har vært innlogget tidligere. (her er det tre mulige alternativer basert på tidligere bruk)

 Microsoft  
test.bruker1@ikomm-mgmt.no

#### Trenger mer informasjon

Organisasjonen trenger mer informasjon for å beskytte kontoen din

[Bruk en annen konto](#)

[Finn ut mer](#)

Neste

 Microsoft

#### Logg på

E-post, telefon eller Skype

Ingen konto? [Opprett en konto](#)

[Får du ikke tilgang til kontoen?](#)

[Påloggingsalternativer](#)

Neste

 Microsoft

#### Velg en konto



ove.jorstad@lillehammer.kommune.no



Bruk en annen konto



#### 4. Velg **Neste**

#### 5. Du får spm om Ytterligere sikkerhetsbekreftelse

Enten får du skjermbilde **5a** eller så får du skjermbilde **5b**.

#### **5a:** (aktuelt ved første gangs konfigurering)

### Ytterligere sikkerhetsbekreftelse

Sikre kontoen din ved å legge til telefonbekreftelse i passordet. Vis video for å lære hvordan du sikrer kontoen din

#### Trinn 1: Hvordan skal vi kontakte deg?

Godkjenningstelefon  Mobil

Velg land eller område

Metode

Send meg en kode via SMS

Ring meg

Velg send meg en kode via SMS

Neste

Telefonnumrene dine vil bare bli brukt til kontosikkerhet. Standardavgifter for telefon og SMS vil påløpe.

Legg inn land og mobilnummer. Velg **Send meg en kode via SMS** og trykk **Neste**  
Du får en SMS med en 6 sifret kode som du legger inn (? er ikke en del av koden).  
Trykk neste og du skal fortsette på 5b.

#### **5b:**

### Ytterligere sikkerhetsbekreftelse

Når du logger på med passordet, må du også svare fra en registrert enhet. Dette gjør det vanskeligere for en hacker å logge på med bare et stjålet passord  
Å lære hvordan du sikrer kontoen din

hvilket alternativ foretrekker du?

Vi vil bruke dette bekreftelsesalternativet som standard.

Varsle meg gjennom appen

hvordan vil du svare?

Velg ett eller flere av disse alternativene. Lær mer

Godkjenningstelefon

Norge (+47)

12345678

Kontortelefon

Velg land eller område

Internett

Telefon for alternativ godkjenning

Velg land eller område

Godkjennerapp eller token

Konfigurer Authenticator-appen

Authenticator-app - LYA-L29

Slett

gjenopprett multi-factor authentication på tidligere klarerte enheter

Gjenopprett

Lagre avbryt

Telefonnumrene dine vil bare bli brukt til kontosikkerhet. Standardavgifter for telefon og SMS vil påløpe.



Merk av ihht skisse og deretter trykk **Konfigurer Authenticator-appen**  
Dette konfigureringsbildet kommer opp

## Konfigurer mobilapp

Fullfør de følgende trinnene for å konfigurere mobilappen.

1. Installer Microsoft Authenticator-appen for [Windows Phone](#), [Android](#) eller [iOS](#).
2. Legg til en konto i appen, og velg Jobb- eller skolekonto.
3. Skann bildet nedenfor.



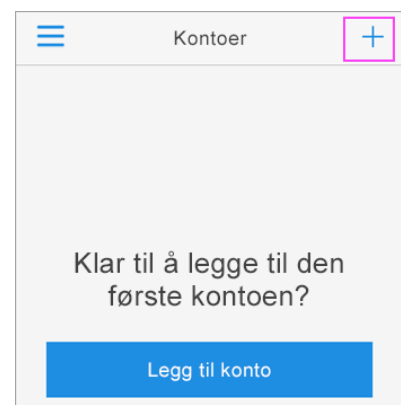
Hvis du ikke kan skanne bildet, skriver du inn følgende informasjon i appen.

Kode: 933 757 394

Nettadresse: <https://cys01eupad03.eu.phonefactor.net/pad/237137809>

Hvis en seksifret kode vises i appen, velger du Neste.

- Åpne Authenticator-appen på telefonen.  
I appen vil  
Er konto forsøkt installert tidligere, men med feil så må denne kontoen fjernes før du fortsetter. (For iPhone klikk på konto og deretter slett, for Android klikk på tre loddrette prikker i høyre hjørne og deretter rediger og slett (rødt kryss))
- Trykk på **Legg til konto** (eller + på iPhone) >  
Velg **Jobb- eller skolekonto**
- Bruk telefonen til å skanne QR-firkanten på PC skjermen og en konto blir lagt til i appen. (3-1 <din mailadresse>)
- Når konto vises i appen  
(og en kode som endres hvert 30 sek)  
**Så trykker du Neste i Konfigurer mobilapp på PC.**



**NB!** Det er viktig at du har appen åpen mens konfigureringen pågår

- Velg lagre i konfigureringsbildet på PC og verifiser (godkjenn) meldingen som kommer på tlf.

Fortsett med pkt 6 hvis aktuelt bilde dukker opp. Hvis ikke fortsett med pkt 7.



## 6. Velg **Mobilapp** og **Motta varslinger for bekreftelse**

### Trinn 1: Hvordan skal vi kontakte deg?

Mobilapp

Hvordan vil du bruke mobilappen?

Motta varslinger for bekreftelse

Bruk bekreftelseskode

Du må konfigurere Microsoft Authenticator-appen for å kunne bruke disse verifiseringsmetodene.

**Konfigurer** Konfigurer mobilappen.

## 7. Når mobilappen er konfigurert for varsler og verifisering > Velg **Neste**

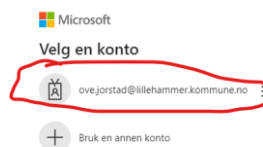
## 8. En kontroll gjennomføres ved at det sendes et varsel til mobilappen > Velg **Godkjenn**

## Ferdig!

## 2. Brukerveiledning ved bytte av mobiltelefon

På PC/Mac kjør <https://aka.ms/mfasetup>

Logg på din konto :



...og godkjenn i app på gammel enhet.

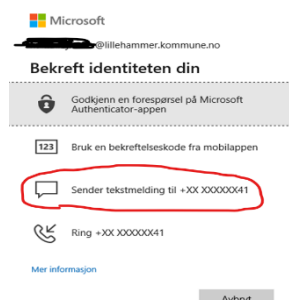


Har du ikke gammel enhet (mobiltelefon) tilgjengelig må du verifisere med sms til tlf nr.

Velg "Logg på på en annen måte"

og velg "Sender tekstmelding til

+XX XXXXXXXX





Du får tilsendt en kode på SMS som du skriver inn for å logge deg på (Kontroller).

 Microsoft

← hanne.bjaanes@lillehammer.kommune.no

### Angi kode

Vi sendte en tekstmelding til telefonen din +XX  
XXXXXX41. Skriv inn koden for å logge deg på.

Kode

Ikke spør på nytt før om 30 dager

[Mer informasjon](#)

Kontroller

Du kommer inn i konfigurasjonsbildet for MFA.

### Ytterligere sikkerhetsbekreftelse

Når du logger på med passordet, må du også svare fra en registrert enhet. Dette gjør det vanskeligere for en hacker å logge på med bare et s  
å lære hvordan du sikrer kontoen din

hvilket alternativ foretrekker du?

Vi vil bruke dette bekreftelsesalternativet som standard.

Varsle meg gjennom appen

hvordan vil du svare?

Velg ett eller flere av disse alternativene. Lær mer

<input checked="" type="checkbox"/> Godkjenningstelefon	Norge (+47)	90613737
<input type="checkbox"/> Kontortelefon	Velg land eller område	
<input type="checkbox"/> Telefon for alternativ godkjenning	Velg land eller område	Internnummer
<input checked="" type="checkbox"/> Godkjennerapp eller token	Konfigurer Authenticator-appen	

Authenticator-app - LVA-L29

Slett

gjenopprett multi-factor authentication på tidligere klarerte enheter

Gjenopprett

Lagre avbryt

Telefonnumrene dine vil bare bli brukt til kontosikkerhet. Standardavgifter for telefon og SMS vil påløpe.

Her er din gamle enhet som skal slettes. (Trykk slett og bekreft sletting. Deretter Lagre.)

Har du kopiert innhold fra gammel telefon til ny telefon så har Authenticator appen blitt kopiert med, men dette er IKKE tilstrekkelig.

Authenticator appen må avinstalleres og installeres på nytt for at den skal fungere. (av sikkerhetsmessige grunner)

Når Authenticator appen er installert på nytt (på ny tlf) klikker du på "Konfigurer Authenticator-appen" på PC (QR kode dukker opp) På telefon legger du til en Jobb eller skolekonto, skanner QR kode og ny konto blir registrert på tlf. Følg instruksjonene (se pkt 5 tidligere i veiledningen).

Lagre når oppsettet er ferdig.



Hva skjer når to-faktor pålogging er i bruk:

Første gang du starter f.eks Teams etter at din bruker er aktivert for to-faktor blir du bedt om å godkjenne påloggingsforespørselen.



ove.jorstad@lillehammer.kommune.no

## Godkjenn påloggingsforespørselen

- 🔒 Vi har sendt et varsel til mobilenheten din.  
Åpne Microsoft Authenticator-appen for å svare.

Har du problemer? [Logg på på en annen måte](#)

På telefonen må du trykke godkjenn. (Alternativt en kode tilsendt på SMS)

Applikasjonen starter som vanlig og to-faktor autentisering er aktivt.

Det vil **ikke** komme flere spørsmål om godkjenning før du evt logger på fra en annen kilde.

Da vil det samme skje med at du får spørsmål om **Godkjenn påloggingsforespørsel** og du må godkjenne denne på telefonen.

Når du bytter påloggingspassord for din bruker så vil det komme en ny **Godkjenn påloggingsforespørsel** som du må godkjenne på telefonen.

Ønsker du å teste ut at to - faktor pålogging virker for din bruker så kan du gjøre dette i

Google Chrome nettleser

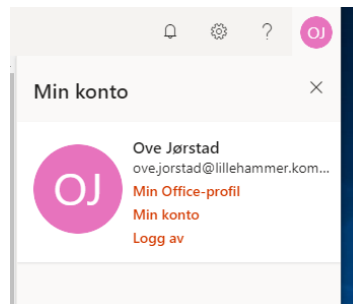
Start Google Chrome



Og logge deg på med din konto (mailadresse). <https://login.microsoftonline.com/>



NB! Husk å logge deg av når du er ferdig!



Noe som ikke virker?

Kontakt Ikomm kundeservice på telefon eller registrer en sak på hendelsen.