

## How to configure Microsoft MFA (2-factor validation)

1. Go to <https://aka.ms/mfasetup>
2. Login using your organization e-mail-address and password.
3. Click "Add sign-in method".
4. Choose "Authenticator app" og click "Add".
5. On your smart-phone: Install the "Microsoft Authenticator" APP  
- looks like this icon 
6. Follow the on-screen instructions.
7. Not mandatory: If needed, you can add another Login method by clicking "Add sign-in method"

## Change standard method for logon

1. Go to <https://aka.ms/mfasetup>
2. Login using your organization e-mail-address and password.
3. Click "Change" left to "Default method for logon"

**Standardmetode for logon:** Microsoft Authenticator – meddelelse [Ændre](#)



Standardmetode for logon: Microsoft Authenticator – meddelelse <a href="#">Ændre</a>			
+ Tilføj logonmetode			
	Telefon	+45 [redacted] 3	<a href="#">Ændre</a> <a href="#">Slet</a>
	Microsoft Authenticator Push multi-factor authentication (MFA)	LE2113	<a href="#">Slet</a>

4. Choose your preferred logon method from the dropdown menu. (We recommend "Appbased authentication") and click "Confirm".

### Skift standardmetode

Hvilken metode vil du bruge til at logge på?



Appbaseret godkendelse – meddelelse
Telefon – opkald +45 [redacted]
Telefon – sms +45 [redacted]
Appbaseret godkendelse – meddelelse
Appbaseret godkendelse eller hardware-token – kode