Guide: Set up multiple factors (MFA) for your NordicHub Identity account

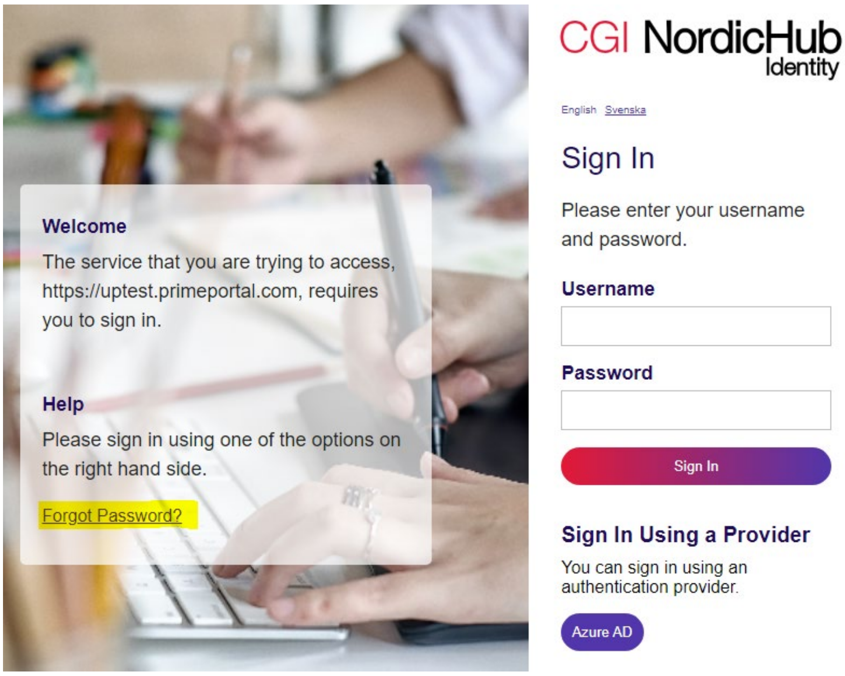
The NordicHub Identity service is used by web applications withing CGI to provide a secure way of signing in. A part of *NordicHub Identity* is the *MFA-configurator* which is used to set up a second factor for your account when signing in.

Use this step by step guide to activate required factors in the *MFA-Configurator*. See the guide on the pages below.

Getting started with MFA

Start by navigating to your service of interest with your browser. Eg. Unified Portal: https://up.primeportal.com.

After navigating to your service, you will end up at a sign-in page (see figure 1). Since MFA has been enabled you have to set a new password for your account the first time you log in. Follow the steps below to set a new password. Your old password won't work.



Welcome

The service that you are trying to access, https://uptest.primeportal.com, requires you to sign in.

Help

Please sign in using one of the options on the right hand side.

Forgot Password?

CGI NordicHub Identity

English Svenska

Sign In

Please enter your username and password.

Username

Password

Sign In

Sign In Using a Provider

You can sign in using an authentication provider.

Azure AD

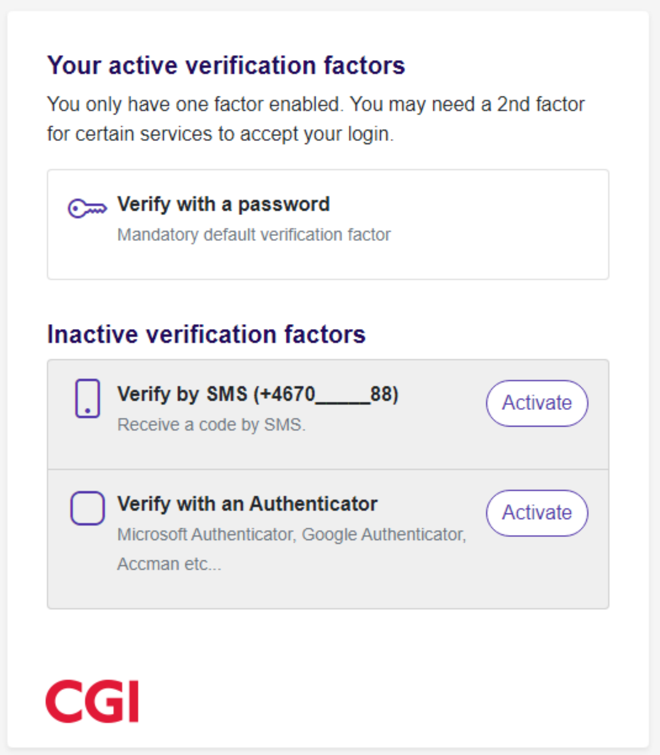
Figure 1: Image of the new sign-in page

How to set a new password for your account:

1. Navigate to your service’s URL in your web browser (eg. Unified Portal)
2. Use the "Forgot Password"-Link" and request a password reset
    a. Follow the instructions in the reset password email and set a new password
3. You have now set your first factor (password). To access your service, you have to set up a 2nd factor as well. Follow the instructions in the *Setting up your 2nd factor*-section below to activate your 2nd verification factor.

Setting up a 2nd Factor

After setting a new password for your account you have successfully enabled your first factor (password). You should now be able to set up a 2nd factor with the MFA-configurator. Follow one of the guides below and set up either SMS or an Authenticator (or both). The first time you configure your account it should look as in figure 2 below.



Your active verification factors

You only have one factor enabled. You may need a 2nd factor for certain services to accept your login.

Verify with a password
Mandatory default verification factor

Inactive verification factors

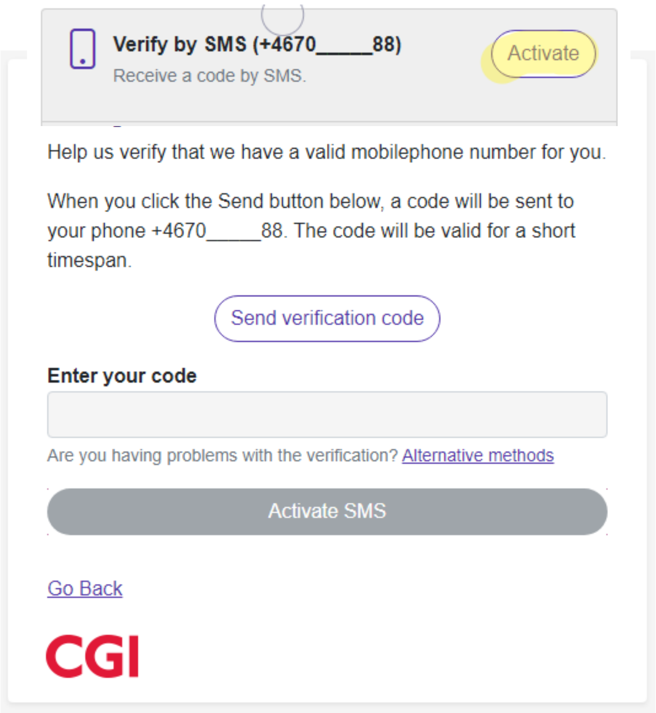
Verify by SMS (+4670_____88)
Receive a code by SMS.

Verify with an Authenticator
Microsoft Authenticator, Google Authenticator, Accman etc...

Figure 2: An Image of the MFA Configurators starting page before setting up a 2nd factor

How to set up SMS as a 2nd factor:

1. Navigate to the MFA-configurator web page in your browser
2. Check that your phone number seems correct in the “verify by SMS” selection.
    a. If your number seems incorrect you can go to the self-service page and set the number that you want to use.
3. Click on the “activate”-button (see figure 2 above) for the **verify by SMS** alternative.



Help us verify that we have a valid mobilephone number for you.

When you click the Send button below, a code will be sent to your phone +4670_____88. The code will be valid for a short timespan.

Are you having problems with the verification? Alternative methods

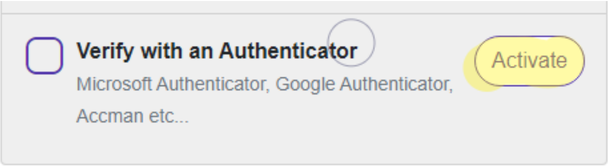
Figure 3: An image of activating SMS as a factor

4. Click on the “Send Verification Code”-button to receive a code by SMS on your phone.
5. Enter the code that you received on your phone in the “Enter your code”-input field.
6. Click on the “Activate SMS” button to finally activate SMS as a 2nd factor.
    a. Note: If your token is not valid please use the “send verification code” button to receive another one.
7. You can now navigate to your service in your web browser again (eg. Unified Portal) and sign-in in on the right-hand side with your password and then verify with SMS (see figure 1).

How to set up an Authenticator as a 2nd factor

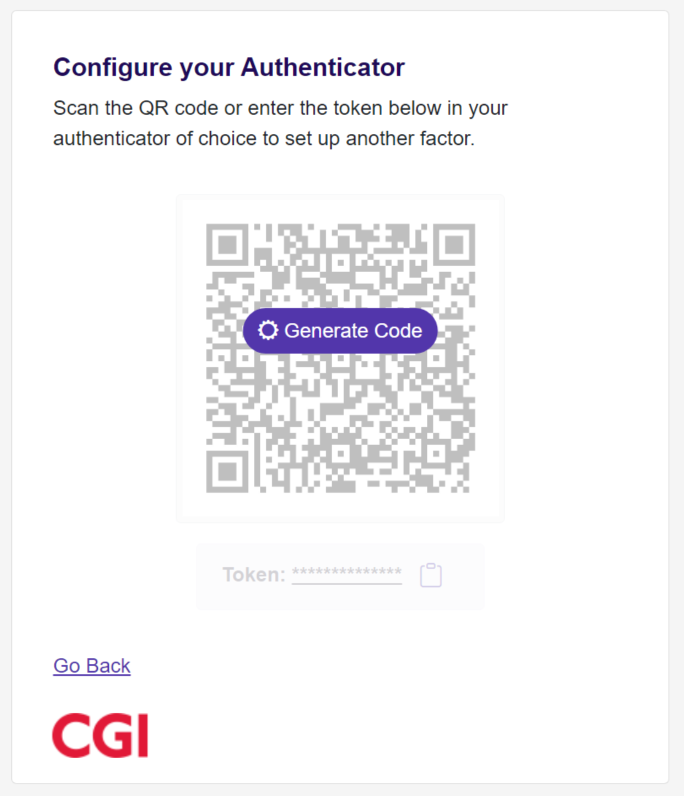
(google authenticator, Microsoft authenticator, Accman…)

1. Download your authenticator of choice to your phone or PC.
    a. Windows Authenticator, Google Authenticator, Accman or others…
2. Go to the MFA-configurator web page.
3. Click on the “activate”-button for the “**Verify with an Authenticator”** factor alternative (see figure 2).



Verify with an Authenticator
Microsoft Authenticator, Google Authenticator, Accman etc...
Activate

4. Click on the “Generate code”-button (see figure 4 below).



Configure your Authenticator

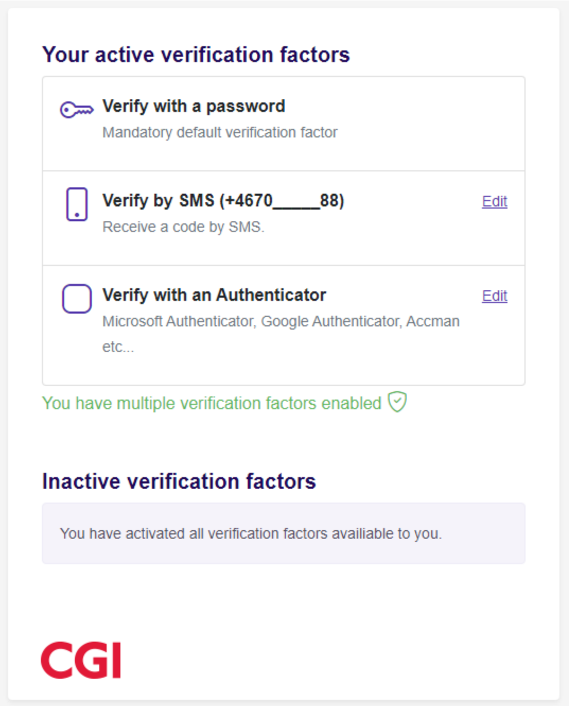
Scan the QR code or enter the token below in your authenticator of choice to set up another factor.

Go Back

CGI

Figure 4: A Image of configuring an authenticator as a factor

5. Scan the generated QR code or enter the token manually into your authenticator.



Your active verification factors

Verify with a password
Mandatory default verification factor

Verify by SMS (+4670_____88) Edit
Receive a code by SMS.

Verify with an Authenticator Edit
Microsoft Authenticator, Google Authenticator, Accman etc...

You have multiple verification factors enabled

Inactive verification factors

You have activated all verification factors availiable to you.

CGI

Figure 5: An Image of an account with all factors active

6. You can now go to your service in your browser again and sign in with your password and newly set up authenticator.