

How to use the Hansken Community Portal

Including setting up the 2-factor-authentication

Learn how to create your account, but also what to expect from the Hansken Community Portal. How does it work? What can it bring you? The do's, the don'ts, and other facts.

In this manual you can find:

1. How to create your account in 4 steps
2. How to set your 2-factor-authentication (MFA)
3. How to use the Portal – in short

1. How to create your account in 4 steps



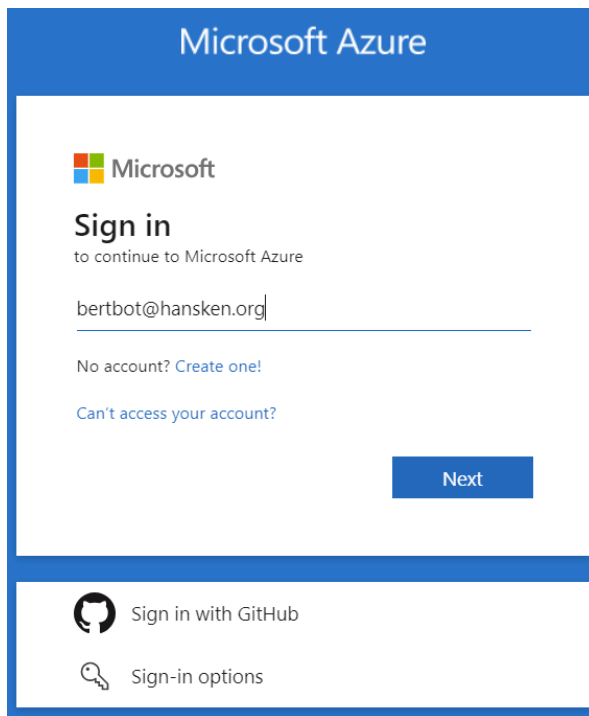
You've received the account details, what happens next?

1. Open [the Hansken Community Portal on the login page](#).
2. Click the button **Log in**.
3. You will be directed to the Azure login screen where you log in with the Azure-login details that you received per e-mail.
4. Then you set up the 2-factor authentication (see the steps below) and you change your password.


And you're all set to go!

2. How to set your 2-factor-authentication (MFA – Multi-Factor Authentication)

1. You're at portal.azure.com.
2. Enter your username (ends with @hansken.org) and click **Next**.



Microsoft Azure

 Microsoft


Sign in
to continue to Microsoft Azure


bertbot@hansken.org

No account? [Create one!](#)

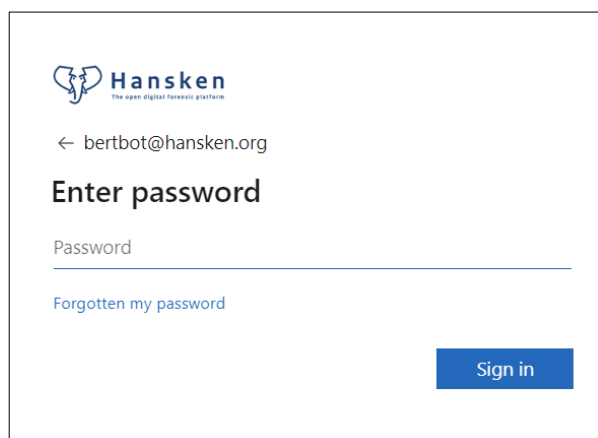
[Can't access your account?](#)


Next

 Sign in with GitHub

 Sign-in options

3. Then enter the password and click **Sign in**.



 **Hansken**
The open digital forensic platform

← bertbot@hansken.org

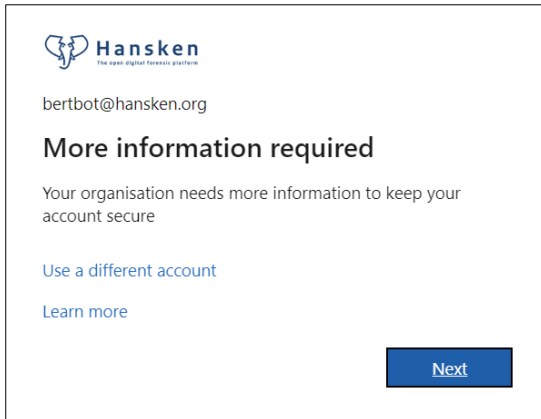
Enter password

Password

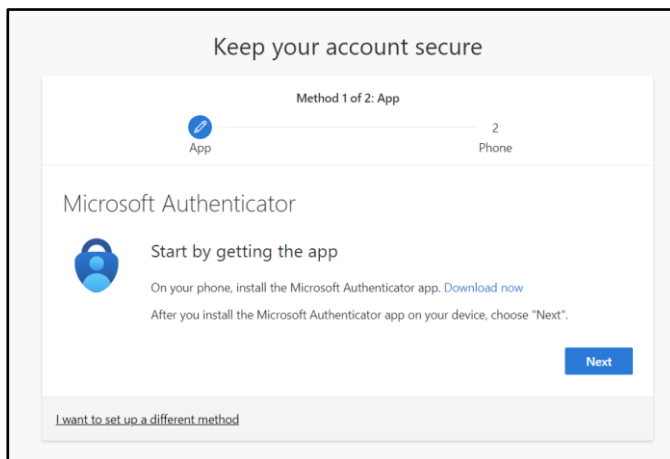
[Forgotten my password](#)

Sign in

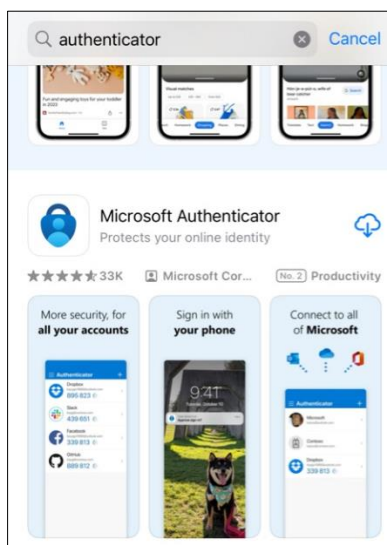
4. You will get a prompt that there is more information needed. In this screen, click **Next**.



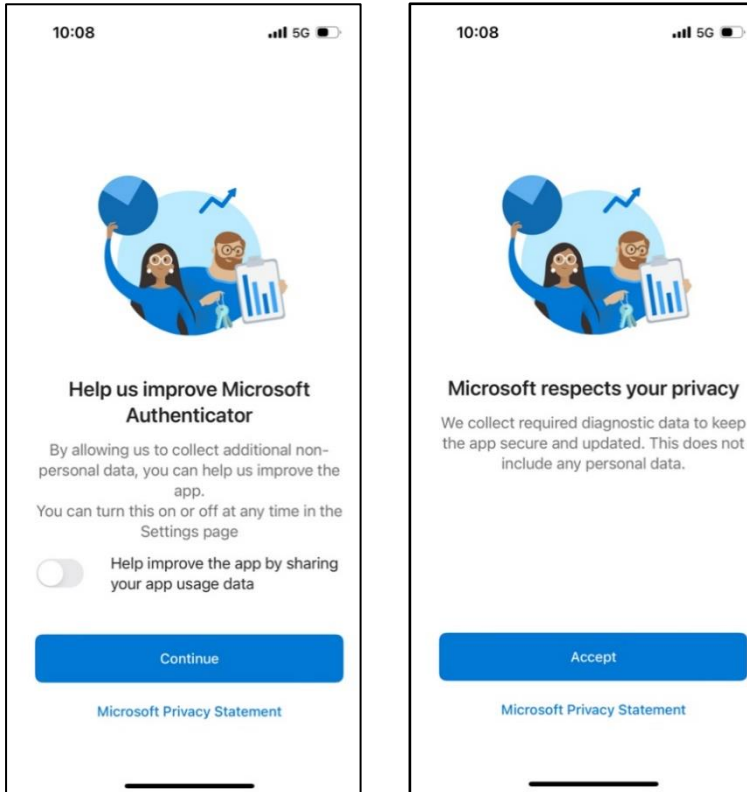
5. Follow the steps that are shown on the screen.



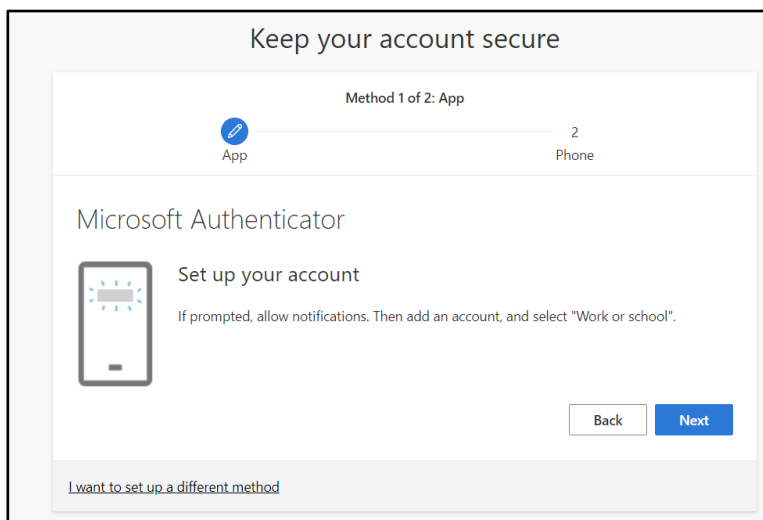
6. Start by downloading the **Microsoft Authenticator-app** on your Smartphone. You can do this via the de Apple Store or Google Play Store. Click **Next**.



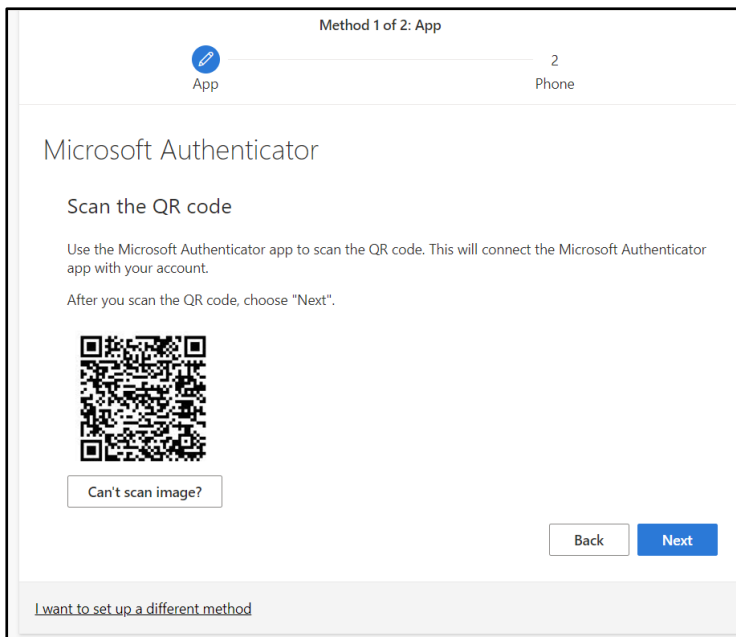
7. Start the application on your smartphone. The first time you start the application please follow through the initial steps.



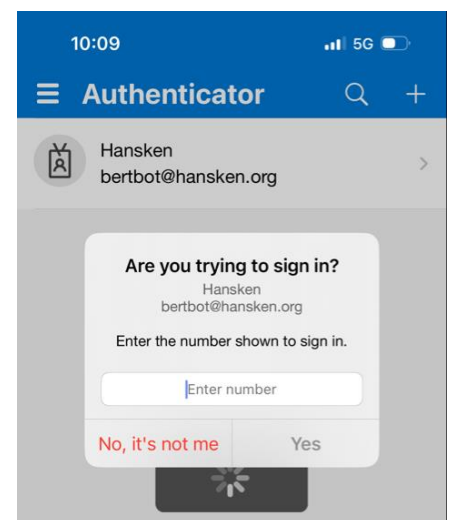
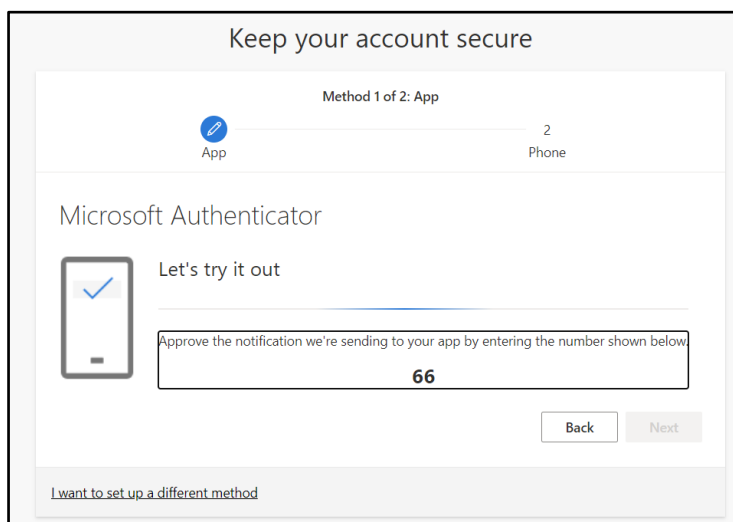
8. Read the following screen and click **Next**.



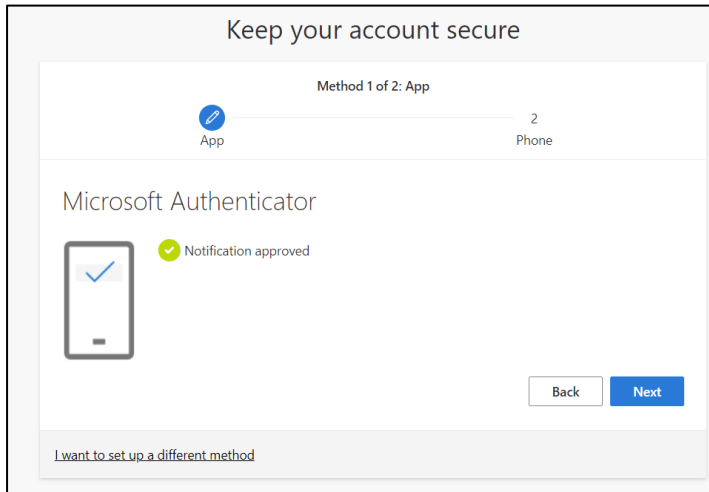
9. Scan the QR-code with the **Microsoft Authenticator-app**. When this is finished, click **Next**.



10. If everything went well, you now get a notification on your smartphone. Please enter the number you see on your computer in the screen that you see on your smartphone.



11. You see 'Notification approved'. Click **Next**.




Keep your account secure

Method 1 of 2: App

App 2
Phone

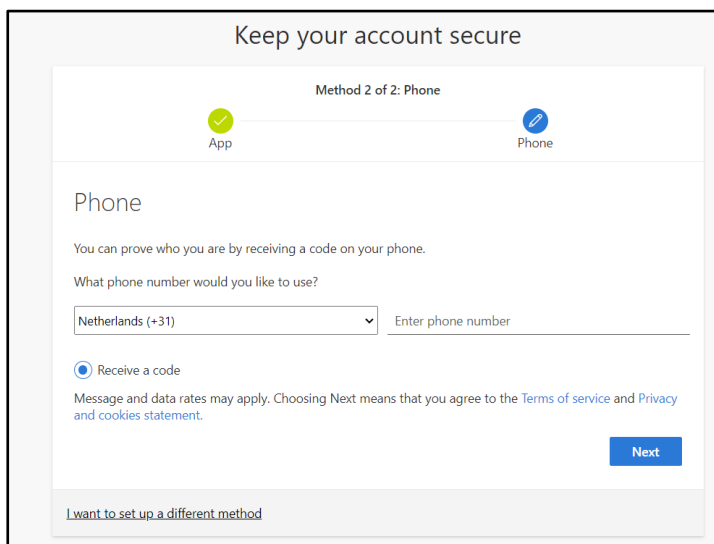
Microsoft Authenticator

 ✔ Notification approved

[I want to set up a different method](#)

[Back](#) [Next](#)

12. Enter your phone number as a back-up method for MFA. Click **Next**.



Keep your account secure

Method 2 of 2: Phone

✔ App ✔ Phone

Phone

You can prove who you are by receiving a code on your phone.

What phone number would you like to use?

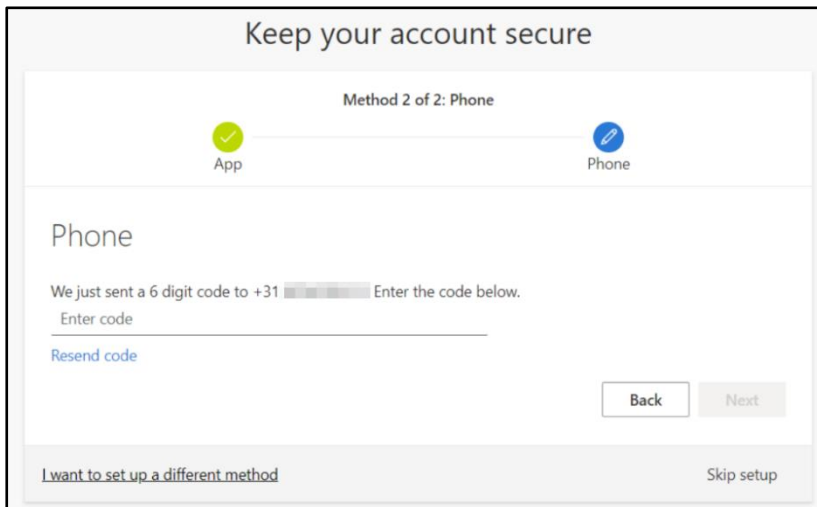
Receive a code

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

[Next](#)

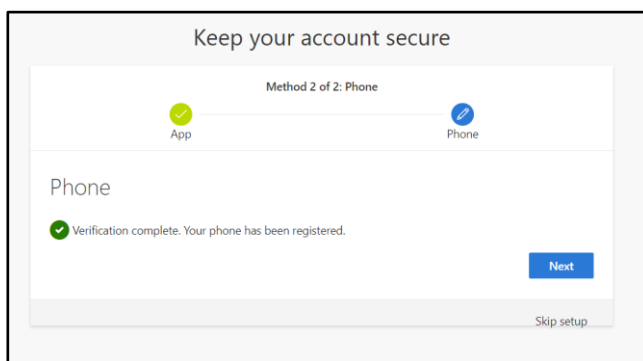
[I want to set up a different method](#)

13. You receive a code via SMS. Enter the code in the appropriate box and click **Next**.



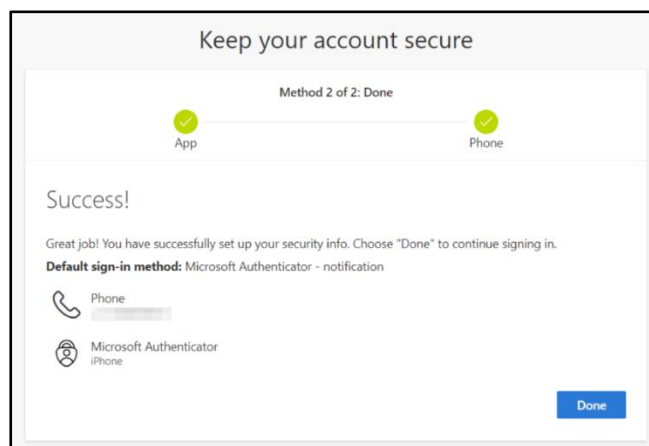
The screenshot shows a screen titled "Keep your account secure" with a progress indicator for "Method 2 of 2: Phone". The "App" method is marked with a green checkmark, and the "Phone" method is marked with a blue pencil icon. Below the progress bar, the "Phone" section contains the text: "We just sent a 6 digit code to +31 [redacted] Enter the code below." There is an input field labeled "Enter code" and a "Resend code" link. At the bottom right, there are "Back" and "Next" buttons. At the bottom left, there is a link: "I want to set up a different method". At the bottom right, there is a "Skip setup" link.

14. Click **Next** when the verification was successful.



The screenshot shows the same "Keep your account secure" screen. The progress indicator now shows both "App" and "Phone" methods with green checkmarks. The "Phone" section contains a green checkmark and the text: "Verification complete. Your phone has been registered." A blue "Next" button is visible at the bottom right, and a "Skip setup" link is at the bottom center.

15. You're good to go!



The screenshot shows the "Keep your account secure" screen with the progress indicator now showing "Method 2 of 2: Done". Both "App" and "Phone" methods are marked with green checkmarks. The main section is titled "Success!" and contains the text: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Below this, it lists the "Default sign-in method: Microsoft Authenticator - notification". There are two options listed: "Phone" with a telephone icon and "Microsoft Authenticator iPhone" with a Microsoft Authenticator icon. A blue "Done" button is located at the bottom right.

16. And then as a final step, you need to change the password that you received to your personal password.

 **Hansken**
The open digital forensic platform

bertbot@hansken.org

Uw wachtwoord bijwerken

U moet uw wachtwoord bijwerken omdat u zich voor het eerst aanmeldt of omdat uw wachtwoord is verlopen.

Huidig wachtwoord

Nieuw wachtwoord

Wachtwoord bevestigen

[Aanmelden](#)

3. How to use the Portal – in short

Who is it for?

For all people related to Hansken, providing that they have a Hansken license, like tactical investigators, digital experts, case operators and developers. But with a focus on the end users of the platform: the tactical investigator working with Hansken in a case.

For the digital/technical people we also have other channels in place, like Mattermost and a GitLab environment.

How does it work?

The Portal works in groups. When you click in the navigation bar, you can click 'All Groups' to see which subjects are accounted for.

In these groups, you can find information (documents, tutorials, publications, FAQ's by other users etc.) You can also post you own question, approach support, learn about the program of the Hansken Academy and other events and Hansken news. And of course the latest – and older – Hansken cartoons!

Chat

You also have the ability to chat with other users in a personal/separate chat in your profile, or set up a group chat in a group.

Add your own group/content

If you have an own subject that you like to gather information about, it is also an option to start a new group, but preferably use the existing groups, so we don't have the risk that we have to work with a hundred slightly different groups. If you miss something or you have an idea for content: please contact the Community Portal Manager (see 'Contact' below).

!! Important! We do not share case-related information!!

The most important rule inside the Portal is: do not talk about your cases!! So, the questions that you can ask of the knowledge that you can share, is purely about the way of working in Hansken or about the platform itself. For example how a feature works or the solution to a problem you're facing.

Password policy

The first time you receive your password, change it to a personal password. After this, there is no periodic question to change your password.

Create your profile

When your MFA is set, you can create your own profile. This can be done with data that you chooses yourself. Of course a profile that is as complete as possible works best. Especially your first name, function and organization are important elements to share. Then other users know who they are talking to. If really necessary, you can also use an avatar and/or a pseudo name.

Point of contact

The system administrators can always contact the Hansken Community Manager (currently Kristien Siemons) for questions and the necessary support. This person works from the NFI and can be reached via Hansken.Community@nfi.nl or by telephone via (06) 28 97 51 98.

If there is a need for contact between partners and the details are not known, this can be requested from Kristien Siemons.