MULTI-FACTOR AUTHENTICATION (MFA)

CONFIGURATION GUIDE

Contents

1. General information....................1
2. Configuring multi-factor authentication (MFA)....................1
   a. Configuration of the authentication application – MFA....................3
   b. Configuration of phone number – MFA....................5
3. Configuring multiple authentication methods. 7
4. Change default authentication factor....................7

1. General information

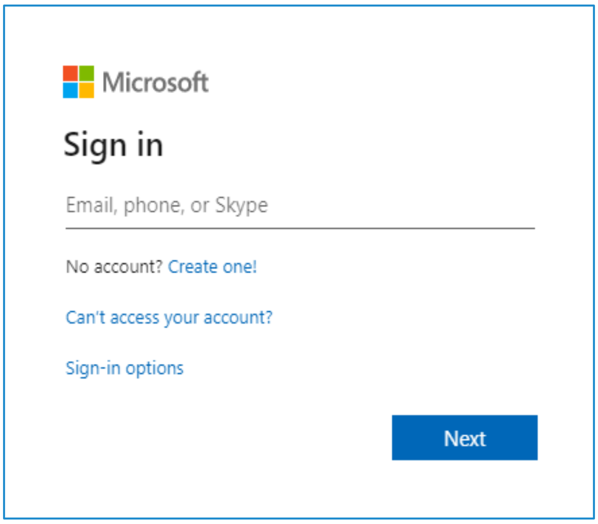
Multi-factor authentication (MFA) is an additional procedure that secures access to university resources. In addition to providing login data, the user in the next step provides a one-time security code sent via an SMS message or generated using a special application (available for all mobile systems).

You can set several authentication methods and select only one default method.

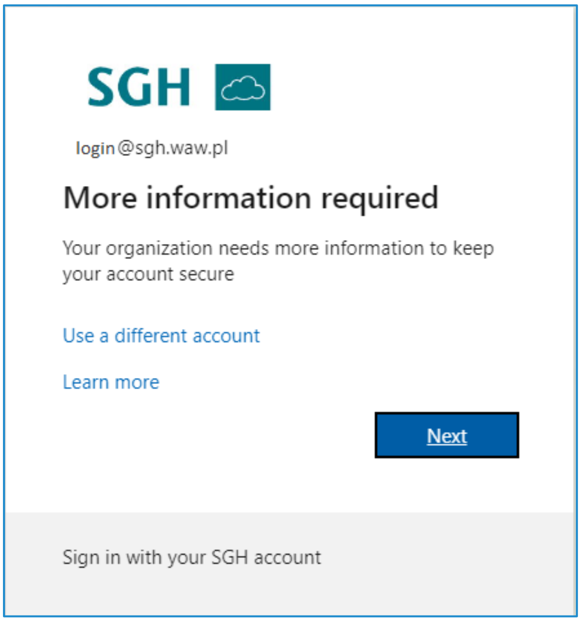
Multi-factor authentication is configured during the first login to the SGH account. After configuring multi-factor authentication, you can make changes in the configuration at https://mfa.sgh.waw.pl website.

2. Configuring multi-factor authentication (MFA)

1. To configure MFA, you need to visit the website https://mfa.sgh.waw.pl and log in to your SGH account.



2. After successful login, the following screen will appear. You need to click “Next”



SGH

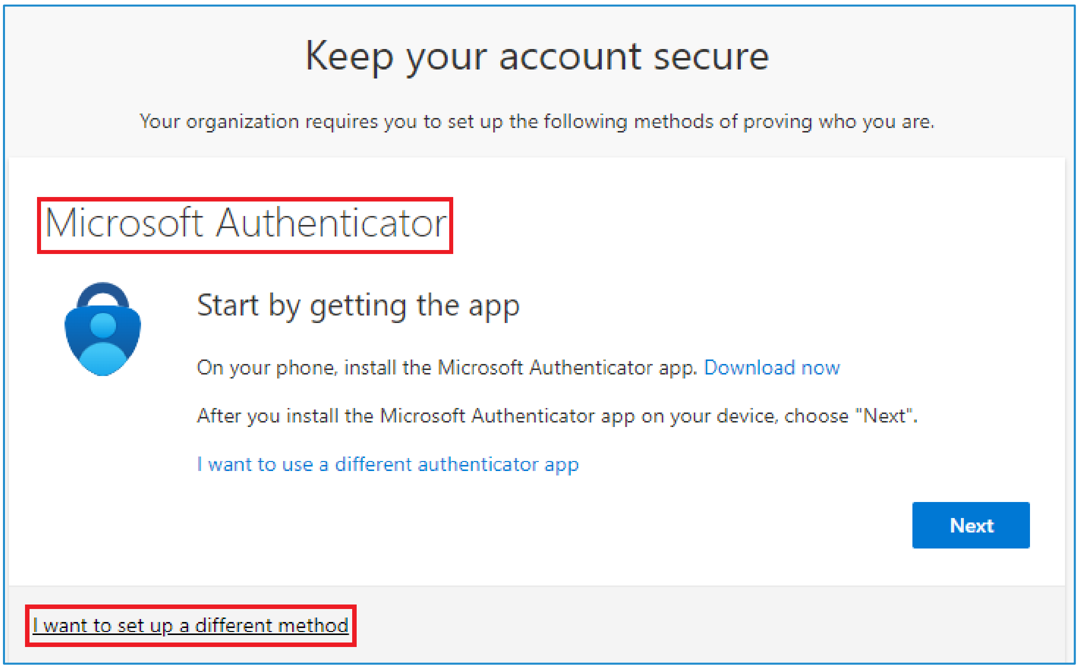
login@sgh.waw.pl

More information required

Your organization needs more information to keep your account secure

Sign in with your SGH account

3. After selecting "Next", a page will open with the option to select a verification method. This can be the Microsoft Authenticator app or another method:



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

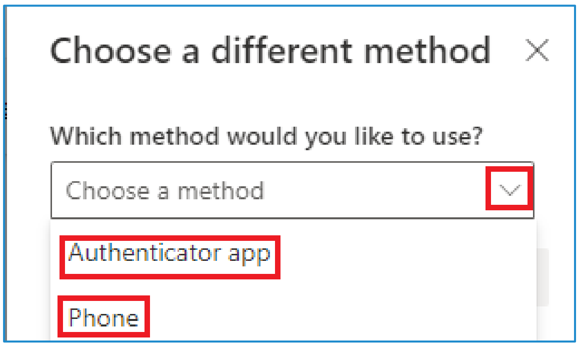
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app
Next
I want to set up a different method

4. When we select the option "I want to configure another method", the method selection window will be displayed:



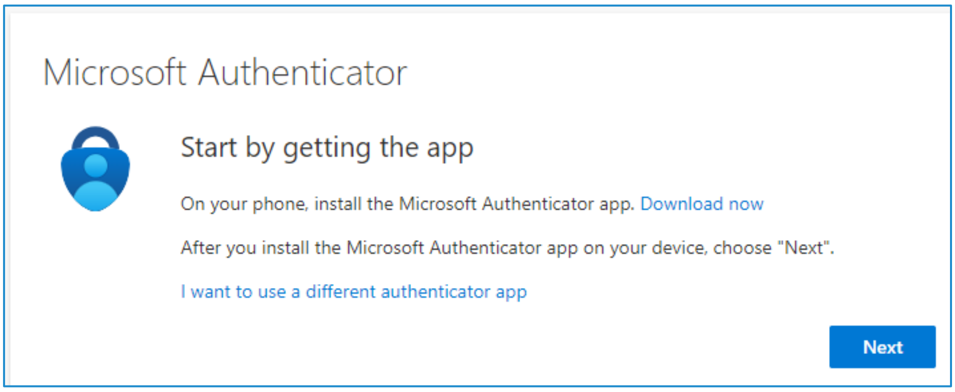
Choose a different method

Which method would you like to use?

a. Configuration of the authentication application – MFA

The application Microsoft Authenticator can be installed on multiple mobile devices – setting up an additional device and installation the application is similar every time.

1. If you select authentication app, the following message will appear



Microsoft Authenticator

Start by getting the app

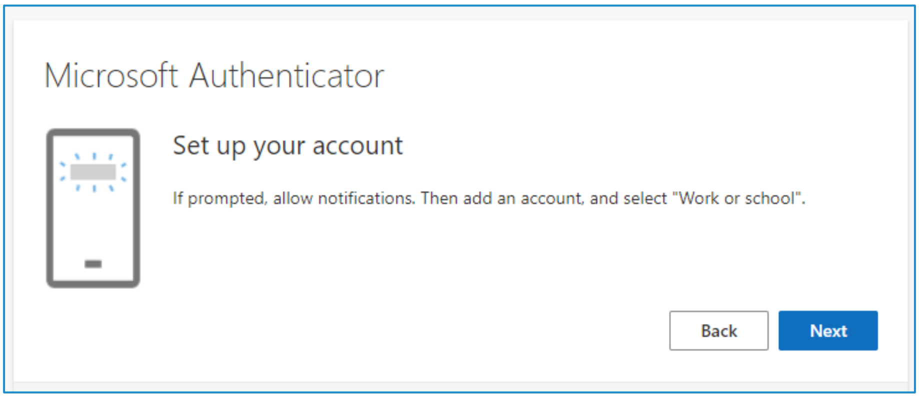
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Download and install the Microsoft Authenticator app on your mobile device. After selecting “Download now”, a page where you can download Android and iOS app will appear.

2. After installing application, you can go to the next step:



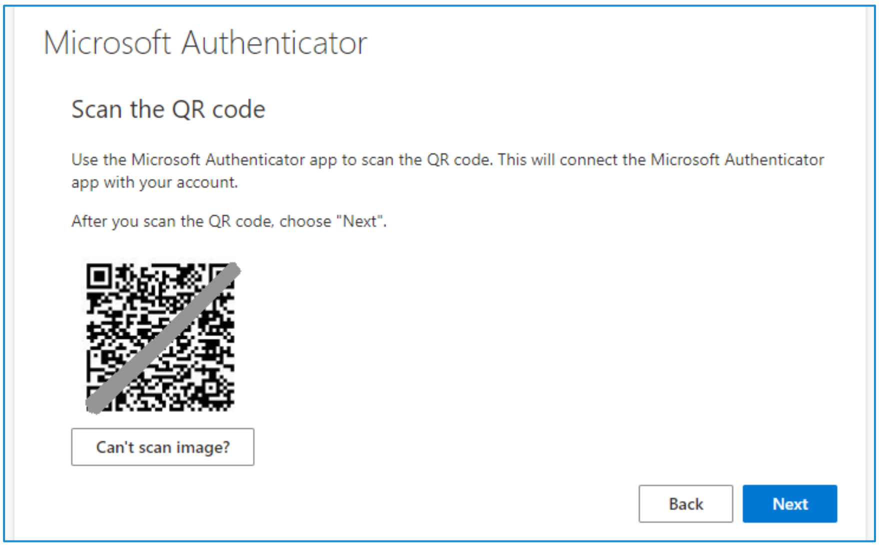
Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Important: Remember to allow the app to send notifications.

3. After selecting “Next”, a QR code will be displayed, which will be necessary to configure the application on mobile device:



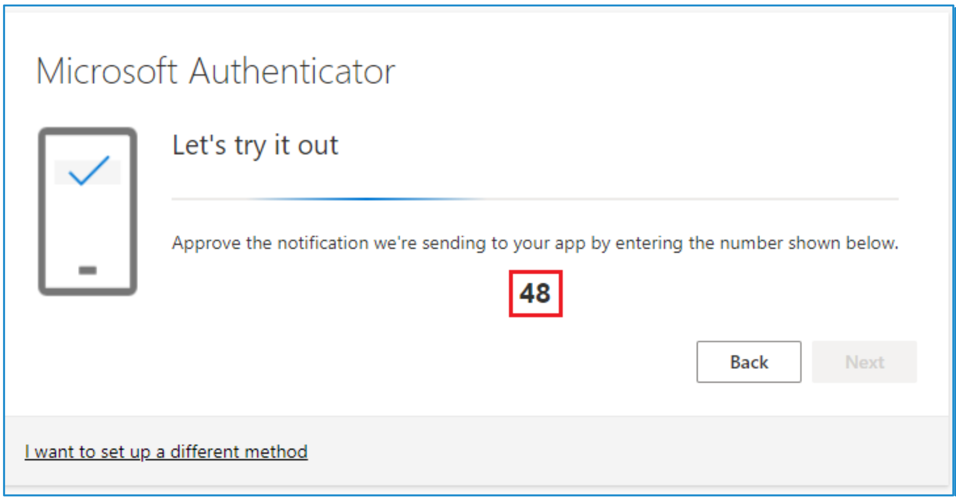
Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

4. After scanning the code, in the application, the information “Account added successfully” will appear.
5. The last step is entering 2-digit code into the application on your mobile device, which will be displayed on the screen.

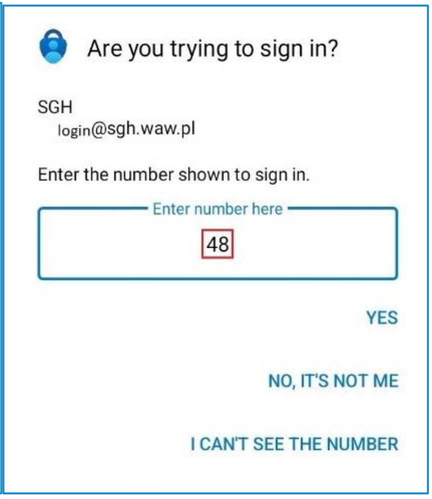


Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

48



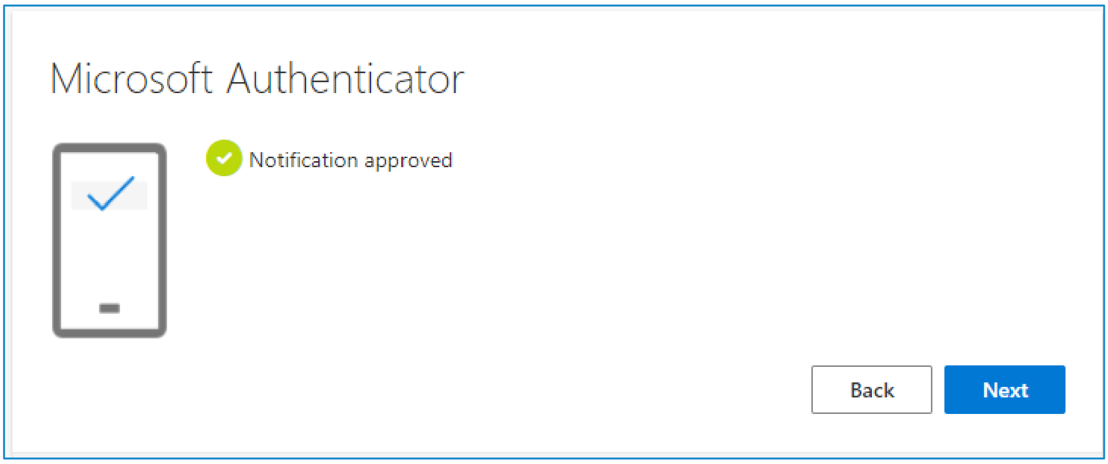
Are you trying to sign in?

SGH
login@sgh.waw.pl

Enter the number shown to sign in.

Enter number here: 48

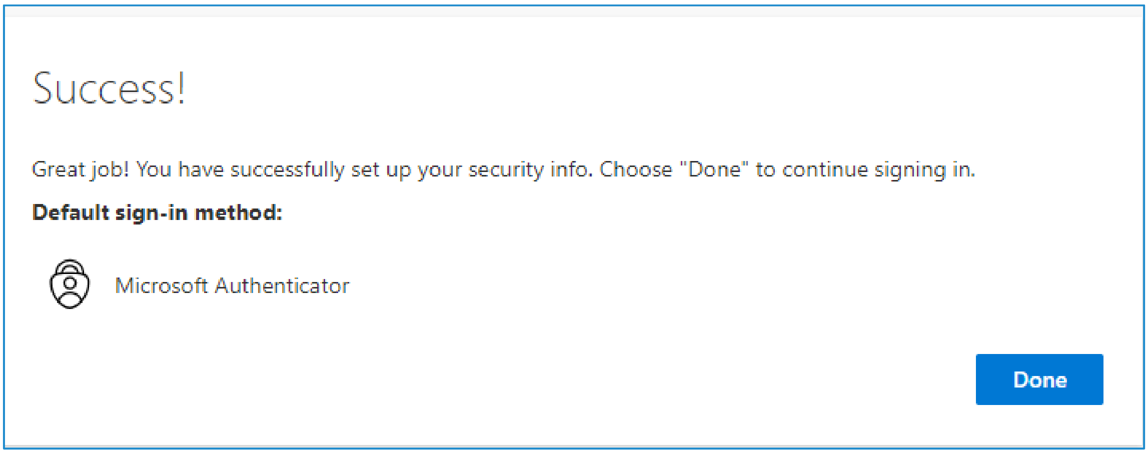
6. Entering the code correctly will complete the setup of authentication application.



Microsoft Authenticator

Notification approved

7. After selecting "Next", information about configuring the method will be displayed, and after selecting "Done", logging in will take place using the second component.



Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

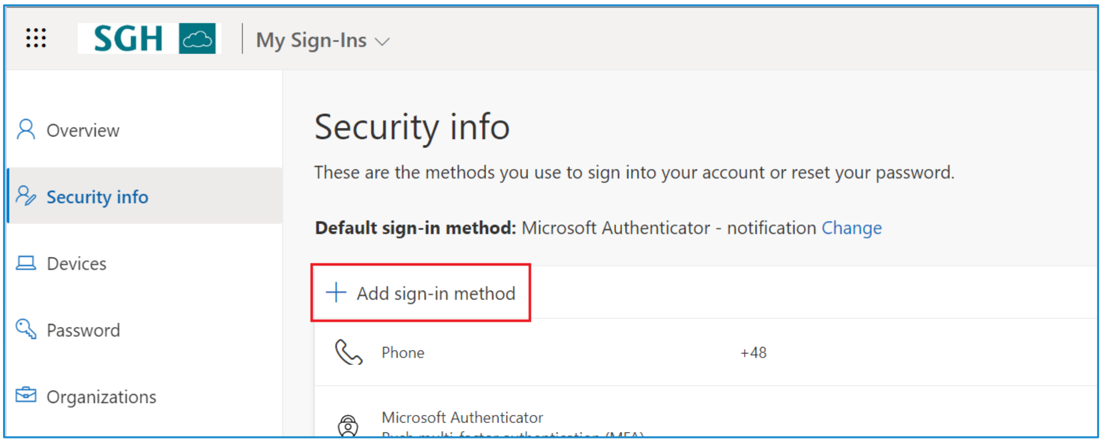
Default sign-in method:

Microsoft Authenticator

b. Configuration of phone number – MFA

Unlike authentication apps, there can only be one phone number for authentication. You can choose the option of "call back" by the machine to confirm the login or receive a verification code by SMS to enter while logging in.

1. To add a second authentication method, on the website https://mfa.sgh.waw.pl, select the "Add login method" option



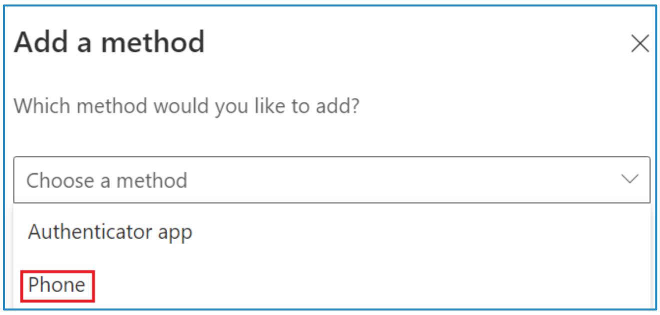
Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

Phone	+48
Microsoft Authenticator Push multi-factor authentication (MFA)	

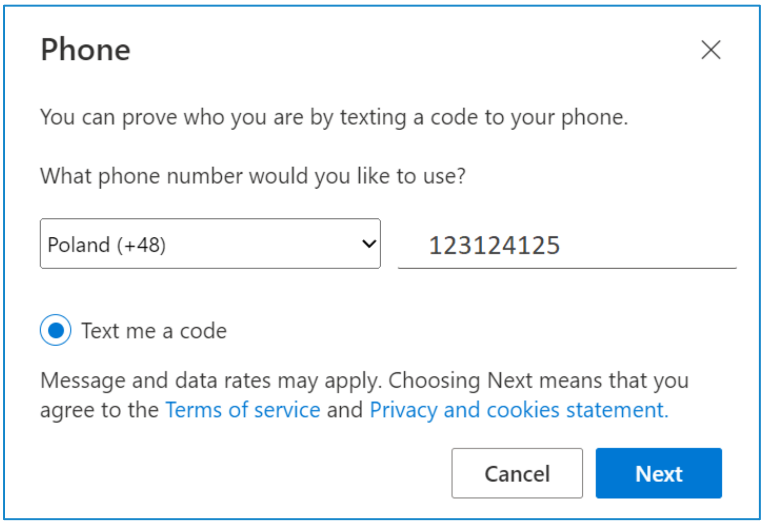
And choose “phone” option:



Add a method

Which method would you like to add?

2. After confirming, a place to enter the phone number will be displayed (unless it was previously used to recover the password - then it will appear by default)



Phone

You can prove who you are by texting a code to your phone.

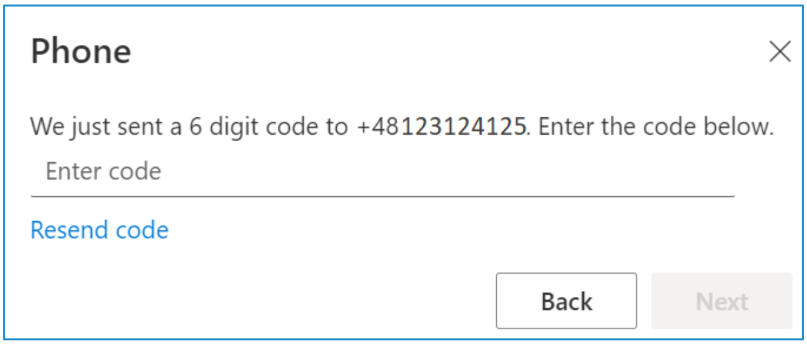
What phone number would you like to use?

Poland (+48) 123124125

● Text me a code

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

3. You must confirm by choosing “Next” to receive the SMS
4. After that a window for entering the code from the SMS will be displayed:

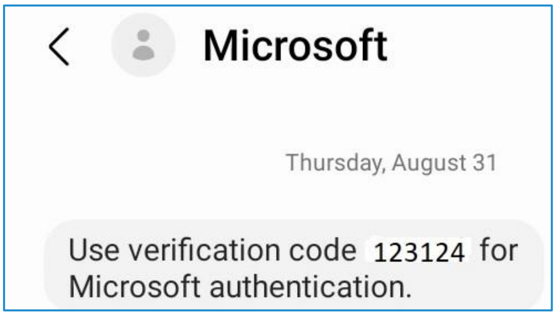


Phone

We just sent a 6 digit code to +48123124125. Enter the code below.

Enter code

5. This is how SMS message with code should looks like:

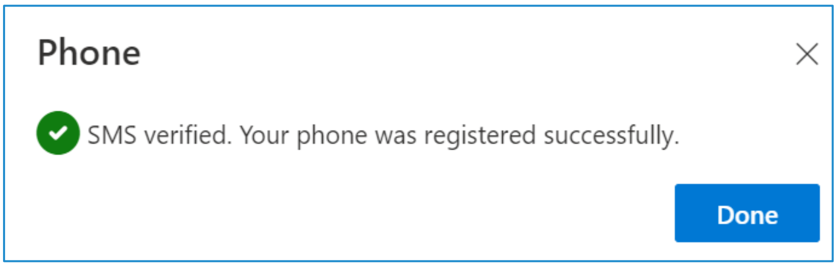


Microsoft

Thursday, August 31

Use verification code 123124 for Microsoft authentication.

6. After entering the code from SMS, confirmation of verification and registration of the phone number will be displayed:



Phone

✓ SMS verified. Your phone was registered successfully.

3. Configuring multiple authentication methods.

Every user has configured a second factor of authentication. However, it’s possible to set several authentication methods (confirmation in the application or SMS message with verifying code). The default authentication method is usually the first one that was set up.

To set several authentication methods go to https://mfa.sgh.waw.pl and configure an additional authentication option.

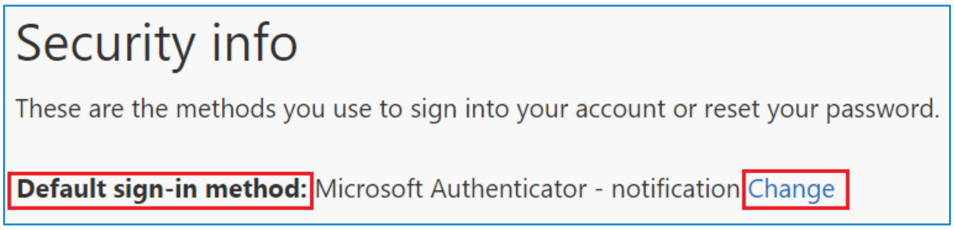
Important: No matter how many authentication factors you add, there can only be one default authentication factor. Therefore, when logging into the SGH Cloud, you will be asked to use the default authentication factor, and not one of the previously set authentication factors.

4. Change default authentication factor.

The default authentication method means that when logging in, after entering your account credentials, you will be asked to confirm your identity with this specific authentication method. If you are unable to use it, it will be possible to confirm your identity through another previously configured verification method (see point 3). You may also change the default authentication method at any time.

To change the default authentication method:

1. Go to the website https://mfa.sgh.waw.pl and log in. Next to the "Default sign-in method" option, select the "Change" option:

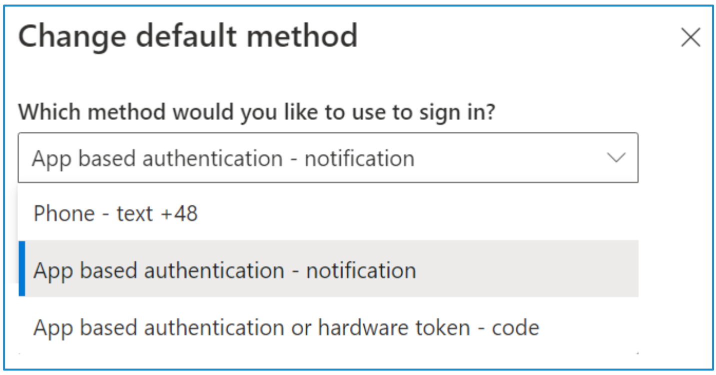


Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

2. Choose a method other than the current one and confirm your choice



Change default method

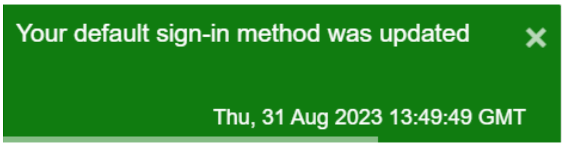
Which method would you like to use to sign in?

App based authentication - notification

Phone - text +48
App based authentication - notification
App based authentication or hardware token - code

.

3. The default method will be changed



Your default sign-in method was updated

Thu, 31 Aug 2023 13:49:49 GMT