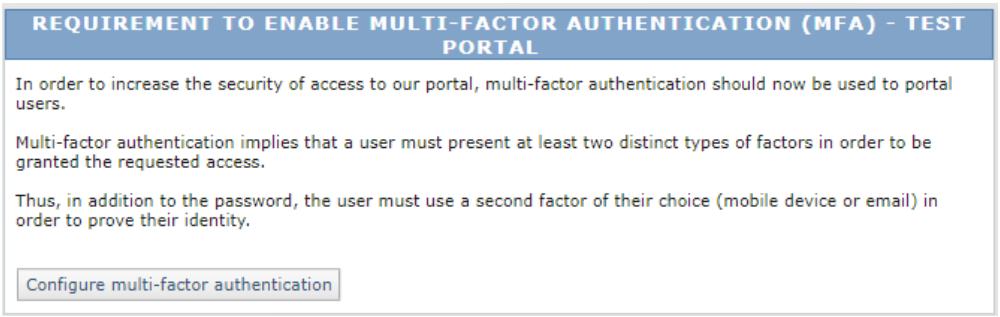
Multi-factor authentication- Campus

Contents

Multi-factor authentication requires a user to present at least two different types of factors in order to be granted the requested access. Thus, in addition to a password, the user must use a second factor of their choice (mobile device or email) to prove their identity.

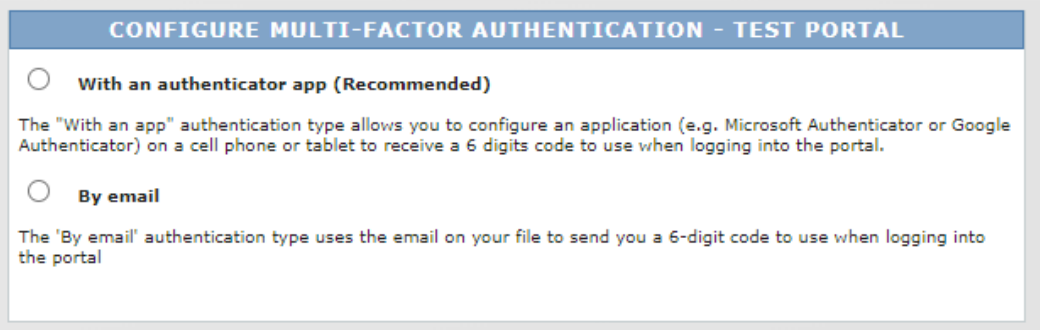
Activating multi-factor authentication

1. Log in to the portal.
2. If you haven't already set up your multifactor authentication method, the mandatory notice will appear.

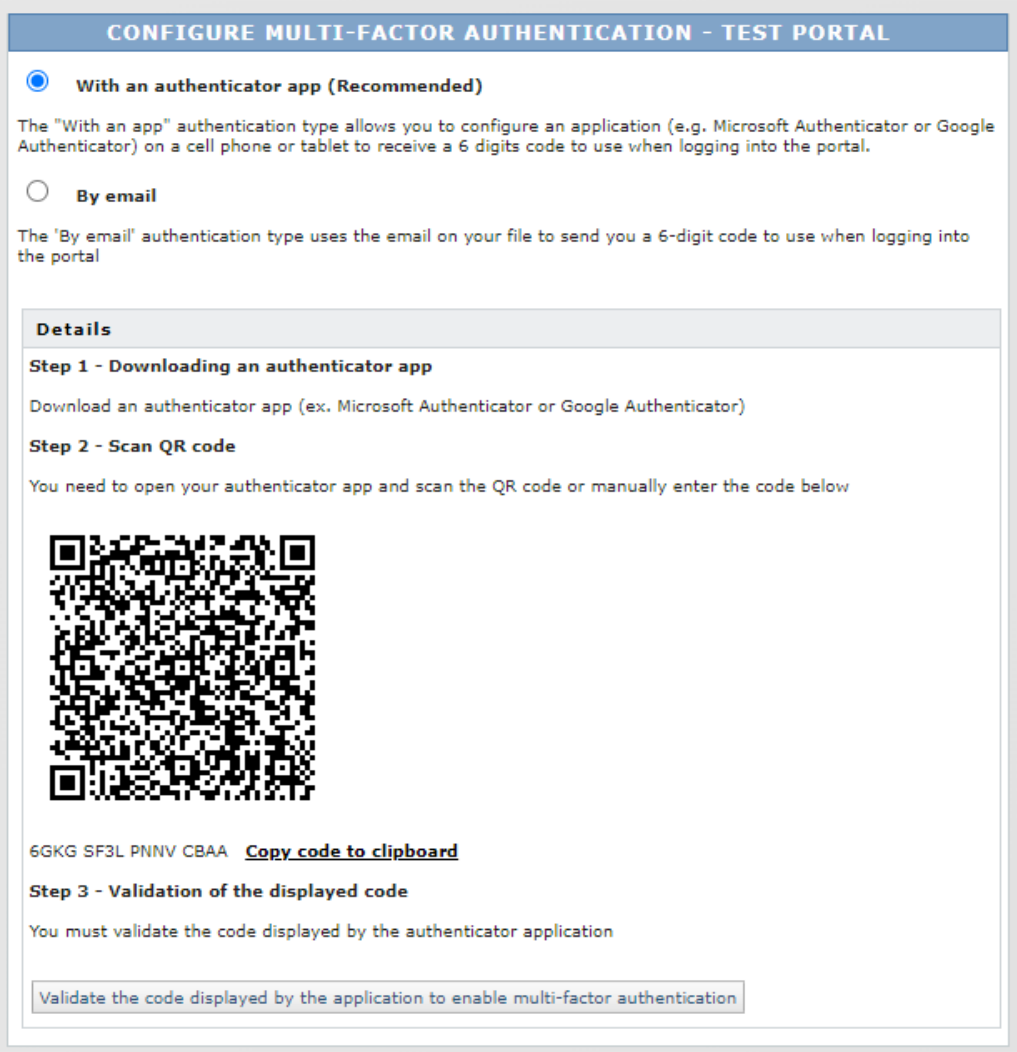


3. Click on **Configure multi-factor authentication**

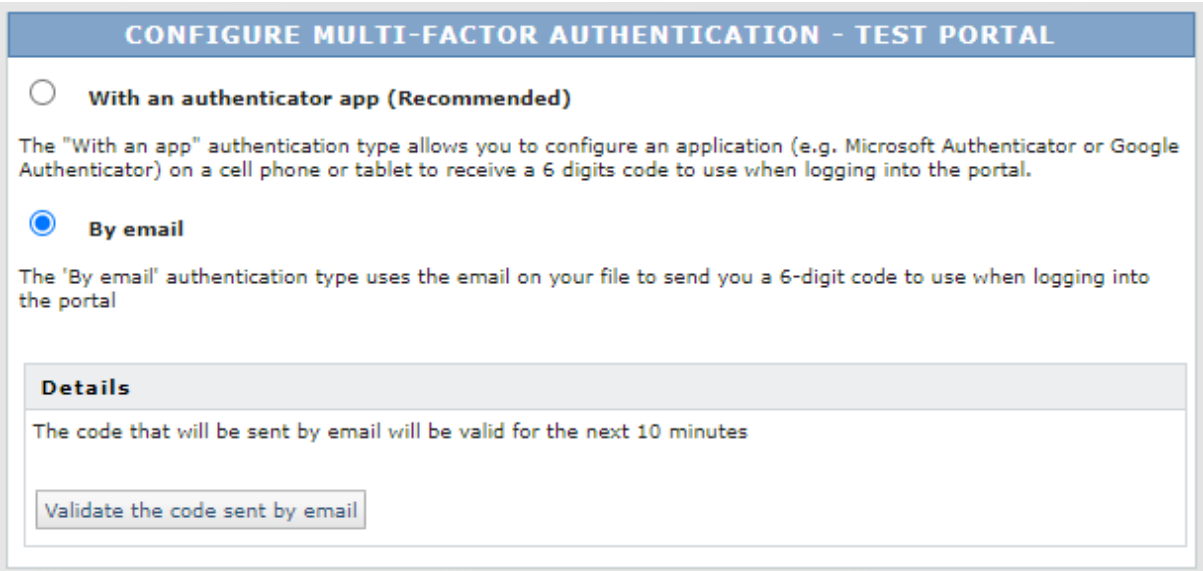
4. Select the type of authentication to configure:



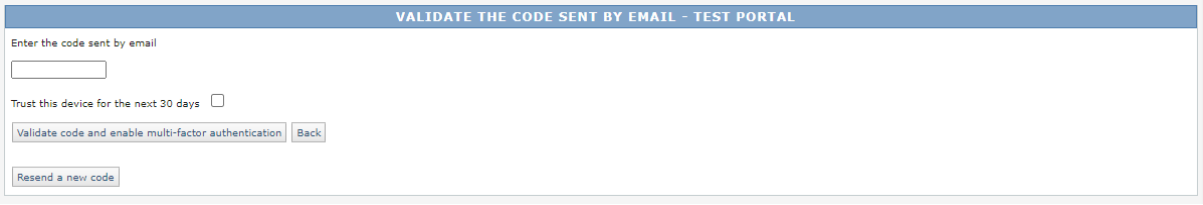
4.1. With an app: you must install Microsoft Authenticator or Google Authenticator app on your cell phone or tablet before scanning the QR code.



4.2. By email

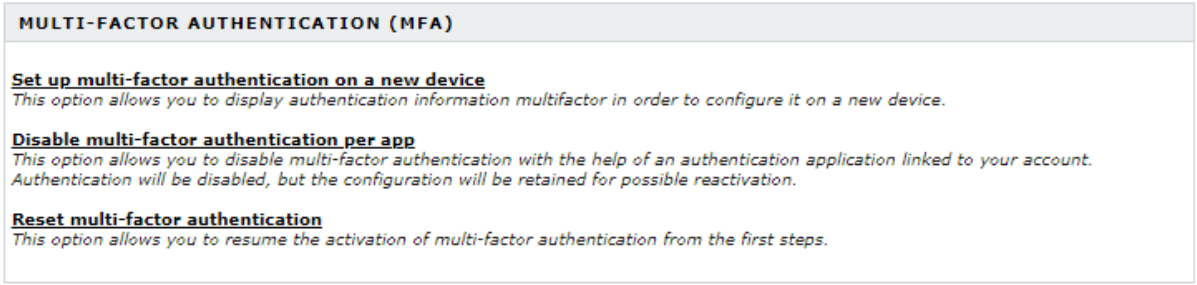


5. Validate the 6-digit code displayed in the app or received by email.



Other options

Once multi-factor authentication is activated, you can return to the **Options** service of the portal to access additional options for managing multi-factor authentication.



1. Set up multi-factor authentication on a new device

In the **Options** service of the portal, this option allows you to display the multi-factor authentication information so you can set it up on a new device.

2. Disable multi-factor authentication per app

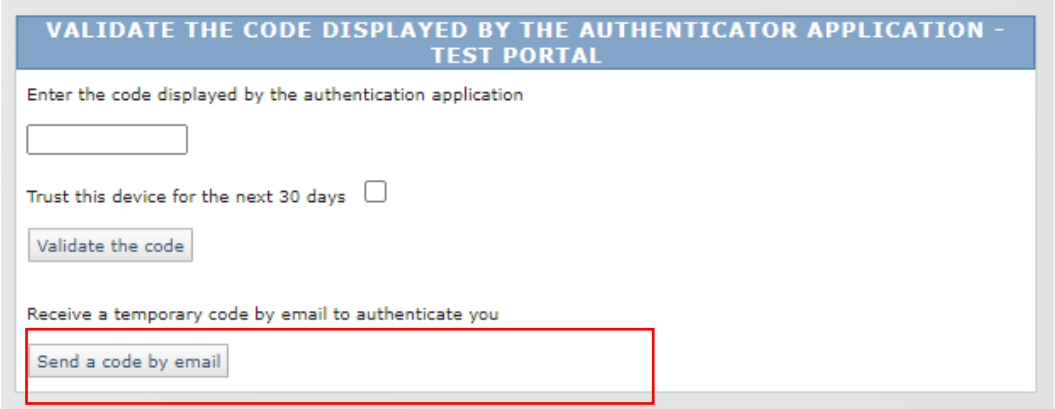
In the **Options** service of the portal, this option allows you to disable multi-factor

authentication with the help of an authentication app linked to your account. Authentication will be disabled, but the configuration will be retained for possible reactivation.

3. Reset multi-factor authentication
   In the **Options** service of the portal, this option allows you to restart the activation of multi-factor authentication from the initial steps.

What to do if you no longer have access to your authentication method?

1. If you had chosen the option of authentication with an app, when you log into the portal, the option to receive a temporary code by email is still available.



   1.1. Click on **Send a code by email**.
   1.2. Validate the 6-digit code received by email.
   1.3. You can then review the configuration of your multi-factor authentication in the **Options** service of the portal. See the section Other Options above.

2. If you chose the **option with an app and you no longer have access to it or to your email address**, or if you had chosen **the email option and no longer have access to that email address**, contact us for a request to reset your multi-factor authentication please contact us at :

   514-864-6464 Montréal area
   1-800-665-6400 toll-free