

# Multi-factor authentication- Campus

## Contents

Activating multi-factor authentication .....	1
Other options.....	3
1. Set up multi-factor authentication on a new device .....	3
2. Disable multi-factor authentication per app .....	3
3. Reset multi-factor authentication .....	4
What to do if you no longer have access to your authentication method? .....	4

*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.

**REQUIREMENT TO ENABLE MULTI-FACTOR AUTHENTICATION (MFA) - TEST PORTAL**

In order to increase the security of access to our portal, multi-factor authentication should now be used to portal users.

Multi-factor authentication implies that a user must present at least two distinct types of factors in order to be granted the requested access.

Thus, in addition to the password, the user must use a second factor of their choice (mobile device or email) in order to prove their identity.

[Configure multi-factor authentication](#)

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

4. Select the type of authentication to configure:

**CONFIGURE MULTI-FACTOR AUTHENTICATION - TEST PORTAL**

**With an authenticator app (Recommended)**

The "With an app" authentication type allows you to configure an application (e.g. Microsoft Authenticator or Google Authenticator) on a cell phone or tablet to receive a 6 digits code to use when logging into the portal.

**By email**

The 'By email' authentication type uses the email on your file to send you a 6-digit code to use when logging into the portal

- 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.

**CONFIGURE MULTI-FACTOR AUTHENTICATION - TEST PORTAL**

**With an authenticator app (Recommended)**

The "With an app" authentication type allows you to configure an application (e.g. Microsoft Authenticator or Google Authenticator) on a cell phone or tablet to receive a 6 digits code to use when logging into the portal.

**By email**

The 'By email' authentication type uses the email on your file to send you a 6-digit code to use when logging into the portal

**Details**

**Step 1 - Downloading an authenticator app**

Download an authenticator app (ex. Microsoft Authenticator or Google Authenticator)

**Step 2 - Scan QR code**

You need to open your authenticator app and scan the QR code or manually enter the code below



6GKG SF3L PNNV CBAA [Copy code to clipboard](#)

**Step 3 - Validation of the displayed code**

You must validate the code displayed by the authenticator application

Validate the code displayed by the application to enable multi-factor authentication

## 4.2. By email

CONFIGURE MULTI-FACTOR AUTHENTICATION - TEST PORTAL

**With an authenticator app (Recommended)**  
 The "With an app" authentication type allows you to configure an application (e.g. Microsoft Authenticator or Google Authenticator) on a cell phone or tablet to receive a 6 digits code to use when logging into the portal.

**By email**  
 The "By email" authentication type uses the email on your file to send you a 6-digit code to use when logging into the portal

**Details**

The code that will be sent by email will be valid for the next 10 minutes

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

VALIDATE THE CODE SENT BY EMAIL - TEST PORTAL

Enter the code sent by email

Trust this device for the next 30 days

## 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.

MULTI-FACTOR AUTHENTICATION (MFA)

**Set up multi-factor authentication on a new device**  
*This option allows you to display authentication information multifactor in order to configure it on a new device.*

**Disable multi-factor authentication per app**  
*This option allows you to disable multi-factor authentication with the help of an authentication application linked to your account. Authentication will be disabled, but the configuration will be retained for possible reactivation.*

**Reset multi-factor authentication**  
*This option allows you to resume the activation of multi-factor authentication from the first steps.*

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

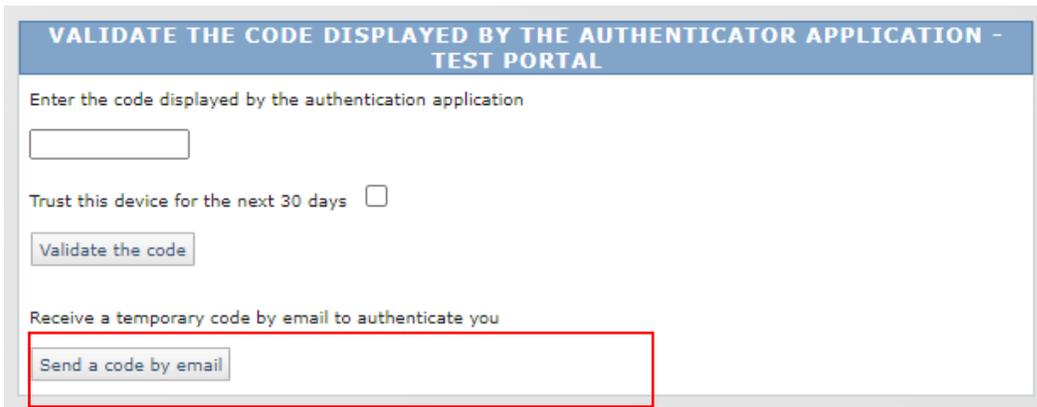
authentication with the help of an authentication app linked to your account. Authentication will be disabled, but the configuration will be retained for possible reactivation.

### 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.



VALIDATE THE CODE DISPLAYED BY THE AUTHENTICATOR APPLICATION - TEST PORTAL

Enter the code displayed by the authentication application

Trust this device for the next 30 days

Validate the code

Receive a temporary code by email to authenticate you

Send a code by email

- 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