Configuring Multi-Factor Authentication on the User Portal

Introduction

Multi-factor authentication, or MFA, adds a second layer of security to a user’s account. Currently, the only method of MFA implemented is using one-time passwords sent via email.

One-Time Passwords

The one-time password is a randomly-generated password that is sent to the user within an email. The password must be entered into the website after the regular login before the user is able to access their account.

Admin Side Configuration

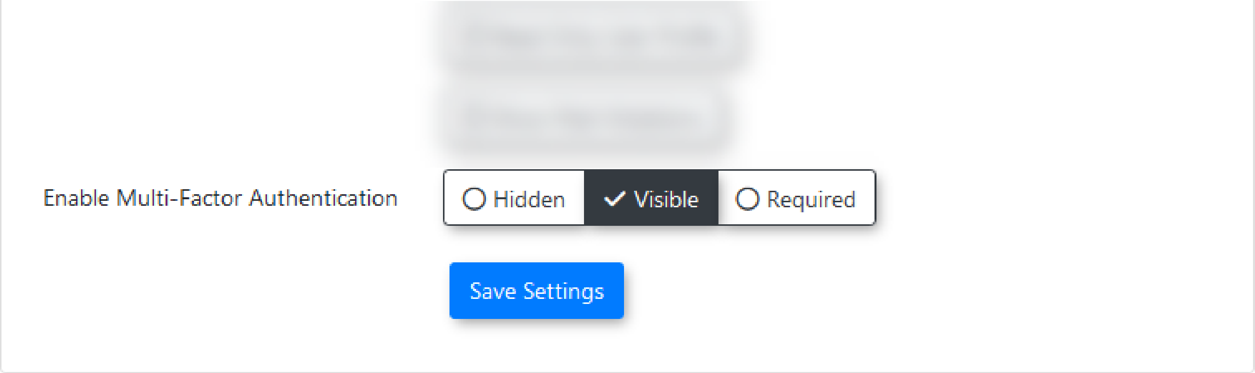
One-time passwords will not be available on a website until it is enabled within system settings.

System settings are located in the menu:

- **System Configuration → System Settings**

The relevant setting can be found under:

- **User Profile → Enable Multi-Factor Authentication**



Enable Multi-Factor Authentication ○ Hidden ✓ Visible ○ Required

The MFA setting within the system settings.

It is a ternary setting, with 3 different states:

- **Hidden** - The use of one-time passwords is disabled.
- **Visible** - The use of one-time passwords is enabled, but it is left up to the user if they want it enabled or not.
- **Required** - The use of one-time passwords is required by all users of the website.

If the use of one-time passwords is required, users who do not have it enabled on their account will be required to set up the use of one-time passwords on their account on their next login.

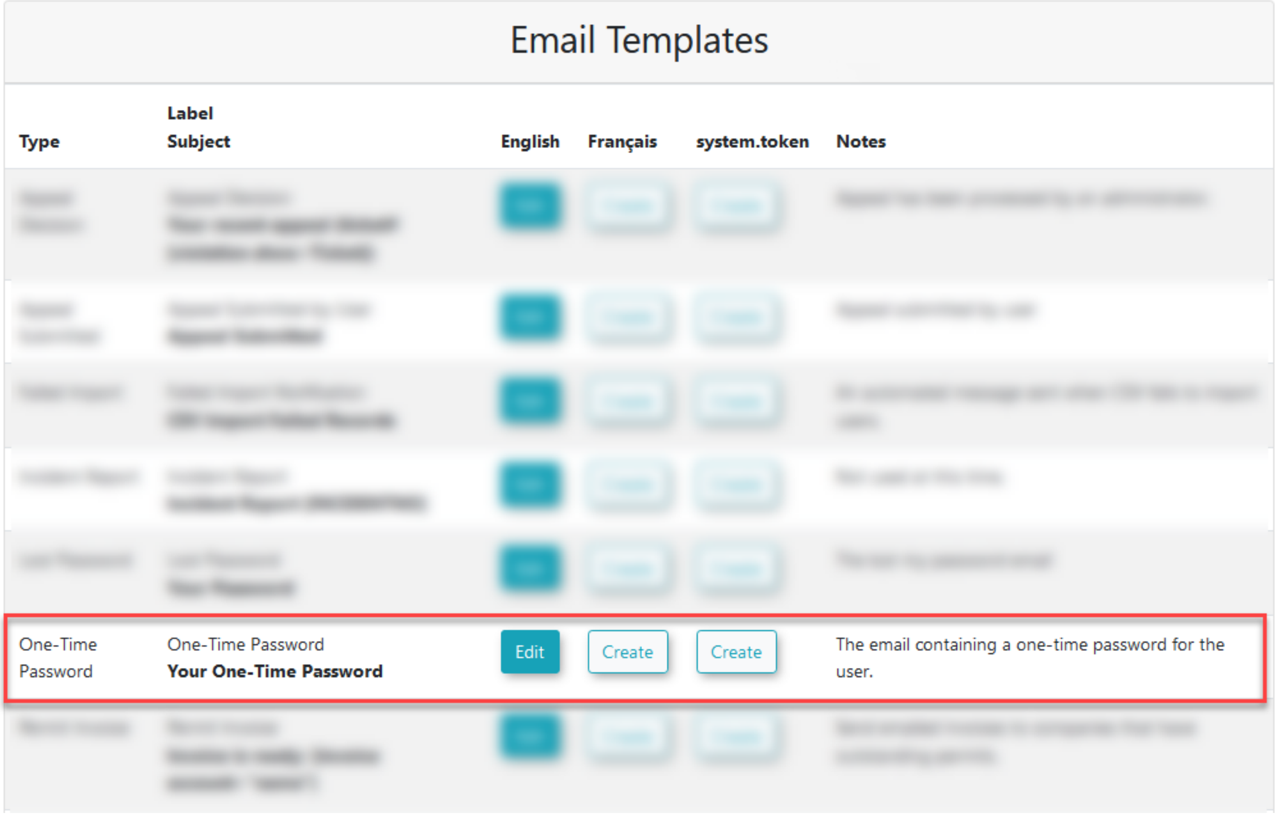
They will be redirected to the setup page until they do so.

Email Template

The content of the one-time password email that is sent to user is defined within the associated email template.

Email templates can be found under the headings:

- **System Configuration → Content & Designs → Email Templates**

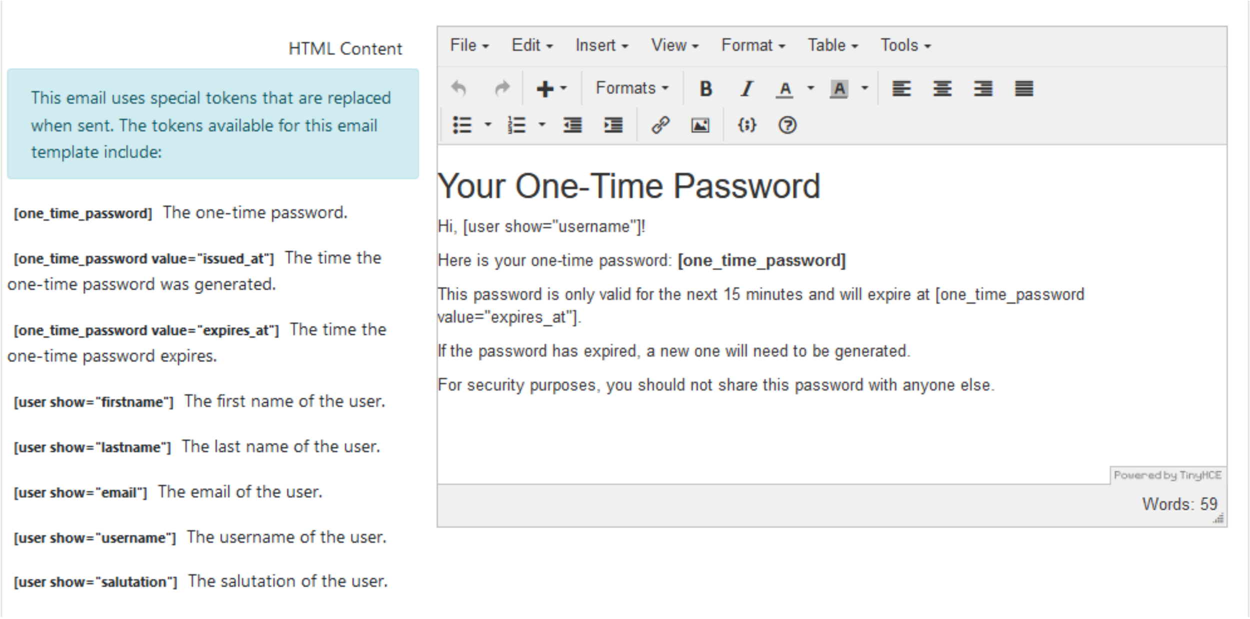


Email Templates

Type	Label Subject	English	Français	system.token	Notes
One-Time Password	One-Time Password **Your One-Time Password**	Edit	Create	Create	The email containing a one-time password for the user.

The one-time password email template.

The content of the email can be defined here.

- 

  This email uses special tokens that are replaced when sent. The tokens available for this email template include:

  [one_time_password] The one-time password.

  [one_time_password value="issued_at"] The time the one-time password was generated.

  [one_time_password value="expires_at"] The time the one-time password expires.

  [user show="firstname"] The first name of the user.

  [user show="lastname"] The last name of the user.

  [user show="email"] The email of the user.

  [user show="username"] The username of the user.

  [user show="salutation"] The salutation of the user.

  Your One-Time Password

  Hi, [user show="username"]!

  Here is your one-time password: **[one_time_password]**

  This password is only valid for the next 15 minutes and will expire at [one_time_password value="expires_at"].

  If the password has expired, a new one will need to be generated.

  For security purposes, you should not share this password with anyone else.

  The email template page.

In addition to the general user-specific shortcodes, the one-time password email template has a number of one-time password specific shortcodes related to it.

The one-time password specific shortcodes are:

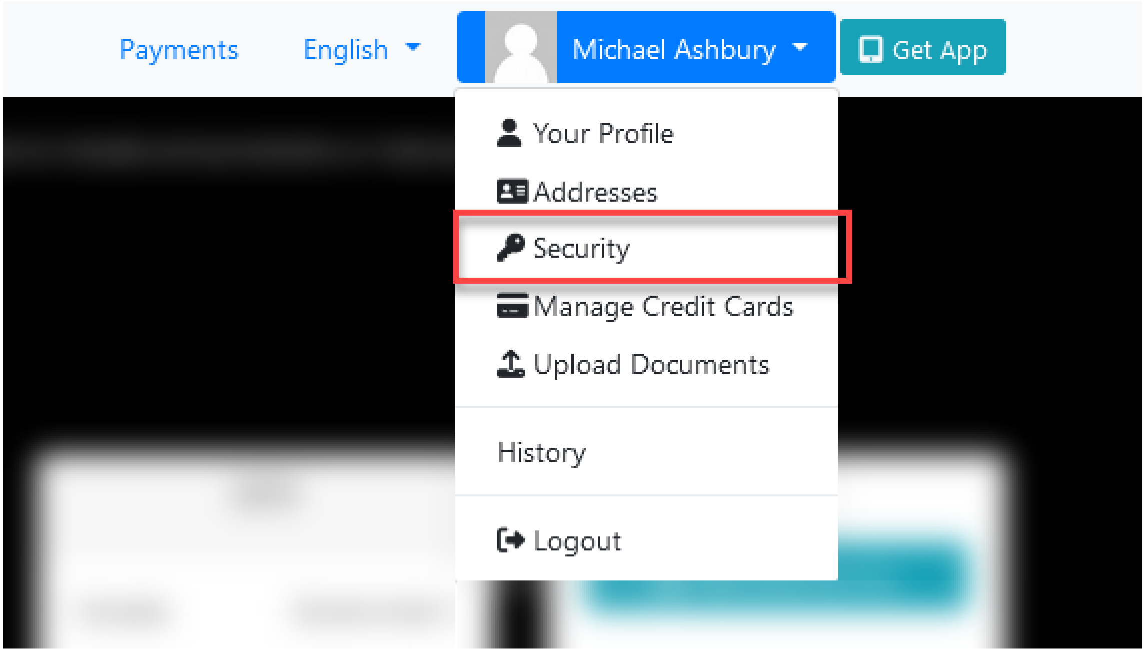
  - **[one_time_password]** The one-time password.
  - **[one_time_password value="issued_at"]** The time the one-time password was generated.

- **[one_time_password value="expires_at"]** The time the one-time password expires.

One-time passwords always expire after 15 minutes.

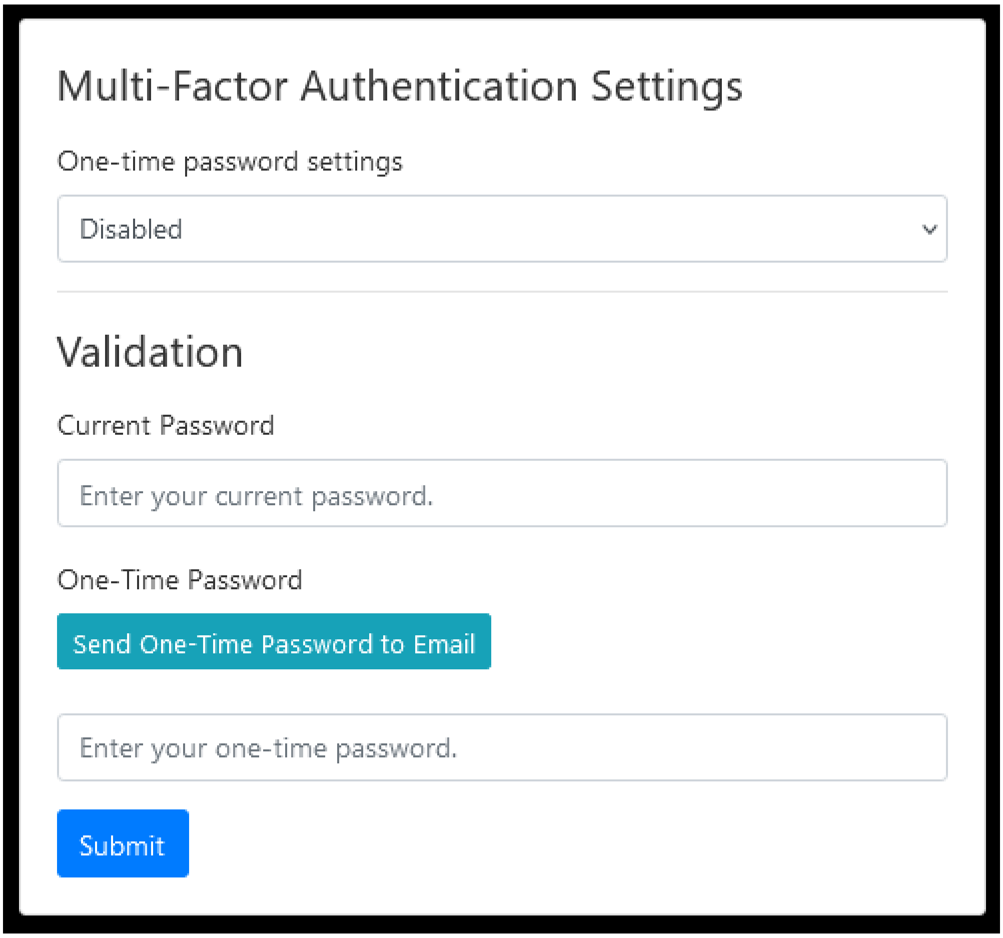
User-Side

A user can enable the use of one-time passwords from the security page, which was formerly the passwords page.



The security setting in the menu.

If MFA is enabled on the site, a section for multi-factor authentication settings will appear below the password section.
It contains a status of the user’s current settings, and a button that links to the page where settings can be managed.
Clicking on the button at the bottom of the page will open to the multi-factor authentications settings page.



Multi-Factor Authentication Settings

One-time password settings

Disabled

Validation

Current Password

Enter your current password.

One-Time Password

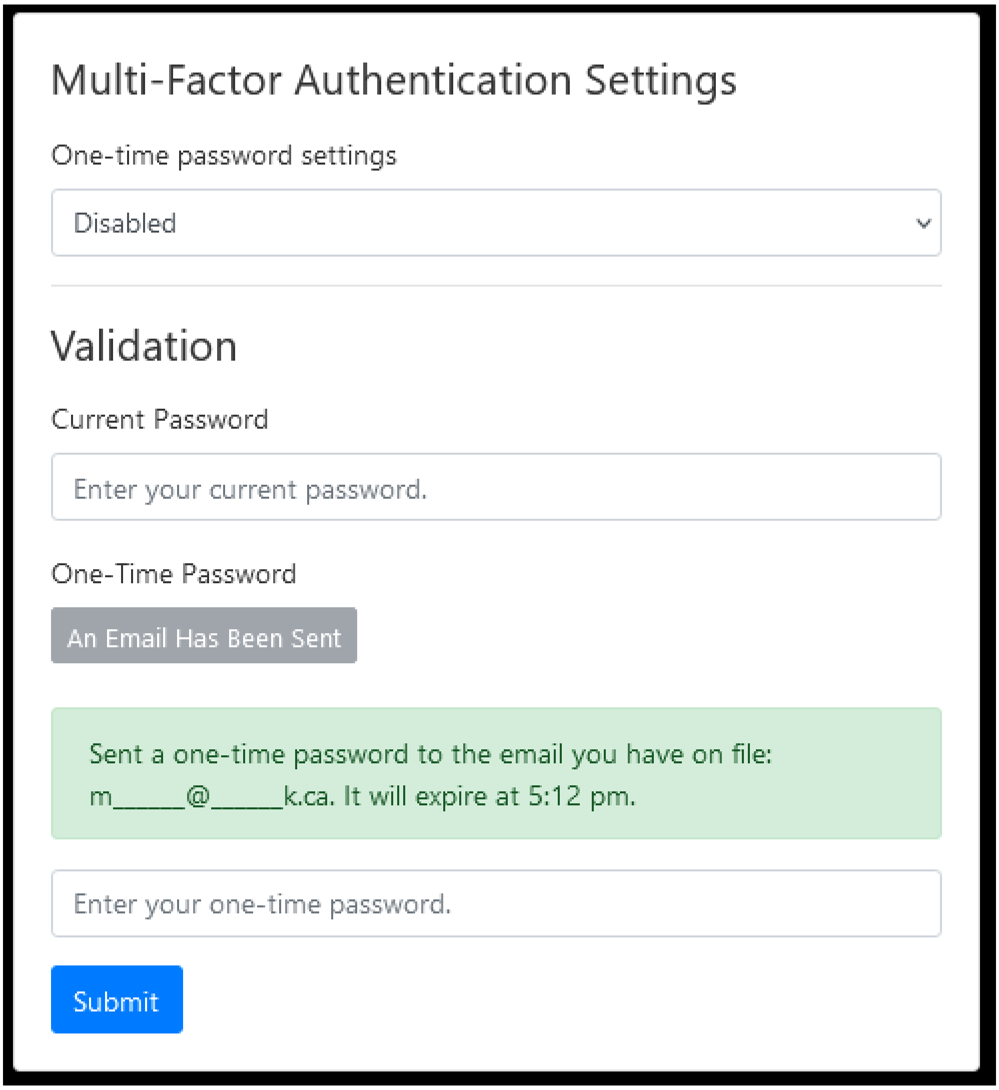
Enter your one-time password.

The multi-factor authentication settings page.

Here, the user can change their MFA settings. Currently, the only options available are to disable MFA, or to use one-time passwords.

In order to save any changes to their settings, the user will need to enter their current password and an initial one-time password.

The user can have a one-time password emailed to the email address they have on file by clicking the button to send a one-time password to their email.



Multi-Factor Authentication Settings

One-time password settings

Disabled

Validation

Current Password

Enter your current password.

One-Time Password

Sent a one-time password to the email you have on file: m_____@_____k.ca. It will expire at 5:12 pm.

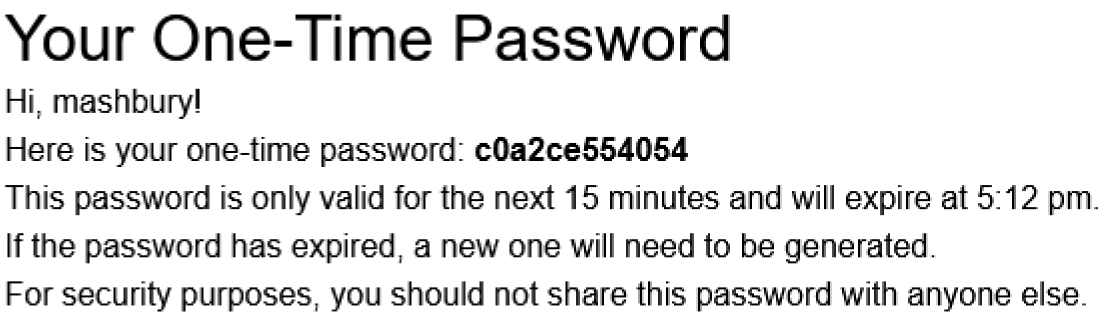
Enter your one-time password.

The message displayed after clicking the send email button.

After the button has been clicked, an email is sent containing the one-time password.

The password is only valid for 15 minutes after the point of generation, at which point it will no longer work if entered. The user will have to generate a new password after it has expired.

When a user generates a new one-time password, any unused passwords they have in the system will be rendered unusable, even if they haven’t expired yet.



Your One-Time Password

Hi, mashbury!

Here is your one-time password: **c0a2ce554054**

This password is only valid for the next 15 minutes and will expire at 5:12 pm.

If the password has expired, a new one will need to be generated.

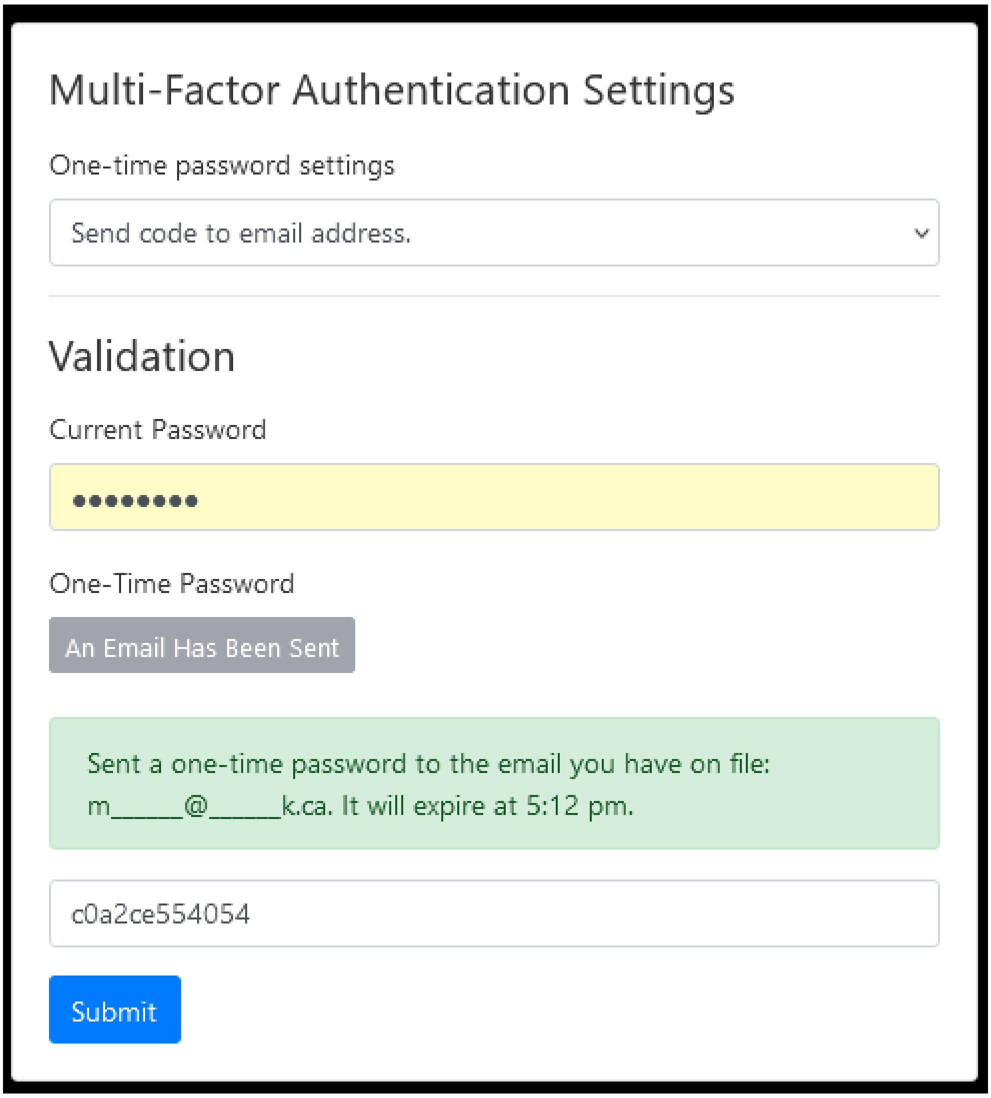
For security purposes, you should not share this password with anyone else.

An example of a one-time password email.

The email will use the formatting of the template that was set up for one-time passwords.

The one-time password must be entered into the box below the current password box.

By pressing the submit button, the user will now be able to update their MFA settings.



Multi-Factor Authentication Settings

One-time password settings

Send code to email address.

Validation

Current Password

●●●●●●●●●

One-Time Password

Sent a one-time password to the email you have on file: m_____@_____k.ca. It will expire at 5:12 pm.

c0a2ce554054

Entering a one-time password.

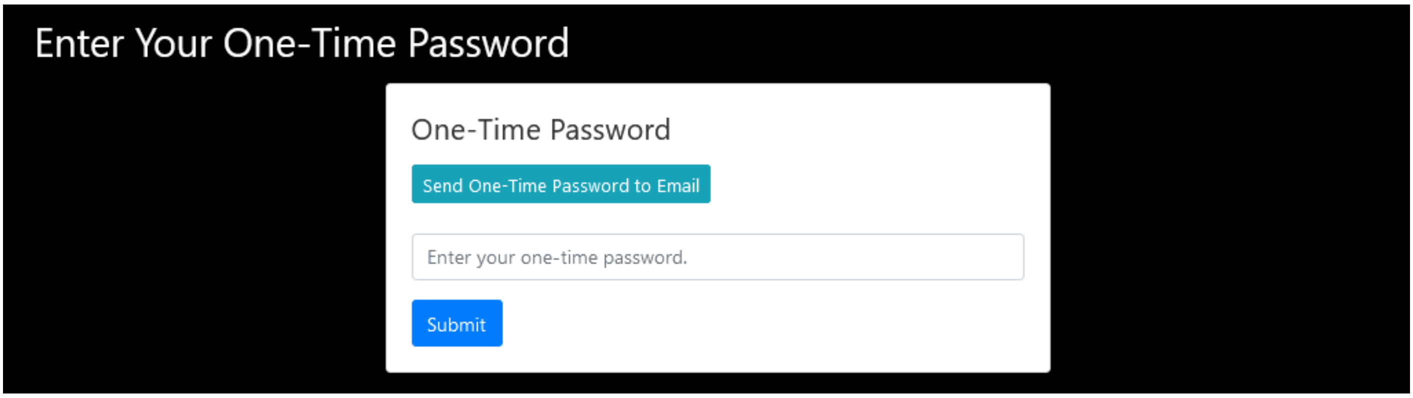
Logging In

When a user has one-time passwords enabled on their account, they will be prompted after every subsequent regular login to enter a one-time password before they can access the site.

The username and password are entered as normal, then the one-time password screen is shown. The user will be redirected to this page whenever they try to access a page other than one of these:

- **/login** - the login page.
- **/logout** - the logout page.
- **/one_time_password** - the one-time password enter screen.
- **/account/send_email** - the one-time password send email endpoint.
- **/account/multiauth** - the user account multi-auth settings page.

If the user does not have one-time passwords setup on their account but the site has one-time passwords set as required on the site, the user will instead be redirected to the multi-authentication setup page. They will not be able to move away from this page until they complete the setup.


Enter Your One-Time Password
One-Time Password
Send One-Time Password to Email
Enter your one-time password.
Submit

The one-time password screen.

The page works just like the setup, with a button to send a new one-time password to the user’s email address.

After the user enters the one-time password and submits, they will be able to proceed to the rest of the website as normal.

The state of their one-time password verification is stored in the local storage of their session data. If the local storage is cleared, they fill have to enter another one-time password.

The data does not persist across web browsers, meaning if the user will have to enter a new one-time password if they try to login using another browser or device.

Image not found or type unknown

Revision #3
Created 9 October 2024 08:02:29 by Co-op Student
Updated 6 December 2024 10:22:49 by Shannon Jones