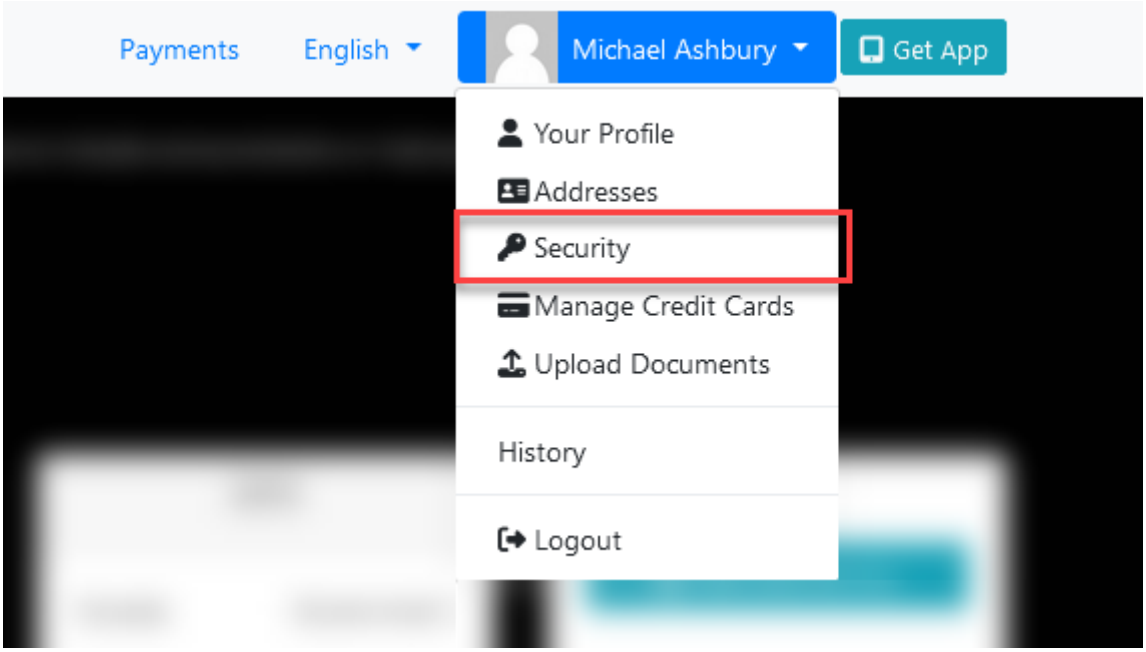
Multi-Factor Authentication

User-Side

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

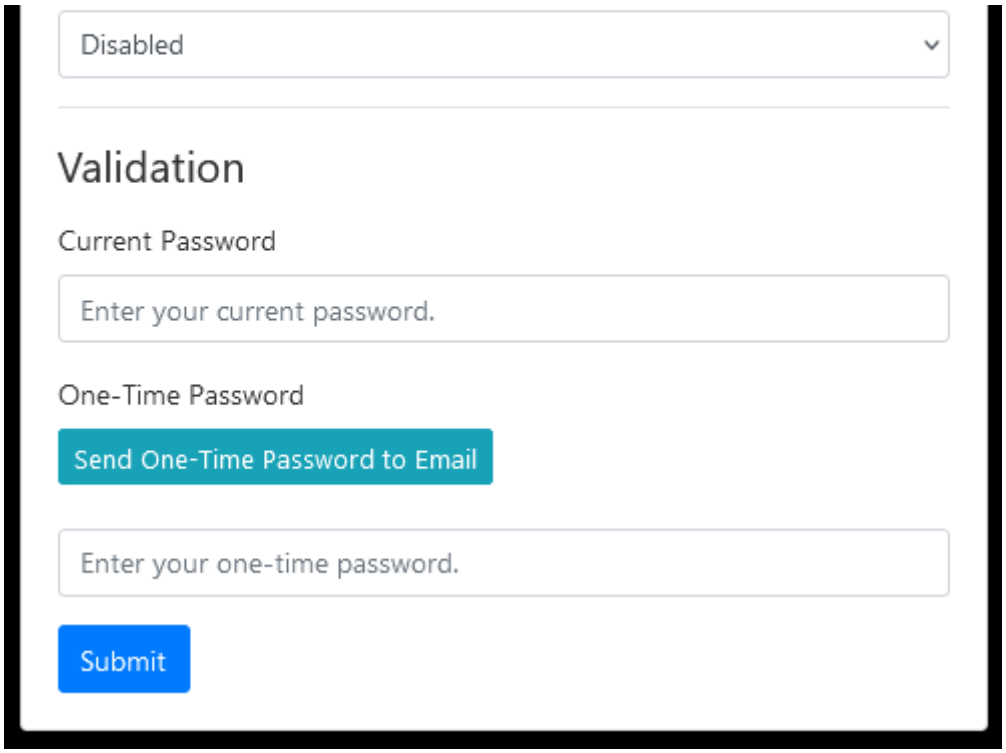


The security setting in the menu.

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.

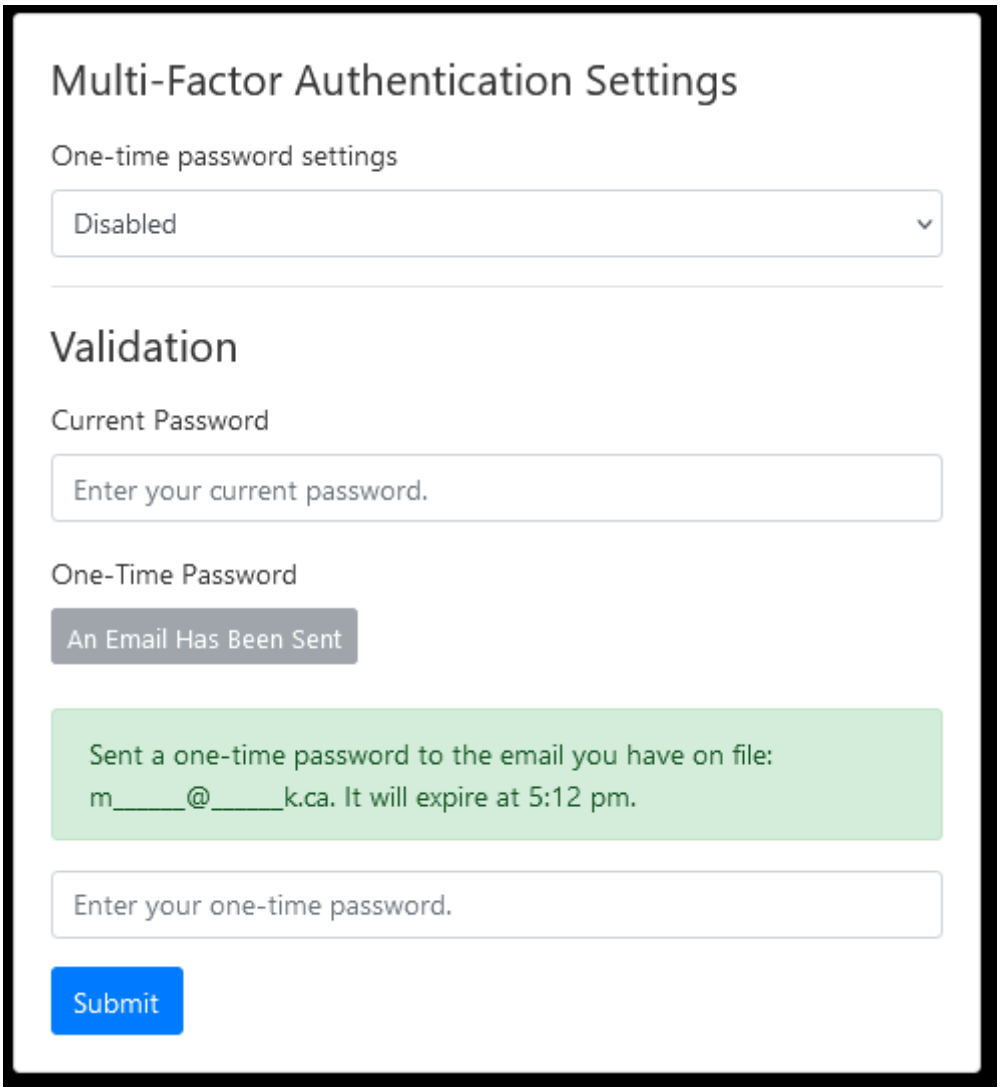


The multi-factor authentication settings page.

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.

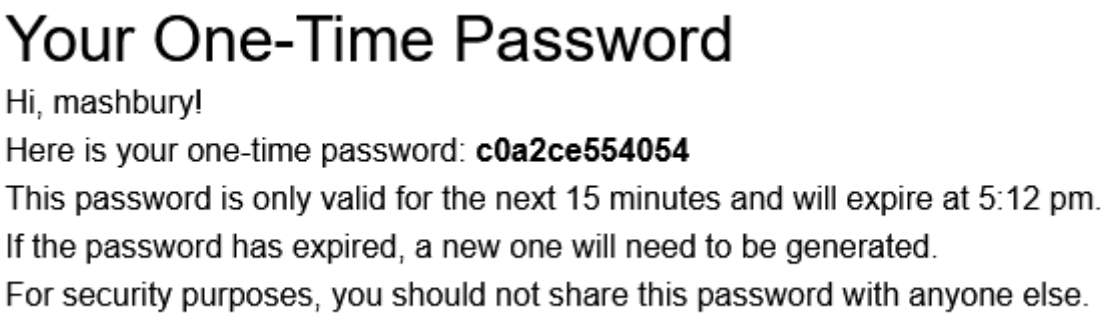


The message displayed after clicking the send email button.

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.

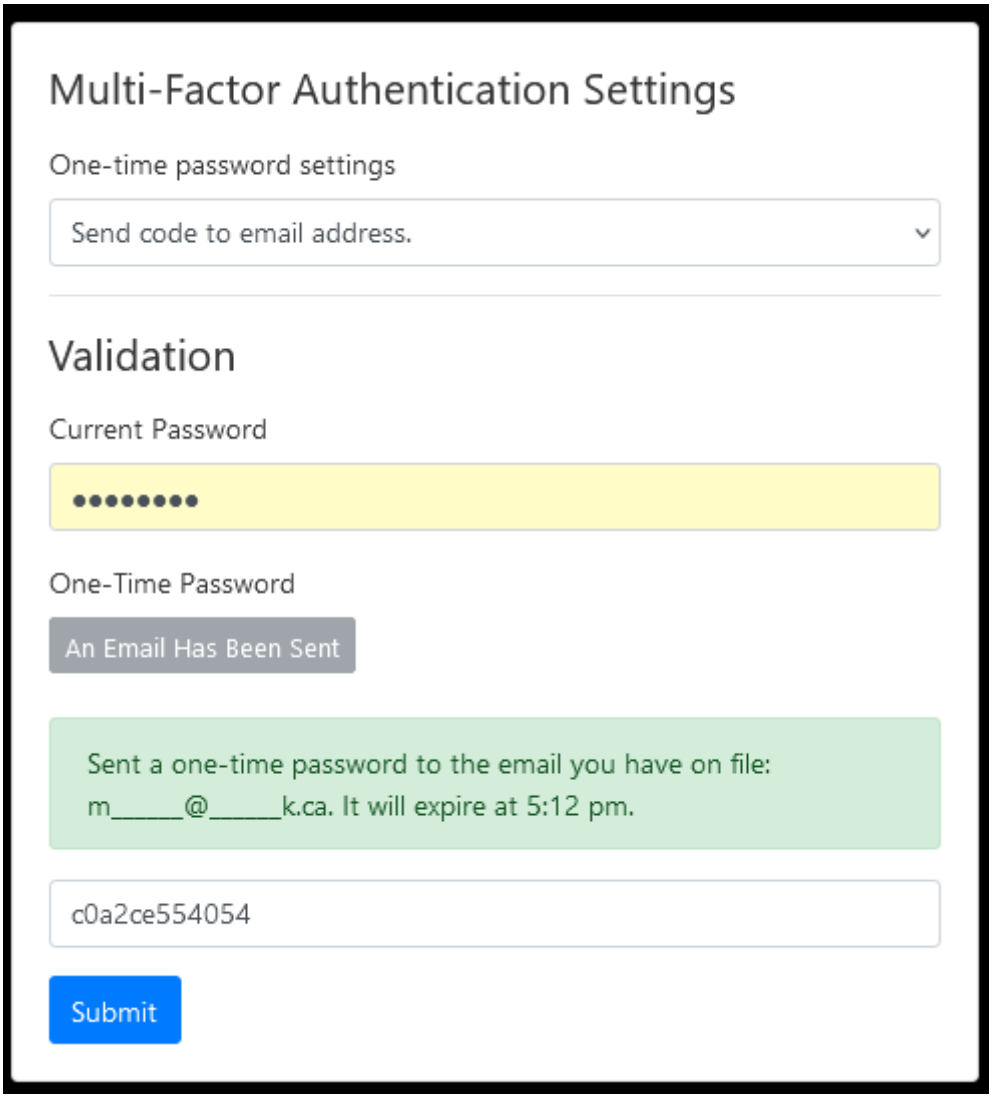


An example of a one-time password email.

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.



Entering a one-time password.

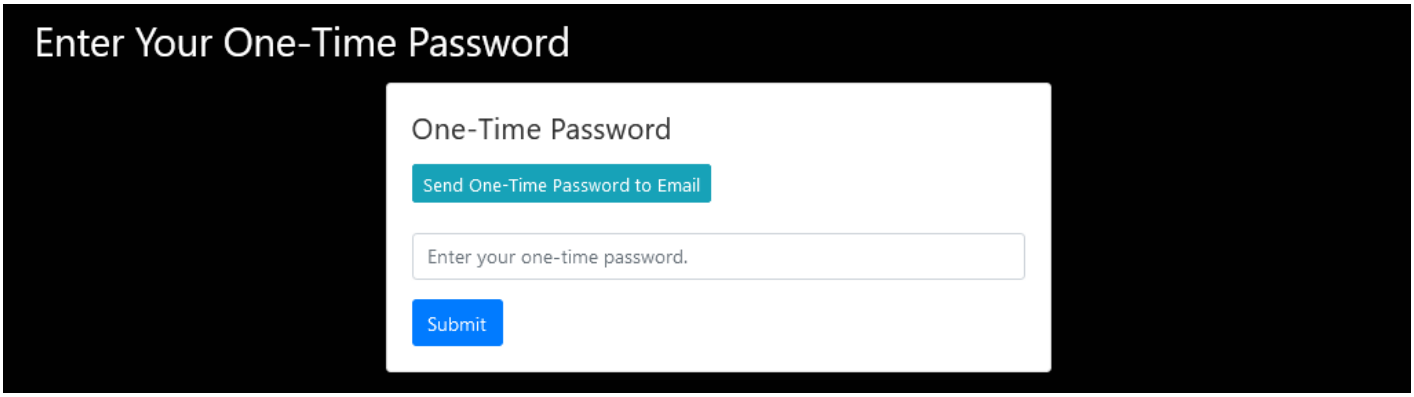
Logging In

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.



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.

Revision #1
Created 9 October 2024 08:10:54 by Co-op Student
Updated 9 October 2024 08:11:19 by Co-op Student