Tokens for Enhanced CWL

Guidelines for using hardware tokens for CWL multi-factor authentication

Table of Contents

Background

As part of our ongoing effort to enhance cybersecurity, UBC introduced Enhanced CWL (eCWL: multifactor authentication) to all faculty and staff, effective **May 31, 2019** for the Okanagan campus.

UBC applications that require a CWL for access, in addition to a username and password, may now also ask to verify user identity using a secondary method to validate logins (based on the risk context of the specific authentication request). For more information about the project, please visit the eCWL page at https://privacymatters.ubc.ca/enhancedcwl.

Note for student employees: To improve the user experience, and for auditing and security purposes, UBC requires users to have only one CWL account. Therefore if a student is hired as an employee they will be required to use eCWL to login to all UBC applications which require CWL (including those not related to their employment) until they are no longer classified as an employee.

This document provides more information about hardware tokens for eCWL which some employees may require to properly fulfill their employment appointment.

Hardware Tokens

When may a hardware token be necessary?
- If your appointment requires you to be away from your desk frequently
- If you do not have a stationary work location equipped with a landline number
- If your appointment requires you to be in locations that do not allow the use of cellular phones
- If you do not have a 'smart' cellular phone or tablet which can download mobile apps

When may a token be preferable over the downloadable app?
- If you do not want to use a personal cellular phone or tablet to download
- If you wish to have your second factor of authentication separate from any of your other devices

What types of tokens are available?
There are two types of tokens available for purchase, OTP tokens and USB Tokens.
- OTP (one-time passcode) tokens generates a one-time six digit passcode which you will manually enter and cost $10.

- USB style tokens will automatically fill the six digit passcode field when plugged into the USB port of your device and cost $25.

Where can you get a hardware token?

- If you would like to purchase a token for yourself as a personal preference, you can visit the UBCO Bookstore. OTP Tokens are available for $10 and USB Tokens are available for $25.
- If a hardware token is necessary to properly fulfill your current appointment, you may be able to obtain a token through your department by speaking to your manager.
  - **Note**: Tokens **cannot be shared** between multiple users at the same time but must be registered and associated to a single employee's CWL. If an employee is using a token supplied by their department, they must de-activate the token from their CWL once their employment term ends.

How to associate a Token with eCWL

- Using your CWL username and password, login to the "Associate OTP Token with CWL Account" page at

  https://mfadevices.id.ubc.ca/secure/tokens.php

- Enter the serial number on the back of the Token into the form and click "**Submit Token ID**" to associate the token with your CWL.
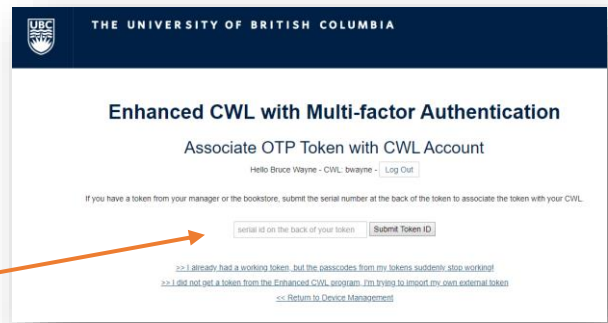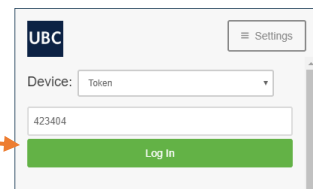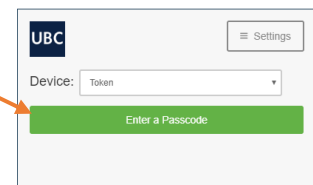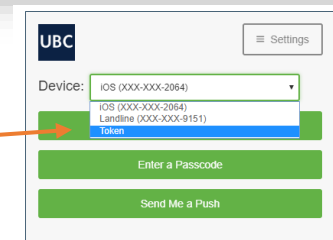
How to use a Token for eCWL

- Use the drop down Device menu to select "Token".

- Click on the green "Enter a Passcode" button.

- **For <u>OTP Tokens</u>:**
  - Turn Token "on" (click large red circle on left side).

  - Enter six digit number on Token screen.
  - Click green "Log In" button.

- **For <u>USB Tokens</u> (with tokens inserted in device's USB port):**
  - Turn Token "on" by touching the metal circle on the device handle.
  - The passcode is then automatically entered.

IMPORTANT: If your **department loans** you a token it should be removed from your list of associated eCWL devices and returned to the department at the end of your appointment.

How to REMOVE a Token from eCWL

- Using your CWL username and password, login to the CWL Account page at https://mfadevices.id.ubc.ca/secure

- Click on blue settings cog next to Token.

- Click on "Delete Device".

- Click on the red "Remove" button.