Generate bypass codes for UTOR Multi-Factor Authentication (MFA)

The University of Toronto will be mandating dual-factor authentication for its systems in 2023. Students will need access to their devices in order to complete the double authentication. This might create a conflicting policy for your activity. For example, to login to Quercus, the student will need to authorize the login via their call phone - but if you have not allowed cell phone use, you might run into issues.

The bypass codes allow users to proactively generate (and save) codes that act as the second factor (instead of a device) for MFA authentication. If you have a policy where students will not be able to access their phones, we recommend sharing instructions on how to generate bypass codes prior to the activity.

For up-to-date details, we recommend that you review the UTORMFA FAQs.

1. How to download bypass codes for UTOR MFA

1. Visit the UTOR MFA Bypass website to generate bypass codes. Codes can be generated in advance (and printed/saved) but each code is one time only use (OTO).

2. How to use UTOR MFA bypass codes for activities

1. After generation, instruct students to bring their bypass codes to the activity (e.g., printed or written down).