# Enrolling in Multi-factor Authentication (MFA)

As a WECC.org user, you may be granted access to certain secure portions of WECC.org that contain confidential information or restricted collaborative community sites. Accessing these portions of WECC.org requires another authentication factor in addition to a username and password.

## Choosing A Second Factor for MFA

Once the WECC administrative services team has assigned your WECC.org user account to the correct access group, login to WECC.org using your previous username and password. You will then see three potential options for your second factor: Google Authenticator (this is a generic, time-based one-time password (TOTP) and should work with any TOTP application, not just Google Authenticator), the Okta Verify app, and ‘Security Key or Biometric Authenticator’ (FIDO2/WebAuthn/Passkeys).

A screenshot of a computer

Description automatically generated

### Google Authenticator

As a second factor, the Google Authenticator option is best used on your mobile device with a camera. However, it also works with desktop browser extensions, like those from Bitwarden and 1Password for Chrome, Firefox, and Edge, without the need for a mobile device. Google Authenticator will work with almost any multi-factor authentication application, not just Google Authenticator, including Microsoft Authenticator, Authy, Bitwarden, Apple ID iCloud Keychain, and others. To enroll:

#### **OPTION 1 – Mobile Device**

1. Click **Set up** under Google Authenticator.

A screenshot of a computer

Description automatically generated

1. Scan the QR code with the MFA mobile app of your choice. Then click **Next**.

A screenshot of a qr code

Description automatically generated

1. Enter the six-digit code assigned to the account in the MFA app (changes every 30 seconds) and click **Verify**.

A screenshot of a computer

Description automatically generated

1. You will see an option to enroll additional factors. Since you have already enrolled in a second factor, skip this step and click **Continue**.

A screenshot of a phone

Description automatically generated

1. You will now have access to WECC.org with elevated permissions and access.

#### **OPTION 2—Browser**

As an alternative to using a mobile device, such as a phone or tablet, many popular password managers offer browser extensions for Chrome, Firefox, and Edge, that can provide QR code-based codes like their mobile app counterparts. Popular options include [Bitwarden](https://bitwarden.com/help/integrated-authenticator/#tab-browser-extension-4eWjy5G0QLbgxyLIzd91g8), [1Password](https://support.1password.com/one-time-passwords/), and [Apple ID iCloud Keychain](https://discussions.apple.com/docs/DOC-250007756)**.** The following is an example of how to use the Google Authenticator option without a mobile device, using only the Bitwarden Chrome extension (paid subscription required). The process will be similar in most other browser extensions:

1. [Install the Bitwarden Chrome extension](https://chromewebstore.google.com/detail/bitwarden-password-manage/nngceckbapebfimnlniiiahkandclblb?hl=en-US&utm_source=ext_sidebar), (**NOTE: this functionality requires an active, paid subscription to Bitwarden**).
2. Log into your existing Bitwarden account, or sign up for a new account. The Bitwarden extension icon will be blue and white when it is active and ready to enroll MFA QR codes:

A screenshot of a computer

Description automatically generated

1. Log into WECC.org using your username and password.
2. Click **Set up** under Google Authenticator.

A screenshot of a computer

Description automatically generated

1. Once you see the QR code, click **Add a login** to create a new entry in Bitwarden.

A screenshot of a computer

Description automatically generated

1. Under “Authenticator key (TOTP),” click the **camera icon**, which will scan the current web page for QR codes.

A screenshot of a login screen

Description automatically generated

1. Click **Save**. Select **login.wecc.org** in the logins list. Click **Verification code (TOTP)** and copy the code to the blank field in the web page. Click **Verify**.

A screenshot of a computer

Description automatically generated

1. You are now enrolled.

#### **OPTION 3—KeePassXC, desktop software**

[KeePassXC](https://keepassxc.org/) is a powerful, advanced, and free password manager and MFA code generator available for Windows, MacOS, and Linux. In addition to managing passwords, you can use KeePassXC to generate MFA codes for WECC.org. To use KeePassXC for MFA in WECC.org, install KeePassXC. Create a new entry for login.wecc.org, then do the following:

1. Right-click the selected entry for login.wecc.org and select **TOTP**, then **Set up TOTP**.

A screenshot of a computer

Description automatically generated

1. Sign into WECC.org using your registered username and password. Click **Set up** under Google Authenticator.

A screenshot of a computer

Description automatically generated

1. When you see the QR code, click **Can’t Scan?**

A screenshot of a qr code

Description automatically generated

1. Copy the code presented in the box. Click **Next**.

A screenshot of a computer screen

Description automatically generated

1. In KeePassXC, copy the code from login.wecc.org into the **Secret Key** field. Click **OK**.

A screenshot of a computer program

Description automatically generated

1. Right-click the entry for login.wecc.org. Select **TOTP**, then **Show TOTP**.

A screenshot of a computer

Description automatically generated

1. You will see a six-digit TOTP MFA code generating every 30 seconds. Click **Copy**.

A screenshot of a computer

Description automatically generated

1. Paste the code into the text box in login.wecc.org. Click **Verify**.

A screenshot of a computer

Description automatically generated

1. You will see an option to enroll additional factors. Skip this step and click **Continue**.

A screenshot of a security method

Description automatically generated

### Okta Verify

Okta Verify is a multi-platform MFA application available for major operating systems including Android and iOS. The setup is similar to the first option, Google Authenticator. The difference is that Okta Verify can send mobile push notifications for verification, removing the need to enter rotating six-digit codes. To set up Okta Verify as your second factor:

1. Download and install the Okta Verify application for iOS <https://apps.apple.com/us/app/okta-verify/id490179405> or Android <https://play.google.com/store/apps/details?id=com.okta.android.auth>
2. Click **Set up** under Okta Verify in the browser window where you have logged into WECC.org

A screenshot of a computer

Description automatically generated

1. Open the Okta Verify app on your mobile device, tap the ‘**+**’ button, then scan the QR code.

A screenshot of a qr code

Description automatically generated

1. Click **Continue** on the next screen to skip the enrollment of any additional factors. You will be redirected to WECC.org with elevated permissions and access.
2. On your next logon, you will see an option to “Enter a code” through Okta Verify, or “Get a push notification” through Okta Verify. Click **Select** next to ‘Get a push notification’. On your mobile device, tap the push notification. Then tap **Yes, it’s me**.

A screenshot of a computer

Description automatically generated

1. You are done! You will be redirected to WECC.org.

### Security Key or Biometric Authenticator

WECC.org supports FIDO2/WebAuthn/Passkeys through the option “Security Key or Biometric Authenticator.” This might be the best option if you are already using FIDO2/WebAuthn/Passkeys or use a security key such as the Yubikey or Google Titan Security Key. To make this method your second factor:

1. Log into WECC.org, then click **Set up** under “Security Key or Biometric Authenticator.”

A screenshot of a computer

Description automatically generated

2) Click **Set up** on the next window.

A screen shot of a computer

Description automatically generated

3) Click **OK** in the next window.

A screenshot of a computer error

Description automatically generated

#### **OPTION 1—iOS device or Android Device**

If you would like to use this option with an iPhone, iPad, or Android device, follow the instructions below. If you would like to use a hardware security key such as the Yubikey or Titan Key, skip to option 2:

1. Click **iPhone, iPad, or Android device**, then click **Next**.

A screenshot of a computer security

Description automatically generated

1. Click **Turn on Bluetooth** (also ensure that Bluetooth is enabled on your mobile device)

A screenshot of a computer

Description automatically generated

1. Scan the displayed QR code with your mobile device’s passkeys-compatible MFA application.

A qr code on a black background

Description automatically generated

1. Click **OK** to save the passkey to your mobile device.

A screenshot of a computer security

Description automatically generated

#### **OPTION 2—Hardware Security Key**

In lieu of an Android or iOS device, you can use a hardware security token such as a Yubikey or Google Titan Security Key. To get started using a hardware security key:

1. Click **Security** **key**, then click **Next**.

A screenshot of a computer security

Description automatically generated

1. Click **OK** to confirm security key setup.

A screenshot of a computer security system

Description automatically generated

1. Click **OK** to continue setup. Ensure that your security key is connected to your computer.

A screenshot of a computer

Description automatically generated

1. Create a PIN, then confirm the PIN. Click **OK**.

A screenshot of a computer

Description automatically generated

1. Touch the hardware security connected to your computer.

A screenshot of a computer

Description automatically generated

1. Click **OK** to save the passkey to the hardware security token and complete the enrollment process.

A screen shot of a computer security

Description automatically generated