How to Set Up Your Security Methods

When you login to the account settings site (https://account.wsu.edu). This will take you to where you can edit your profile settings and locate the Security Methods box.

Once you are on the editable profile screen:

   - **Password**
   - **Okta Verify**
   - **Pixel 3a**
   - **Security Key or Biometric Authenticator**
     - Fieren ePass FIDO2-NFC Authenticator
     - Last used 4 seconds ago
     - Enrolled 2 years ago
   - **Google Authenticator**
   - **Phone**
   - **Security Question**

2. Select at least one Security Method. (Note: If you set up more than one Security Method, you will have the option to choose your preferred verification method at every login.)

Okta Verify Mobile App

2. On the "Setup Okta Verify" screen, click the device type icon.
3. Click “Next.”

4. Follow the instructions to install the Okta Verify Mobile App for your device.

5. Launch the Okta Verify application and select “Add Account.” (Note: You may be asked to allow Okta access to your camera for QR scanning).

6. Scan the QR code on the screen to configure the application.

7. Click “Done” to complete the process.
8. You will then be prompted to sign in to Okta to complete the “Verify” factor.

9. You will then be prompted to verify a factor. You can choose the factor in the pop-up menu attached to the right side of the circle in the window.

10. During this process, you will have received emails confirming the setup.
Hi Butch,

You enrolled in multi-factor authentication for your account butch.cougar@wsu.edu.

Details

Security Key (U2F)
Wed, February 20, 2019 @ 06:58 PM (UTC)
Pullman, Washington, US

Don't recognize this activity?

The purpose of this email is to ensure that we update you whee important actions are taken. The security of your account is important to us. If you don't recognize this activity, please contact your administrator immediately.

This is an automatically generated message from WSU Okta System. Replies are not monitored or answered.
Hi Butch,

You enrolled in multi-factor authentication for your account burch.cougar@wsu.edu.

Details

Okta Verify Push
Wed, February 20, 2019 @ 07:03 PM (UTC)
Pullman, Washington, US

Don’t recognize this activity?

The purpose of this email is to ensure that we update you whee important actions are taken. The security of your account is important to us. If you don’t recognize this activity, please contact your administrator immediately.

This is an automatically generated message from WSU Okta System. Replies are not monitored or answered.
2. On the "Setup Google Authenticator" screen, click the device type icon.

Install the Google Authenticator App

1. On your mobile device, open the application store:
   - On an iOS device, open the "Apple App Store."
   - On an Android device, open the "Google Play Store."
2. Search for and install "Google Authenticator."

3. Open the Google Authenticator app.

4. Tap "Scan a barcode." (Note: You may need to additionally install the "Barcode Scanner" app). Follow the prompts, and then re-tap "Scan a barcode."

5. Hold your device up to the computer screen and scan the barcode.
6. Click "Next."

**Complete the Okta login process**

7. A Google Authenticator code will appear on your mobile device. Type the code into the "Setup Google Authenticator" screen on your computer, and click "Verify."
2. On the “Set Up Text Message Verification” screen, type your phone number.
3. Click “Send Code.”

**Code Verification**

4. An SMS code will be sent to your mobile device. Type the code into the “Enter Code” field, and click “Verify.”

**Voice Call**
2. Enter your phone number and click “Call.”
3. Answer the call, and listen for the code.
4. Enter the code that is given.
5. Click “Verify.”

Authenticate using Security Key

Security Method Enrollment using Security Key (Note: Security keys are typically in the format of a USB, but are also available in other formats.)

1. From your account screen, find the Security Methods box. (Note: Currently compatible web browser extensions include Chrome, Firefox, Edge, and Safari.)
2. Next, click the setup button next to the “Security Key or Biometric Authenticator” section.
Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your account.

SECURITY KEY OR BIOMETRIC AUTHENTICATOR

Use a security key (USB or Bluetooth) or a biometric authenticator (Windows Hello, Touch ID, etc.).

Setup

Set up security key or biometric authenticator

Your browser will prompt to register a security key or biometric authenticator (Windows Hello, Touch ID, etc.). Follow the instructions to complete enrollment.

Enroll

Back to factor list
3. When you see the prompt to do so, insert your security key into your computer's USB port, and activate the security key.

Firefox browser

Firefox can anonymize this for you, but the website might decline this key. If declined, you can try again.

1. In Firefox, you must click on the option to "Proceed," then plug the device in to finish registration.

2. Once this is complete, return to your account settings page.

Chrome browser

You should get the following boxes:

Set up your security key to sign in to login.wsu.edu as wdonnell.okta@wsu.edu.

This request comes from Chrome, published by Google LLC.
The FIRST TIME you plug in your Security Key, the system will request that you create a PIN Number for your Security Key. **YOU SHOULD TREAT THIS PIN AS A ONE-TIME SETUP SPECIFIC TO YOUR USB SECURITY KEY!** Pay Attention to this and keep your PIN as you cannot reset it, and the system will always ask for the PIN Number after you set it up, even if you remove and try to re-setup this USB Security Key again. (There may be a way to Reset Your USB Security Key PIN - but it isn't guaranteed to work with ALL keys.)
Once you touch your security key at the end, the system finishes the Setup.

When you go to use your Security Key for MFA later, the system WILL ASK for the PIN you set on the key as well as asking you to touch it again after you have plugged it in.

For Security Keys that WSU has tested, please see below:

Security Key Options for Multi-Factor Authentication (MFA)