



Multi-factor Authentication (MFA) for TriWest Staff Laptop Users

Purpose

The purpose of this job aid is to assist TriWest (Direct/Contractor/Temporary) staff with activating their Okta account and setting up multi-factor authentication (MFA) or to authenticate using a YubiKey.

Overview

Multi-factor authentication enhances the organization's security by requiring users to identify themselves by more than a username and password. This job aid assists staff with activating a new account and setting up their personal MFA. You are prompted to use the MFA each time you log in to TriWest's environment.

The steps below walk you through how to activate and set up your Okta account and how to log in each day using the MFA or to authenticate using a YubiKey device. The options you are presented with are based on your employment type with TriWest:

- **Direct Hire** –
 - **Assigned a TriWest smartphone** – Okta Verify using assigned smartphone
 - **Reside in CA** – YubiKey ONLY (unless you have an assigned TriWest smartphone)
 - **All others** – Okta Verify using personal smartphone

- **Contractor/Vendor/Temporary** - Okta Verify using personal smartphone OR voice call back to a predefined phone number

Contents

[Terms and Definitions](#)

[Set up MFA](#)

- **[YubiKey](#)** – Hardware device that supports touch authentication **Note: YubiKeys are assigned ONLY under certain circumstances. See your Supervisor if you are unable to use a smartphone or call back to a cell phone for verification. Supervisors must submit a hardware request form to request a YubiKey for staff.*
- **[Okta Verify](#)** – Verification push to the Okta Verify App on a smartphone
- **[Voice Call Authentication](#)** – Calls to a landline or cell phone

[Logging in to TriWest environments after MFA is set up](#)

[Okta Self Service](#)

Terms and Definitions

Term	Definition
Multi-factor Authentication - Also referred to as MFA	A security technology that requires you to answer an MFA challenge question in addition to providing your regular user ID and password when logging in each day, or when logging in to an application that is protected by this technology.
Okta	Identity management service that TriWest uses to better position the organization to align with current system authentication trends and requirements.
Push Notification	Security mechanism used by Okta to send authentication to you each time you log in to a TriWest system that requires Okta MFA.
YubiKey	Hardware authentication device to protect access to computers, networks, and online services that supports one time passwords and authentication.

Setting up MFA

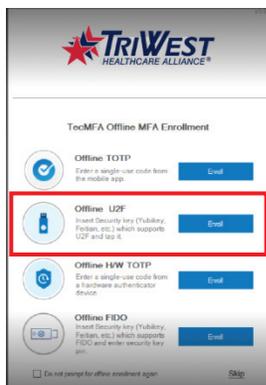
The next step is to set up the MFA. Once you attempt to access the TriWest environment, you are prompted to perform a one-time MFA set up. Then each subsequent access to the TriWest environment you will receive a notification/call based on your initial MFA selection. If you are presented with more than one MFA option (Okta Verify, or Voice Call), the application prompts you to perform a one-time set up for each one. Setting up additional verifications allows you to have more than one MFA to use as a backup.

Follow the steps below to set up your initial and additional MFAs (if presented to you).

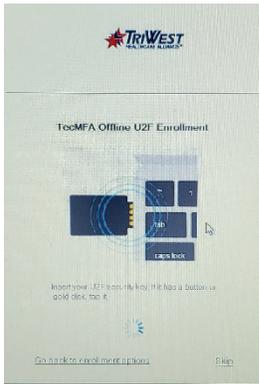
- **YubiKey Authentication**

1. Access the TriWest environment (the way you normally do).
2. Click **Enroll** for the **Offline U2F** option.

Note: Offline TOTP is for Okta Verify users and the Offline U2F option is for YubiKey users. TriWest does not use the Offline H/W TOTP or Offline FIDO options.



3. Insert the YubiKey into a USB port on your computer.



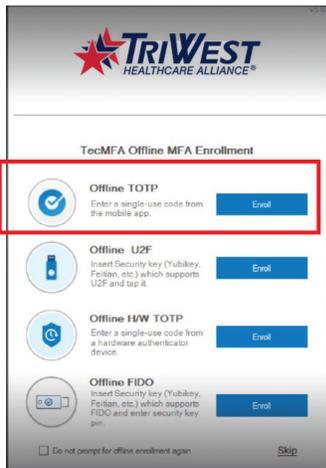
4. Hold your thumb/finger on the “Y” in the gold circle on the YubiKey for 1 second
RESULT: Authentication code auto populates and verifies you.

- **Okta Verify Setup** If you select to use Okta Verify, you will need to download the Okta Verify App from the App store/Google Play store. The application is where the authentication is “pushed” to you each time you log in to the TriWest environment. This is a one-time set up so if you have not set it up yet, you are prompted to set it up.

1. Access the TriWest environment (the way you normally do).

2. Click the **Enroll** for the **Offline TOTP** option.

Note: Offline TOTP is for Okta Verify users and the Offline U2F option is for YubiKey users. TriWest does not use the Offline H/W TOTP or Offline FIDO.



3. Select your **device type**:

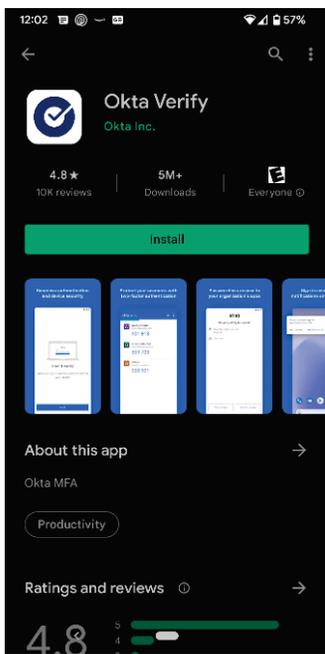
- iPhone
- Android

4. Access your phone and download the Okta Verify App

- iPhone – App Store



- Android – Google Play Store



5. Click **Next** on your computer screen to **Setup Okta Verify**.

- From your phone:

1. Press **Open** on the Okta Verify app on your phone.
2. Press **Get started**.
3. Press **Next**.
4. Press **Add account**.
5. Press **Organization**.
6. Press **Yes, ready to scan**.
7. Press **OK** in the pop-up message to allow Okta Verify to Access camera and Push notifications while using the app.
8. Scan the **QR code** on your laptop screen.

If you are...	Then...
Able to scan QR code	Account added displays on your mobile device
Not able to scan QR code	You are able to request an activation link to be sent via: <ol style="list-style-type: none"> i. SMS (Text Message) ii. Email (Opening the email displays a code that you enter into the Okta Verify app.) (Install the App if not already done.) <li style="text-align: center;">or iii. Set up manually without push notification by typing in the code that is presented

Important: Keep Okta Verify installed on your device, as you will need it to sign in daily.

9. Press **Allow**.

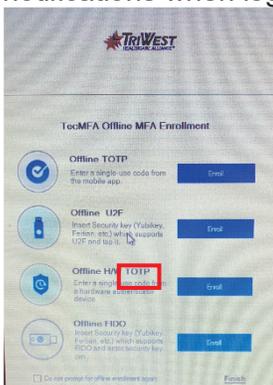
RESULT: Account is added

10. Enter the notification number.

11. Click Verify.

12. Press **Finish** in the bottom right-hand corner.

Note: The Okta Verify app installs your credentials to the app so you can now receive push notifications when logging in to TriWest systems that require MFA for access.



13. **END OF PROCEDURE**

- **Voice Call Authentication**

Note: If your mobile device blocks spam calls, it may block Okta Voice Call.

If you selected your MFA via a voice call, you will receive a recorded call from Okta Verify (872-278-8883) to the phone number you provided each time you log in to the TriWest environment. The recording provides you with a 5-digit code you will enter into your computer to be authenticated. Follow the steps below to set up your voice call MFA.

1. Click **Setup** under **Voice Call Authentication** on your computer screen.
2. Enter your **Phone number** and extension (if needed).
3. Click **Call**.
4. A **5-digit code** is provided via a recorded call to the phone number entered.
5. Enter the 5-digit code in the field provided.
6. Click **Verify**.
7. **END OF PRECEDURE**

Logging in to TriWest Environment after MFA is set up

Follow the steps below when logging in to TriWest environment.

If you are using YubiKey to authenticate:

1. Log in with your TriWest username and password.
RESULT: YubiKey Authentication screen displays
2. Click **Verify**
3. Insert the YubiKey into a USB port on your computer.
4. Hold your thumb/finger on the “Y” in the gold circle on the YubiKey for 1 second

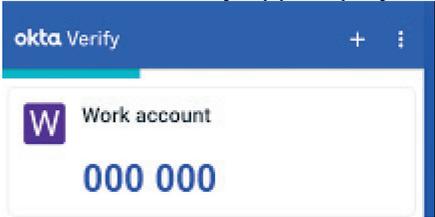


Result: Authentication code auto populates and verifies you

5. **END OF PROCEDURE**

If you are using MFA for Okta Verify, Push or Code:

1. Log in with your TriWest username and password.

If you select...	Then...
<p>Send Push</p> <p>Notes:</p> <ul style="list-style-type: none">• Use Push notifications so that you do not need to type in the code• You can also select Send Push Automatically to have them automatically send you a login	<ol style="list-style-type: none">1. You receive a notification on your Mobile Device. "Did you just try to sign in?"2. Select Yes, It's me.3. You are authenticated and granted access to the TriWest environment.4. END OF PROCEDURE
<p>Or enter code</p>	<ol style="list-style-type: none">1. The Okta Verify app displays a 6 digit code. 2. Enter the 6-digit Code in field provided.3. Click Verify.4. You are authenticated and granted access to the TriWest environment.5. END OF PROCEDURE

If you are using MFA for Voice Call Authentication:

1. Log in with your TriWest username and password.
RESULT: Voice Call Authentication screen displays
2. Click **Call.**
3. A **5-digit code** is provided via a recorded call to the phone number entered.
4. Enter the 5-digit code in the field provided on your computer screen.
5. Click **Verify.**
6. You are authenticated and granted access to the TriWest environment.
7. **END OF PRECEDURE**

Okta Self Service

Using the Okta Self Service allows you to make edits to some things that will reduce the need to contact TriWest IT Service Desk. Follow the steps below to access Okta Self Service.

1. Enter the URL <https://login.triwest.com> in a Google Chrome browser window.
2. Enter your TriWest username and password.
3. Authenticate using your Multi-factor Authentication (if do not already have set up.)
4. Click the down arrow “carrot” on the top right of your screen.
5. Click **Settings**.
6. Select the edit(s) you wish to make
 - Personal Information
 - Security Image
 - Display Language
 - Forgotten Password Question
 - Extra Verification
7. **END OF PROCEDURE.**