Access and Setup Guide

Contents

Introduction

The Michigan Data Collaborative (MDC) is a nonprofit healthcare data organization at Michigan Medicine. MDC produces dashboards to support Collaborative Quality Initiatives (CQIs) aiming to improve patient outcomes across Michigan.

This Access and Setup Guide describes the steps that you must complete to access the MDC dashboard. If you need assistance with any of these steps, see *Getting Help* for support contact information.

Before You Begin

Verify that your web browser meets one of the following requirements to ensure it will be supported by Tableau:

- Chrome on Windows, Mac, and Android
- Microsoft Edge on Windows
- Mozilla Firefox & Firefox ESR on Windows and Mac
- Apple Safari on Mac and iOS

You may need to contact your local IT support if you do not have permission to install software on your computer.

Overview

I. Obtain a U-M User Account

1. Connect with your PO's Acknowledger to request an MDC account.

2. Once MDC receives the request from your PO Acknowledger, you can expect the following communications:

3. ***New users*** will receive emails containing login credentials and login instructions.

   i. The first email message will come from *it.accounts@umich.edu* with the subject line "Your U-M uniqname and password" and will include your username (U-M uniqname) and the instructions on initial password setup.

   ii. The second email message will come from *mdc-accounts@med.umich.edu* with the subject line: "New User Account: Access Granted to MCT2D Interactive Reporting Site".

4. ***For existing users***, your existing login credentials will remain the same. We will notify you by email when you have been granted access to the MDC user interface.

If you have any questions in the meantime, please contact the MDC account team at *mdc-accounts@med.umich.edu*.

II. Duo to Okta Verify Transition

On **February 25, 2026**, Michigan Medicine and the University of Michigan switched from Duo to Okta Verify for multi-factor authentication. MFA provides a second layer of security to ensure that your account remains secure and to verify that the person logging in is you. Each time you log in to the MDC dashboard, you will get a notification on a separate device to confirm that it is you who is logging in.

If you haven't enrolled in Okta yet, please do the following:

- **Enroll in Okta Verify for the First Time.** MDC users must take action to continue to access to the CQI dashboards hosted by MDC. Visit *Enroll in Okta* for step-by-step instructions and a short video.
- **Do not delete the Duo app** from your mobile device before you install the Okta Verify app enroll in Okta.

View the U-M Information and Technology Services (ITS) Help page to read more about switching from Duo to Okta Verify: *Okta Help | U-M Information and Technology Services*.

Go to the *Okta or Password Help* section in this document to view contact information for the ITS Service Center.

III.   About the Okta Verify App

- Okta Verify is a free application.
- Okta Verify requires approximately 67.5 MB of internal storage on an Android device and 109.1 MB on an iPhone.
- In order to install the Okta Verify app, your mobile device must run on a supported operating system (OS) version:
    - Apple Devices: Requires iOS 17 or higher
    - Android Devices: Requires Android 12 or higher
- Okta Verify requires access to send you notifications and to your device's camera. The camera access is only used to scan a code as part of the activation process.

IV.   Enroll in Okta Verify

Follow the steps below to enroll your UMICH account in Okta. Note that while not all possible options are described below, these steps provide the simplest method of enrolling in Okta.

Using a Mobile Device and Desktop Computer

- **Watch a YouTube video**. Here is a short video demo of the Okta enrollment process: *How to Enroll In Okta for the First Time*.

- Or follow the detailed step-by-step instructions below.

1. Go to *oktaverify.umich.edu* (opens in new window) on your computer.

2. Click **Enroll your UMICH account**.

3. Log in with your uniqname and UMICH password and complete Duo authentication.
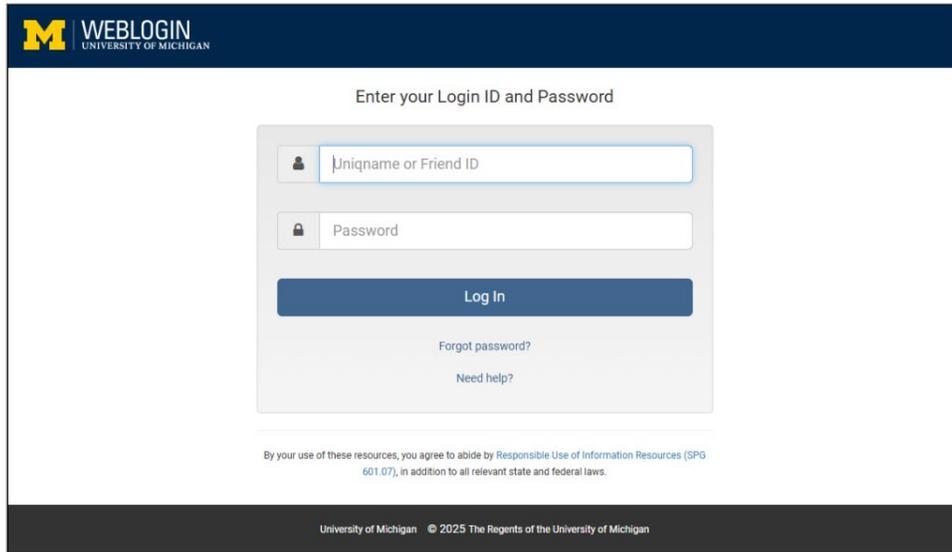
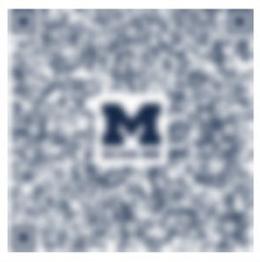4. Scan the applicable QR code with your mobile device to download the Okta Verify app. Once the app is downloaded, return to your computer and click **Continue**. *Note: Ignore any prompts in the Okta Verify app for now and close it.*
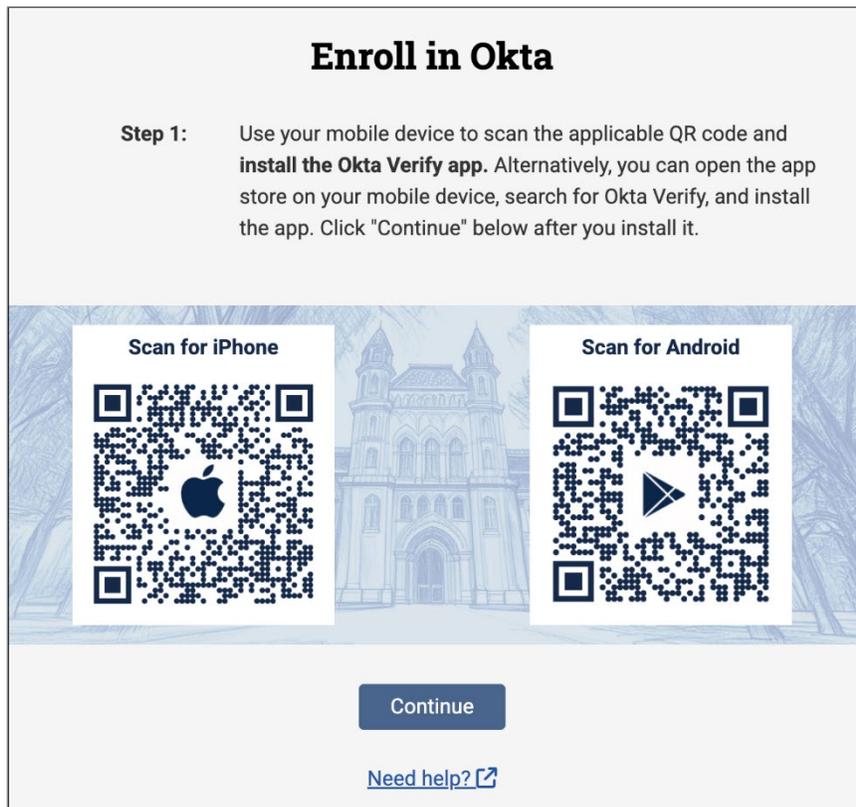
5. With your mobile device, scan the QR code that displays on your computer.

6. On your mobile device, tap **Get Started**. If desired, tap **Enable** to enable biometric authentication (Face ID or Fingerprint ID) or tap **Not Now** to bypass this feature. Tap **Done**, close the Okta Verify mobile app, and return to your computer.
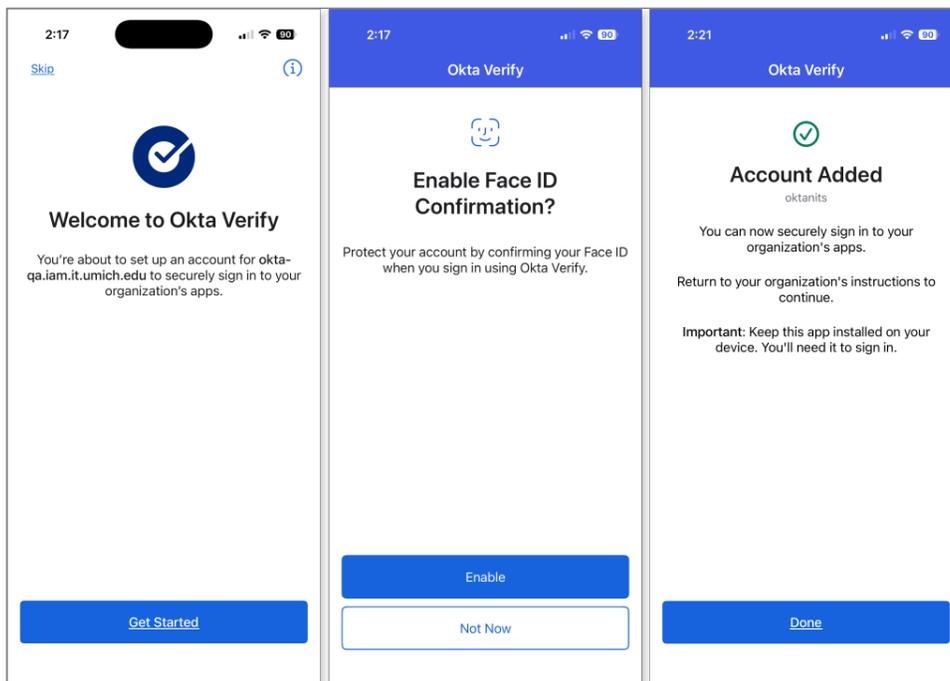
7. (Optional) Click **Sign in with Okta** to test your Okta login.
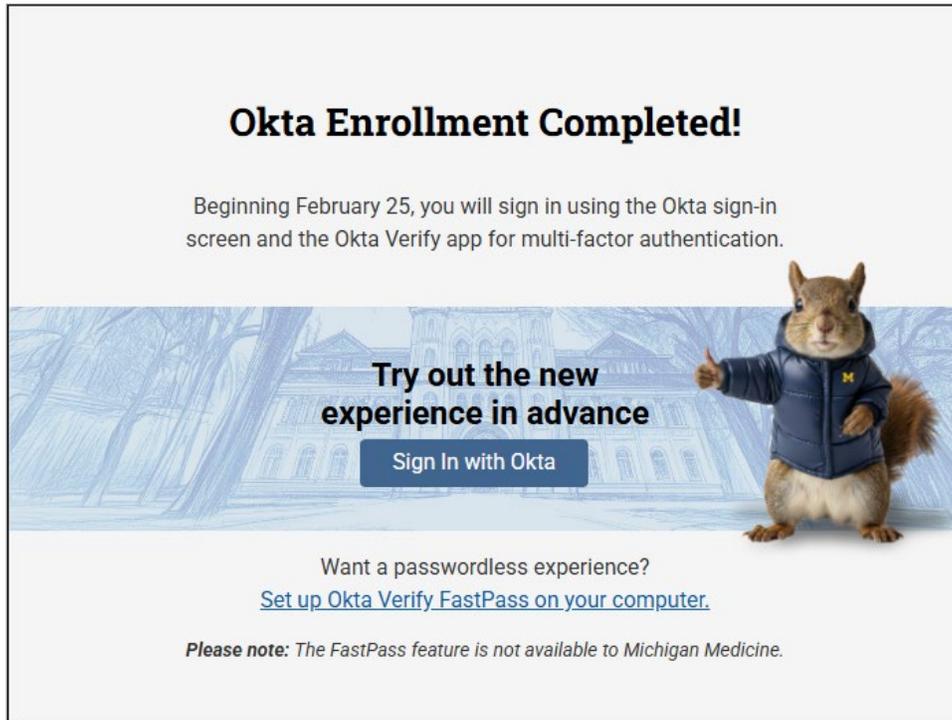
8. Log in to the Okta Sign-In page with your uniqname and UMICH password.
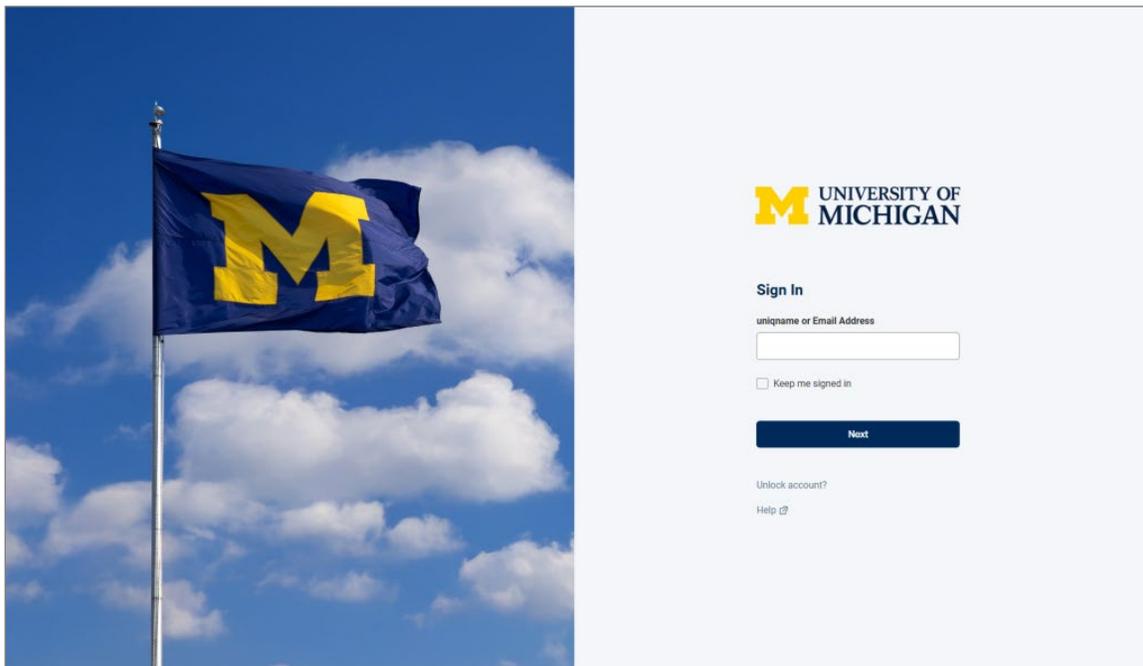
9. Select the **Okta Verify - Get a push notification** option. A verification number displays on your computer and notification is sent to your mobile device. Open the notification on your mobile device, tap the corresponding number, and complete biometric authentication, if prompted.
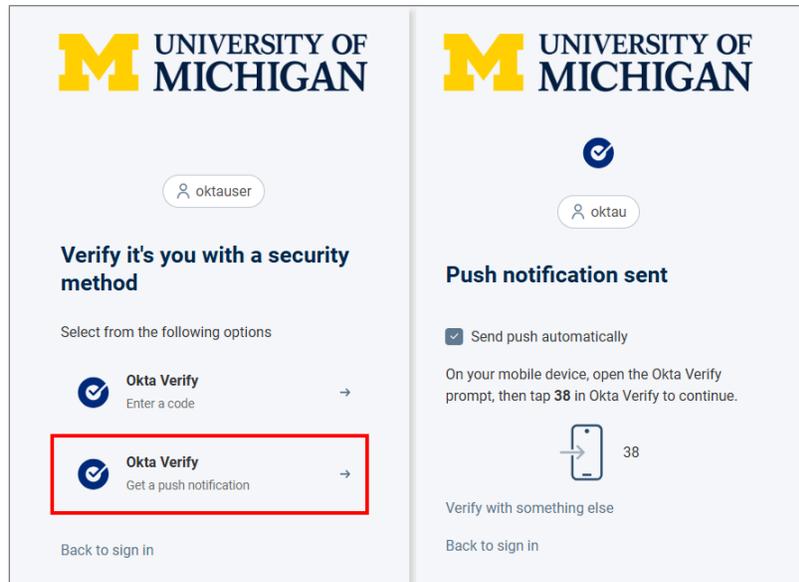
You are now successfully enrolled in U-M Okta. You can close the Okta Verify app on your mobile device and close any browser windows you used to enroll.

Source: _Enroll in Okta | U-M Information and Technology Services_

Related Articles: _Enroll in Okta Using the Okta Verify App_

Enroll in Okta Verify Without a Smartphone or the App

Follow these steps, if (i) Your mobile device is not compatible with Okta Verify (requires Android 12+ or iOS 17+), or (ii) you don't have a smartphone or tablet.

The *Okta Verify Mobile App* is the preferred and recommended multifactor authentication option as it provides the easiest and best experience in almost all cases; cellular service is not required.

If you cannot update your OS, or do not have a smartphone or tablet:

1. *Obtain and enroll an Okta hardware token*.

    a. We highly recommend obtaining your hardware token prior to February 25, 2026, to ensure your access to U-M computing services is not interrupted.

2. After receiving your hardware token, visit *https://oktaverify.umich.edu* to complete enrollment.

Note: The university will cover the cost of an initial Okta hardware token for each user (faculty including emeriti, staff, students, retirees, alumni, and sponsored affiliates). Shipping is not included. Replacement tokens are available at the current list price to the user.

Source: *https://teamdynamix.umich.edu/TDClient/30/Portal/KB/ArticleDet?ID=14707*

Add, Remove, or Reactivate Devices with the Okta Verify App

Follow the steps below, if one of the following applies to you:

- I need to add another device to my account, for use with the Okta Verify app (you have multiple devices)
- I need to reactivate the Okta Verify app because...
    - I got a new phone
    - I deleted the Okta Verify app
    - I removed my UMICH account from the Okta app
- I need to remove an obsolete device from my Okta account

Add or remove Okta Verify devices from Okta Account Settings.

1. Sign into *Okta End User Settings* and then follow the applicable steps below to add or remove a device.

    a. If you are not able to approve the Multi-Factor Authentication (MFA) request, click **Verify with Something Else** and choose another device that you can verify the request with.

    b. If you don't have another Multi-Factor Authentication (MFA) device you can use to verify the request, *call or chat with the ITS Service Center* for assistance.

Add a New Okta Verify Device

1. Click **Security methods** in the left sidebar.

2. Click **+ Set up another** in the **Okta Verify** section.

3. Enter your UMICH password on the Okta Sign-In page.

4. Click **Okta Verify - Set up Another**.

5. Follow the instructions that display to set up Okta Verify on your new device.

Remove an Okta Verify Device

1. Click **Security methods** in the left sidebar.

2. Click **Remove** next to the applicable MFA device listed in the **Okta Verify** section.
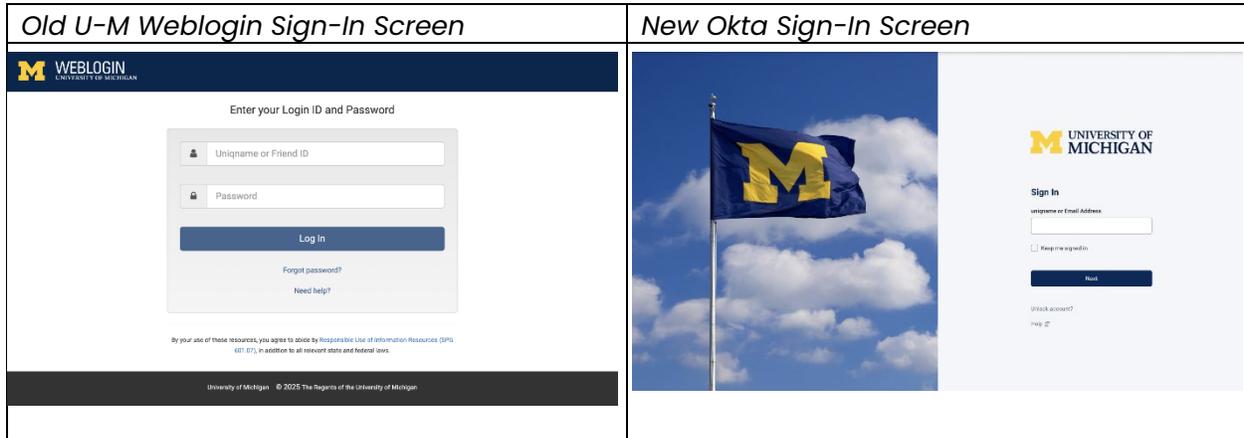
   Note: If you have multiple devices with the same name, you can check the enrollment time or the last used time to determine which one needs to be removed.

3. Click **Yes** to confirm you wish to remove the device.

4. Sign in and complete multi-factor authentication, if prompted.
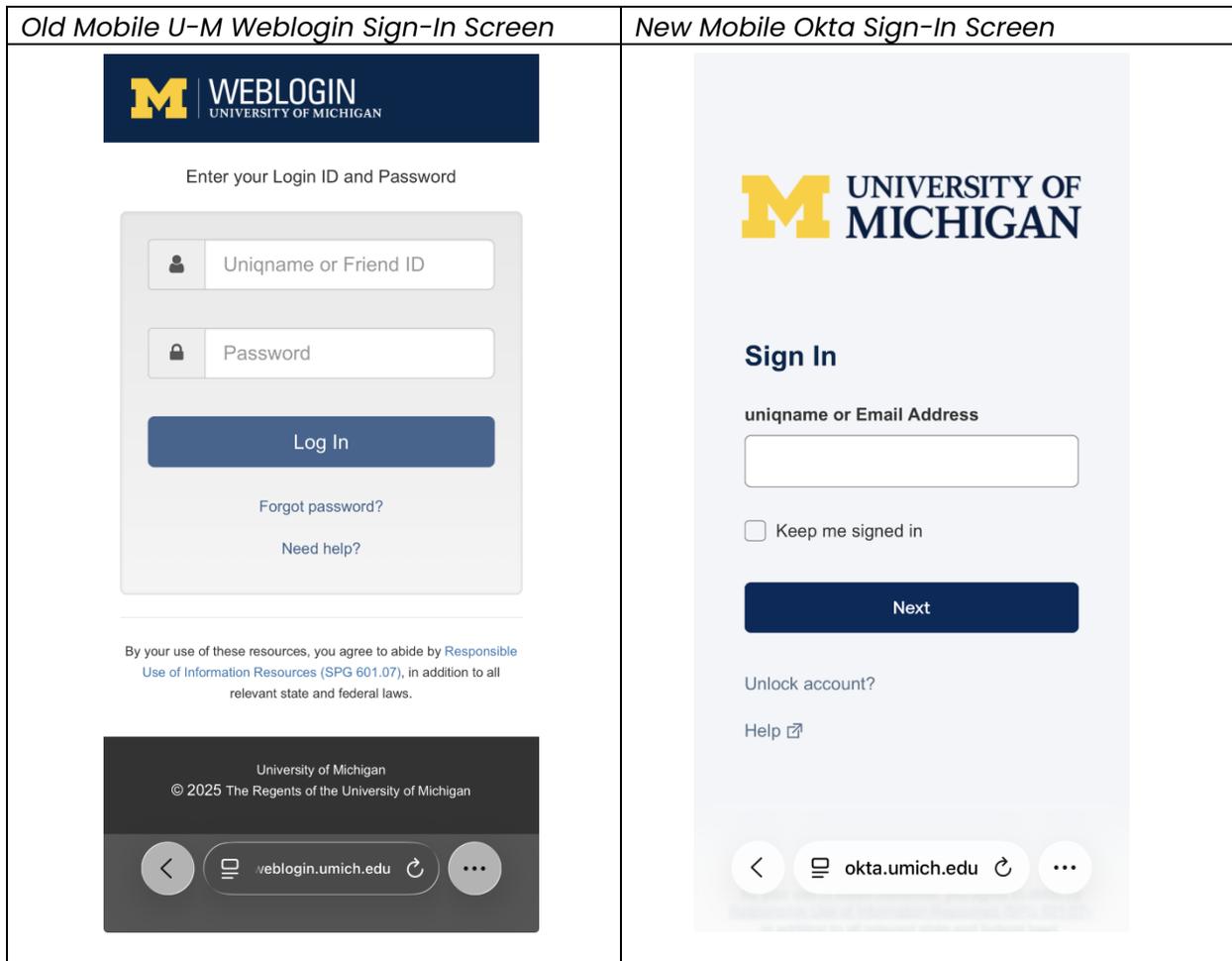
Source: *[Add, Remove, or Reactivate Devices with the Okta Verify App](#)*

V.   Comparing Duo vs Okta Verify Sign-In Screens

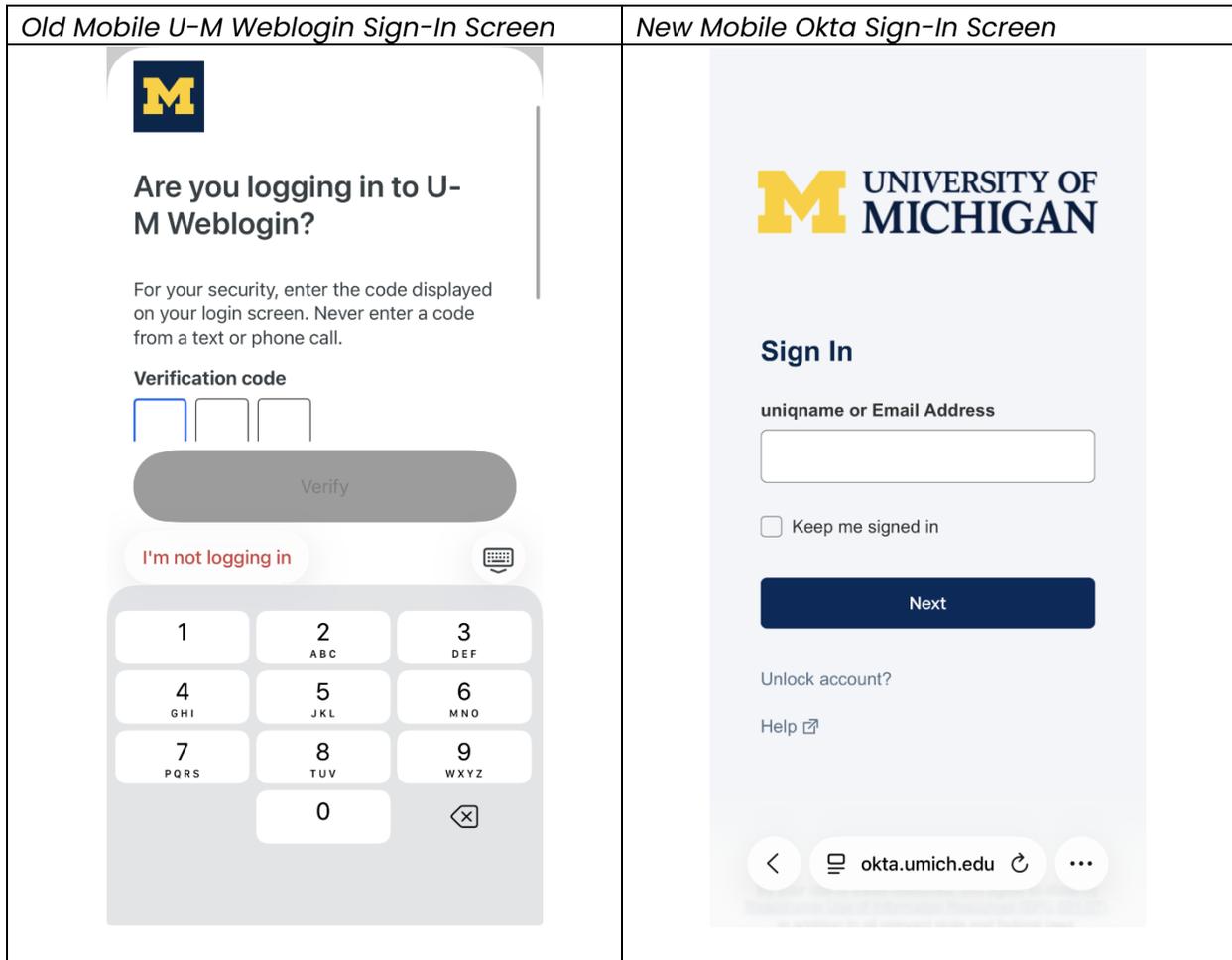### Old vs New Desktop Sign-In Screen

Old U-M Weblogin Sign-In Screen	New Okta Sign-In Screen

Old vs New Mobile Sign-In Screen

Old Mobile U-M Weblogin Sign-In Screen	New Mobile Okta Sign-In Screen

Old vs New MFA App

Old Mobile U-M Weblogin Sign-In Screen	New Mobile Okta Sign-In Screen

Source: *Signing in with Okta | U-M Information and Technology Services*

VI.   Account Lifecycle with Okta

With the transition to Okta for identity and access management at U-M, a new account lifecycle will be introduced in order to reduce security risks associated with inactive accounts.

Keeping Your Account Active. Once the transition to Okta occurs on February 25, 2026, you will be required to sign in to your UMICH or Friend account at least once a year in order to retain access.

Source: *Account Lifecycle with Okta | U-M Information and Technology Services*

VII.   Access the MDC Dashboard

To access the MDC Dashboard, navigate to the *[Michigan Data Collaborative](#)* website and click *[Login](#)*.

To access the User Guide for a specific project, navigate to the Support page for the project on the MDC website and select the User Guide link.

VIII.   Getting Help

If you need additional help with any steps in this guide, access the resources below.

General Account Information

If you have questions about how to access the MDC dashboard, contact MDC at *[MichiganDataCollaborative@med.umich.edu](#)*.

Password Help

If you have forgotten your password, email *[mdc-accounts@med.umich.edu](#)* to get instructions on resetting your password.

Okta or Password Help

For Okta or additional password help, contact the U-M ITS Service Center.

Service Center Hours: Mon–Thurs: 7 am–7 pm; Fri: 7 am–6 pm; Sat: Closed; Sun: 2–7 pm

Chat Support: *[Chat Support / U-M Information and Technology Services](#)*

Phone: 734-764-4357

Password help: *[4HELP@umich.edu](#)*

Okta transition help: *[okta-transition@umich.edu](#)*

Website: Visit the U-M *[Okta Help](#)* page.

MDC FAQS page: *[Okta Verify FAQs](#)*

- **Note:** When you contact ITS, be prepared to provide the following information, as applicable:
    - Inform the Service Center employee that you are a user of the Michigan Data Collaborative's User Portal. You are not a U-M employee; however, you have an MDC Sponsored Account with a U-M ID and uniqname to access the MDC dashboard.
    - If possible, access your U-M ID, U-M username (uniqname). You may be required to use your Level-1 password to log in.
    - **Caution**: do not provide your password to anyone!