C·B·H

a division of DBHIDS

COMMUNITY BEHAVIORAL HEALTH

Okta: Provider User Guide

Updated April 10, 2025

TABLE OF CONTENTS

1. INTRODUCTION TO OKTA

1.1. Okta Overview

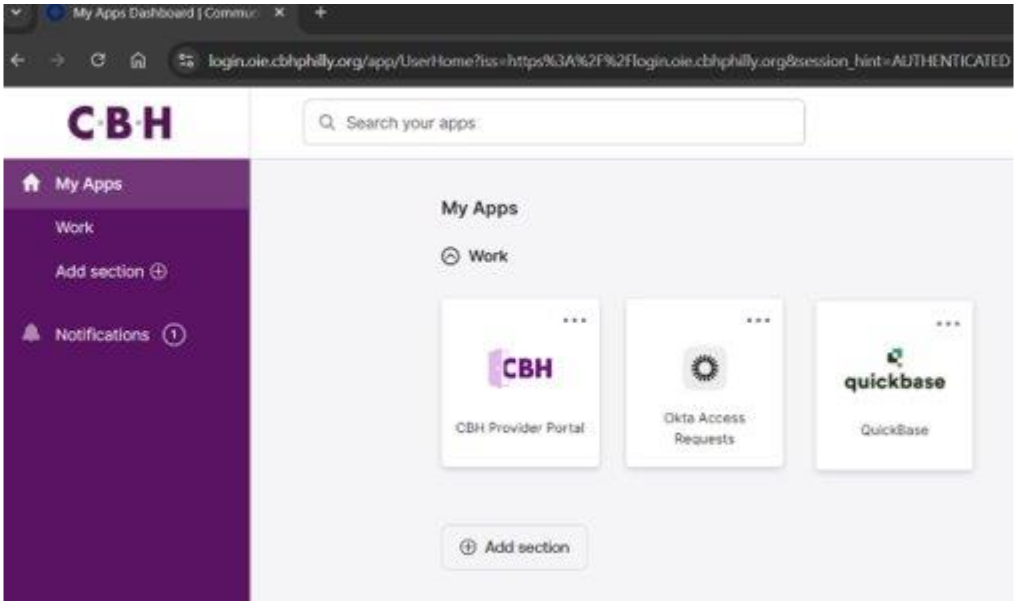
Okta is a single sign-on (SSO) tool that allows users to securely access applications provided by Community Behavioral Health (CBH) across devices by logging into one single location. It reduces the need to register for applications and remember multiple passwords separately. Okta also gives your Information Technology (IT) team added security so they can keep the network, data, and you safer.

1.2. Single-Sign On

SSO is a user authentication process that allows a person to access multiple applications with one set of login credentials. Instead of remembering different usernames and passwords for each service, SSO enables users to log in once, and then securely access all connected systems without needing to log in again.

1.3. Okta Dashboard

CBH Okta features a dashboard linking users to CBH-related platforms and software.



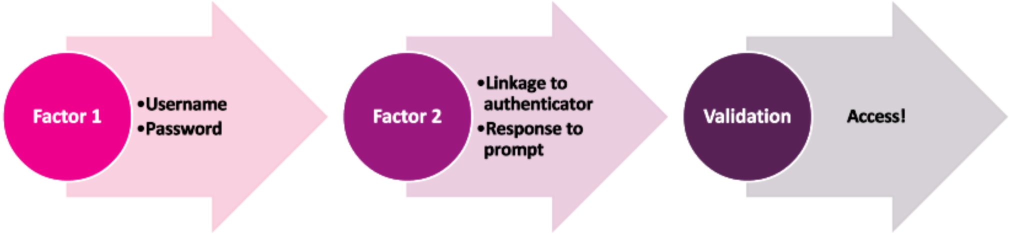
2. MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) enhances account security by requiring two or more types of verification before granting access. This additional layer of protection helps safeguard sensitive information from unauthorized users.

MFA adds an extra layer of security to your account, preventing unauthorized access even if your device or password is compromised. It helps protect against a range of security threats, such as phishing and password theft.

2.1. Accessing Accounts Via Okta with MFA

In order to log in to the Okta dashboard, you will be required to verify your identity using two authentication factors each time. The first factor is something only you know—your username and password. The second factor is a one-time code sent to your mobile device via Google Authenticator, with additional verification options available, such as Okta Verify.



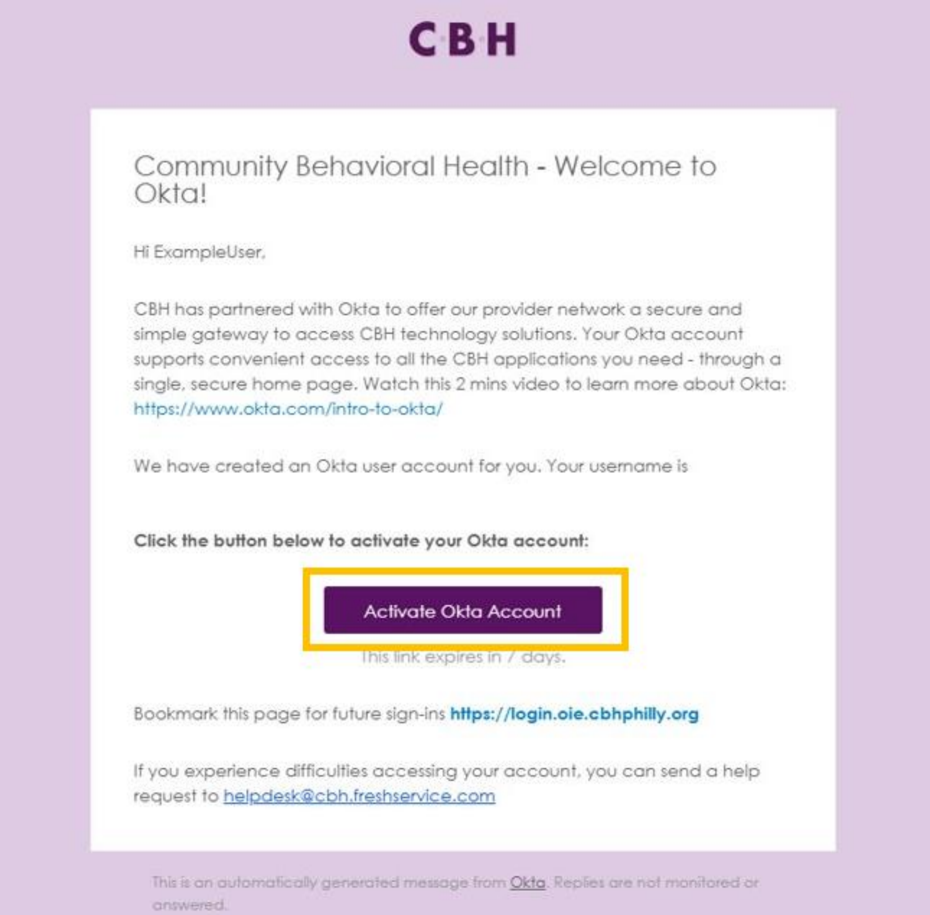
3. ACTIVATING OKTA ACCOUNT WITH MFA

To complete the set-up process, reserve about 5-10 minutes to:

- Access your computer with an e-mail or the internet.
- Access a secondary device, such as a personal smartphone or work-provided mobile device.
- As a new user, you will receive an email with the following subject, “CBH Rolls out Okta.”

3.1. Getting Started

- Open the Okta Activation e-mail on your computer.
- In the body of the e-mail, you will see a button that says, Activate Okta Account, once you click the button, you will begin the MFA registration process.



Community Behavioral Health - Welcome to Okta!

Hi ExampleUser,

CBH has partnered with Okta to offer our provider network a secure and simple gateway to access CBH technology solutions. Your Okta account supports convenient access to all the CBH applications you need - through a single, secure home page. Watch this 2 mins video to learn more about Okta: https://www.okta.com/intro-to-okta/

We have created an Okta user account for you. Your username is

Click the button below to activate your Okta account:

Activate Okta Account

This link expires in 7 days.

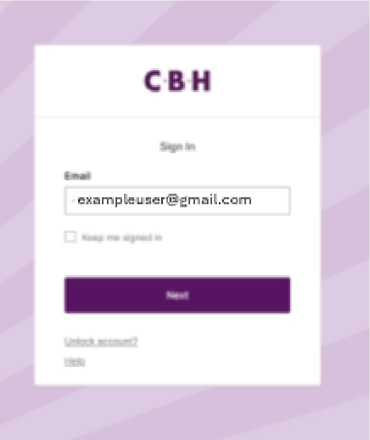
Bookmark this page for future sign-ins **https://login.oie.cbhphilly.org**

If you experience difficulties accessing your account, you can send a help request to helpdesk@cbh.freshservice.com

This is an automatically generated message from Okta. Replies are not monitored or answered.

- Upon clicking the button, the link will open a new browser tab. The instructions direct you to set up security measures for your account within seven days of receiving the link.

- If the activation link expires, you will be redirected to a new tab to type and verify your email address. After verification, a new activation link will be sent to you.



C·B·H

Sign In

Email

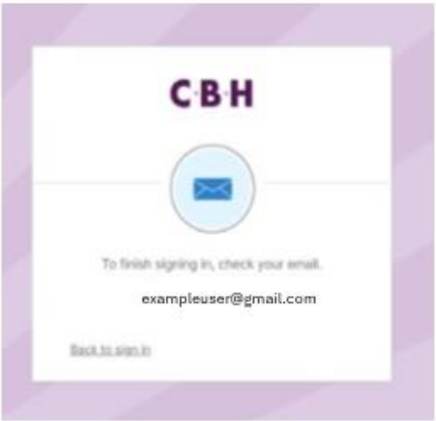
exampleuser@gmail.com

□ Keep me signed in

Next

Unlock account?

Help

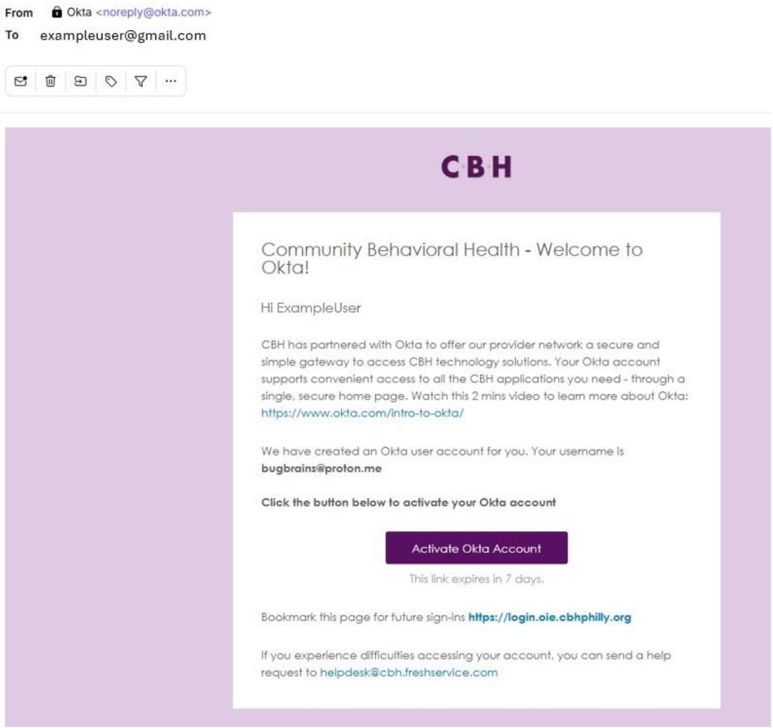


C·B·H

To finish signing in, check your email.

exampleuser@gmail.com

Back to sign in



From 🔒 Okta <noreply@okta.com>

To exampleuser@gmail.com

C·B·H

Community Behavioral Health - Welcome to Okta!

Hi ExampleUser

CBH has partnered with Okta to offer our provider network a secure and simple gateway to access CBH technology solutions. Your Okta account supports convenient access to all the CBH applications you need - through a single, secure home page. Watch this 2 mins video to learn more about Okta: https://www.okta.com/intro-to-okta/

We have created an Okta user account for you. Your username is **bugbrains@proton.me**

Click the button below to activate your Okta account

Activate Okta Account

This link expires in 7 days.

Bookmark this page for future sign-ins **https://login.oie.cbhphilly.org**

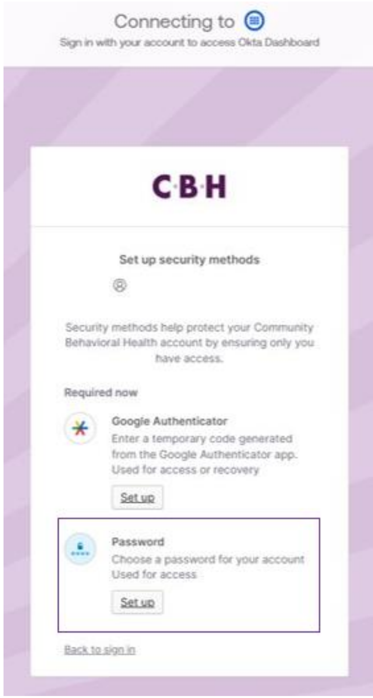
If you experience difficulties accessing your account, you can send a help request to helpdesk@cbh.freshservice.com

3.2. Setting Up Multi-Factor Authentication

When setting up MFA, you will be prompted to configure at least two identity verification factors for your account. CBH requires users to create a password and register their Okta access with Google Authenticator. ***If the application is not already installed on your smartphone, you will need to download it.***

3.3. Set Up a Password

- Click **Set up** within the Password section.
- Create a password that meets the specified requirements.
- Type the password twice to confirm.


Connecting to

Sign in with your account to access Okta Dashboard

Set up security methods

Security methods help protect your Community Behavioral Health account by ensuring only you have access.

Required now

Google Authenticator

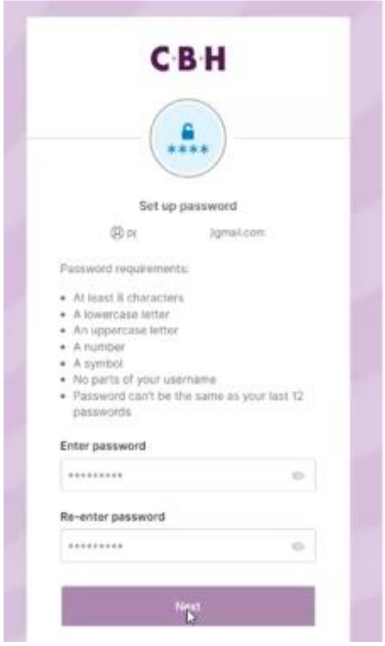
Enter a temporary code generated from the Google Authenticator app.

Used for access or recovery

Password

Choose a password for your account

Used for access


Set up password

pc)gmail.com

Password requirements:

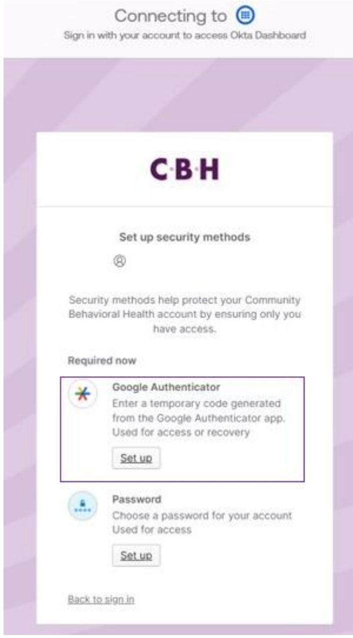
- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Password can't be the same as your last 12 passwords

Enter password: *********

Re-enter password: *********

3.4. Set Up Google Authenticator

- In the Google Authenticator section, click **Set up** to begin the process.
- Your computer will display a QR code. (a)
- Users who cannot access Google may use Google Authenticator on a phone, wit hout a Google account.
- Open the app and click the "+" in the bottom right to add an account.
- Select "scan a QR code."
- Scan the code on the computer, using your phone's camera.
- If you cannot scan, select that option on the computer, then enter the long code on the computer into the phone app – use "enter a setup key" instead of selecting "scan a QR code."



Connecting to

Sign in with your account to access Okta Dashboard

C·B·H

Set up security methods

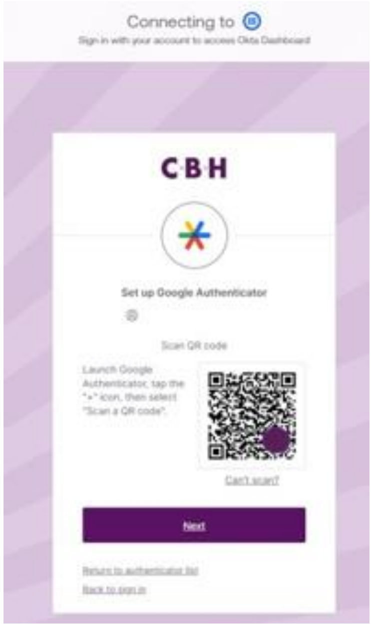
Security methods help protect your Community Behavioral Health account by ensuring only you have access.

Required now

Google Authenticator
Enter a temporary code generated from the Google Authenticator app.
Used for access or recovery
Set up

Password
Choose a password for your account
Used for access
Set up

Back to sign in



Connecting to

Sign in with your account to access Okta Dashboard

C·B·H

Set up Google Authenticator

Scan QR code

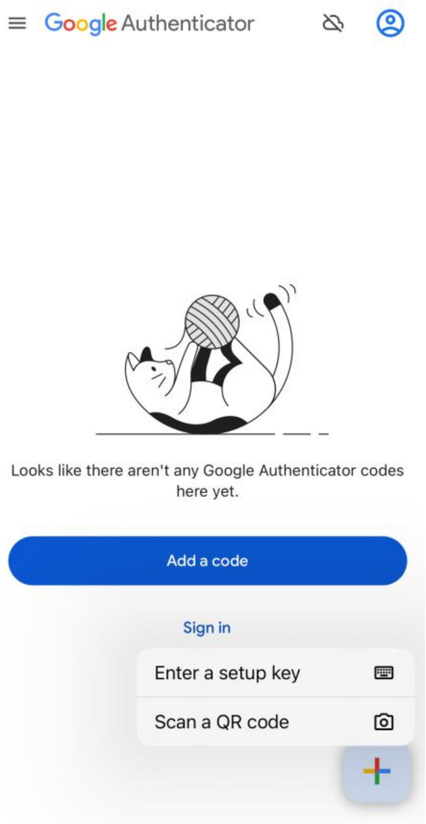
Launch Google Authenticator, tap the "+" icon, then select "Scan a QR code".

Can't scan?

Next

Return to authenticator list

Back to sign in



Google Authenticator

Looks like there aren't any Google Authenticator codes here yet.

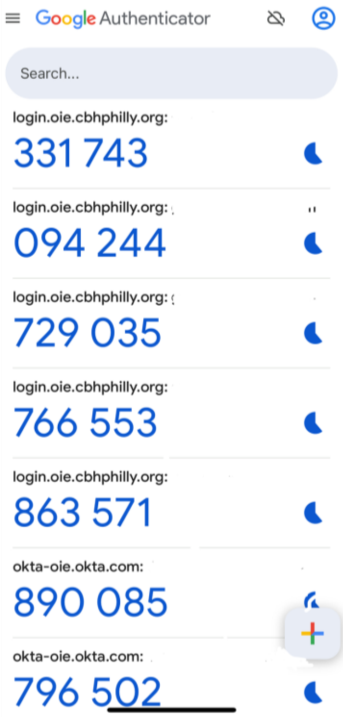
Add a code

Sign in

Enter a setup key

Scan a QR code

- To enable MFA, follow the instructions and prompts in the authenticator application on your phone to link to your Okta account and complete the MFA setup.
- You will know if you have been successful when you see a new login.oie.cbhphilly.org account with your username listed in the Google Authenticator app.
- The app will display a unique code for each linked account.
- Codes refresh every 30 seconds, with a countdown displayed in the application before a new code is generated.



Google Authenticator

Search...

login.oie.cbhphilly.org:
331 743

login.oie.cbhphilly.org:
094 244

login.oie.cbhphilly.org:
729 035

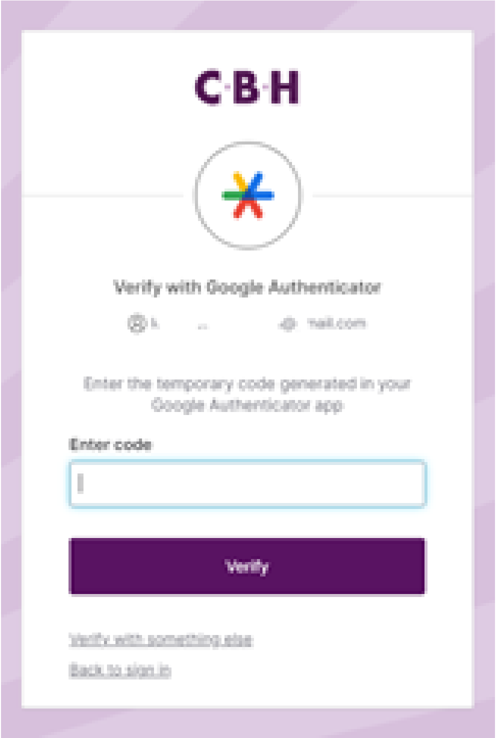
login.oie.cbhphilly.org:
766 553

login.oie.cbhphilly.org:
863 571

okta-oie.okta.com:
890 085

okta-oie.okta.com:
796 502

- Type the new code displayed for Okta in the authenticator application into the field on the computer to complete the linkage.
- On the next screen, you'll see additional verification methods available. These methods are *optional* to support user choice of other MFA apps or to ensure access in the event your phone with Google Authenticator is unavailable, if preferred.



C·B·H

Verify with Google Authenticator

Enter the temporary code generated in your Google Authenticator app

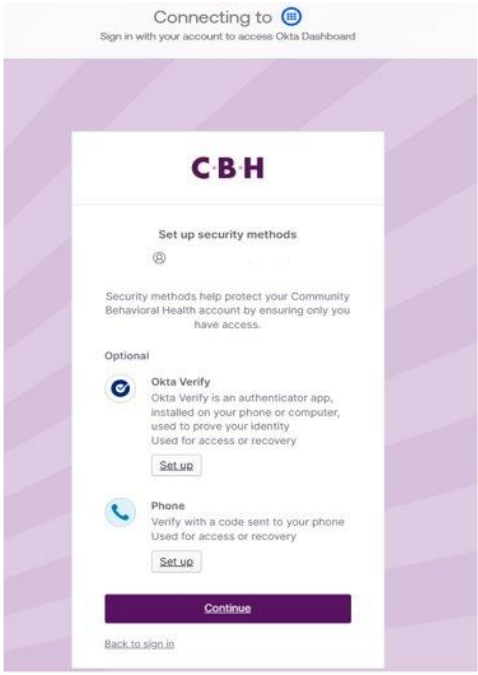
Enter code

Verify

Verify with something else

Back to sign in

- Click **Continue** to finish your Okta registration.


Connecting to

Sign in with your account to access Okta Dashboard

Set up security methods

Security methods help protect your Community Behavioral Health account by ensuring only you have access.

Optional

Okta Verify

Okta Verify is an authenticator app, installed on your phone or computer, used to prove your identity

Used for access or recovery

Phone

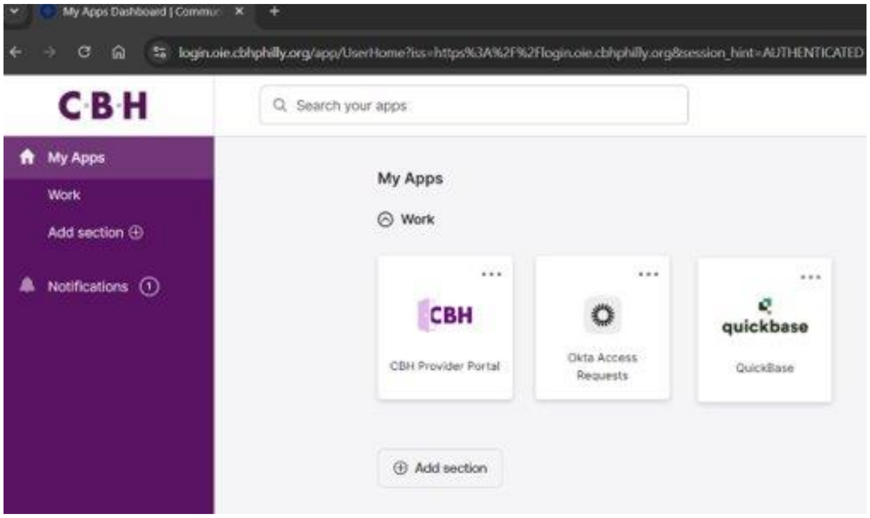
Verify with a code sent to your phone

Used for access or recovery

CBH

3.5. Logged In to Okta

- After completing authentication, you will be directed to the My Apps dashboard, where you'll see tiles for all relevant applications.


login.oie.cbhphilly.org/app/UserHome?iss=https%3A%2F%2Flogin.oie.cbhphilly.org&session_hint=AUTHENTICATED

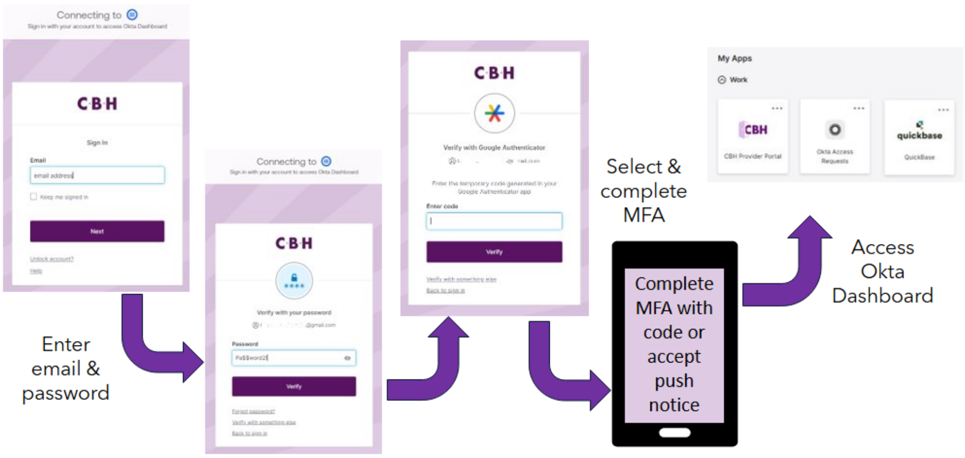
4. LOGGING INTO AN EXISTING OKTA ACCOUNT

If you already created your CBH Okta account, you **will not** get an activation e-mail.

Returning users can sign in at **https://login.oie.cbhphilly.org/** by following the prompts to enter their password and complete MFA verification. Once signed in, you will have access to the applications provided by CBH. The process is outlined below.

RETURNING USER LOGIN WITH MFA

CBH Okta: https://login.oie.cbhphilly.org/



Enter email & password

Select & complete MFA

Complete MFA with code or accept push notice

Access Okta Dashboard