Inclusivity Portal Multi-Factor Authentication Quick Reference Guide

CFPB is enhancing our cyber and data security through multi-factor authentication (MFA) for all systems accessed by external users.

The Office of Minority and Women Inclusion (OMWI) Inclusivity Portal now requires users to go through an MFA process when logging into their accounts. This means that users will have to provide additional information or credentials, apart from their username and password, to access their Inclusivity Portal accounts.

MFA is a security technique that verifies a user's identity by requiring them to provide multiple pieces of information or credentials. In practice, this means that when you log into your Inclusivity Portal account, you will be prompted to enter a code sent to your registered device, answer security questions, or use an authenticator app.

MFA is a vital security measure that protects your account from unauthorized access or cyber-attacks. The OMWI Inclusivity Portal encourages all its users to take advantage of this feature and ensure that their accounts are as secure as possible.

MFA Overview

What is MFA?

MFA is a way for Inclusivity Portal users to securely log into the site that requires using "factors" to verify who they are before gaining access. With MFA, users must use at least two or more "factors" to log in. These factors can be:

- **Something You Have**: Something that only the user possesses to login, such as a token from an authentication app on a mobile device or a hardware security device.

- **Something You Know**: A password or PIN.

- **Something You Are:** Biometrics, such as a fingerprint scan or facial recognition.

Why is CFPB requiring MFA?

MFA is an essential tool that organizations and individuals can use to help protect against cyber threats. President Biden issued an [Executive Order on Improving the Nation's Cybersecurity](#) on May 12, 2021, directing federal agencies and departments to improve cybersecurity, including rapidly implementing MFA across their enterprises. The administration then provided more specific MFA guidance in the federal Zero Trust Strategy ([M-22-09](#)).

CFPB is serious about implementing MFA and making the login process more secure and convenient. By doing so, we are further protecting our mission-critical systems and data, which is critical to helping us protect the American consumer.

MFA Options

When accessing the Inclusivity Portal, after entering your username and password, you need to select at least one of three CFPB-supported second authentication methods:

1. Salesforce Authenticator Mobile App

The Inclusivity Portal is powered by Salesforce. The Salesforce Authenticator mobile app is integrated with the login process, is simple to install, and connects to your Inclusivity Portal account. Once set up, you will receive a push notification to your mobile device that can be used to approve the secondary authorization request to login. As needed, the Salesforce Authenticator mobile app can generate a six-digit code that users can enter on the second challenge screen with or without a cellular or wi-fi connection.

You can download the Salesforce Authenticator mobile app from the Google Play or Apple App Store.

2. Non-Salesforce (3rd Party) Authenticator Application (e.g., Google, Apple, Microsoft, Okta, or other mobile / desktop TOTP authenticators)

Salesforce also supports a wide variety of 3rd party verification applications that are simple to install on multiple operating systems and do not require connectivity. Like the Salesforce Authenticator application, the 3rd party application generates unique, temporary verification codes, and they can connect to your Inclusivity Portal accounts.

You can download the 3rd party authenticator mobile apps from the Google Play or Apple App Store or desktop applications from the Microsoft Windows store.

3. Hardware Security Device (e.g., Yubikey)

Hardware security devices, also known as security keys, are physical devices that connect to a user's computer and use public-key cryptography. Security keys are easy to use as they do not require any installation or manual entry of any codes. By pressing the key's button(s), the device automatically generates and enters a code into the second challenge screen. Security keys are a good option if you do not have a mobile device near upon login or if you cannot download apps.

NOTE: CFPB is not responsible for providing any physical device to use this type of MFA. If you wish to use this option, follow the known channels through your IT department to request an approved device.

MFA Use, Considerations, and Additional Guidance

Before proceeding with MFA registration, please follow your organization's Cybersecurity team or Information Technology department guidance for installing one of these supported MFA methods. It is recommended that the organization use their current/existing MFA app/key as the first option.

NOTE: Though not often, web compatibility issues sometimes occur with MFA. If you do experience MFA verification issues, please verify that you are not using an outdated web browser. This can cause issues when using MFA because it may not support the latest security protocols or may have known vulnerabilities that can be exploited by hackers.

Additionally, the plugs-ins or extensions that you have installed in your browser, or browser settings set forth for your browser by your organization, may disrupt the verification process.

To avoid web compatibility issues with MFA, we encourage Inclusivity Portal users to:

1. Use the most recent version of the browser listed above and keep it up-to-date with the latest security patches and updates;
2. Clear or reset cookies and cache data from previous activities; and
3. Verify if the browser has enabled pop-up blockers by default and adjust settings accordingly. Some pop-up blockers may prevent MFA prompts from appearing.

Steps to Access the Inclusivity Portal Using the Salesforce Authenticator App

Step 1: Install the Salesforce Authenticator Mobile App

If you do not have the Salesforce Authenticator application already installed on your device, visit the Google Play or Apple App Store to locate and install the Salesforce Authenticator application. Please follow the prompts to install.

Step 2: Access the Inclusivity Portal

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Inclusivity Portal.

Step 3: Login with Existing Inclusivity Portal Username and Password

Enter your existing **'Username'** and **'Password'** into the login screen. Ensure the username ends in ".cfpbportal."
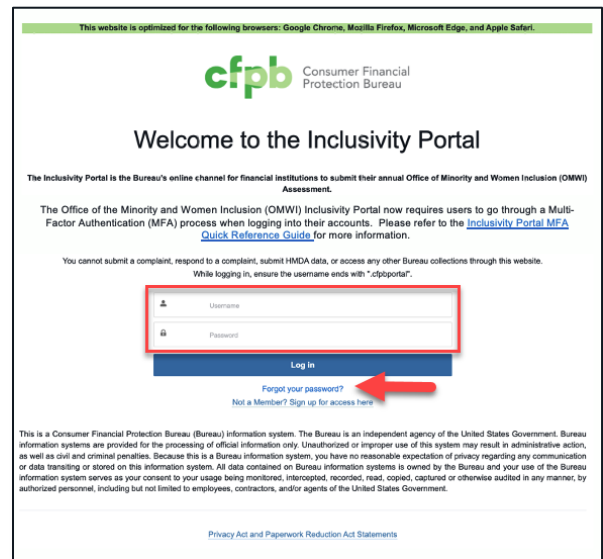
If you have forgotten the Password, use the **'Forgot Your Password'** link below the **'Login'** button.

Step 4: Choose the Salesforce Authenticator Verification Method
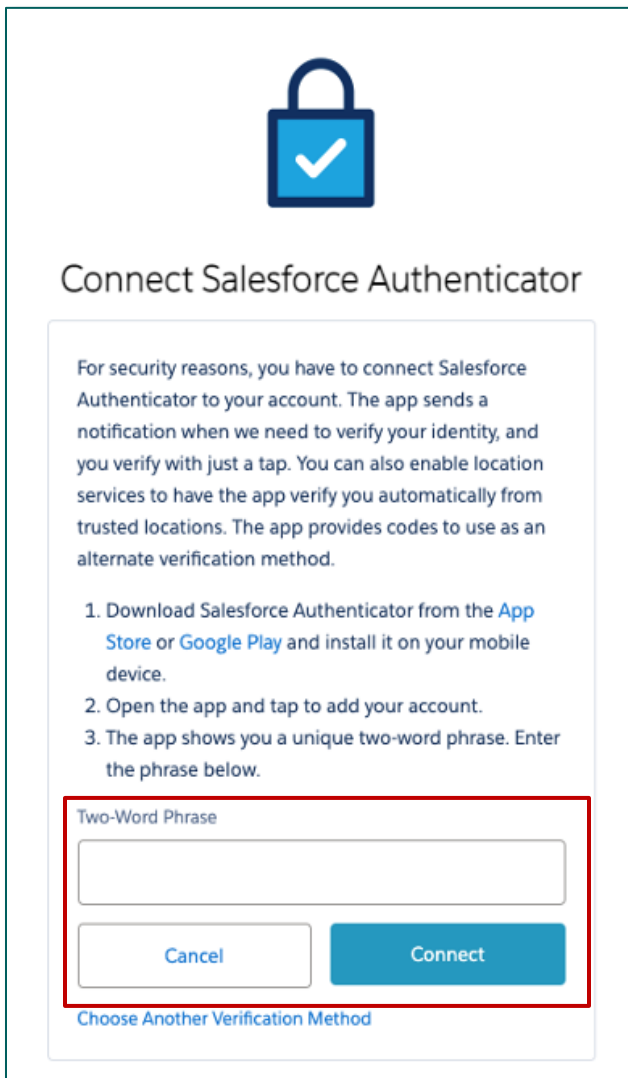
On the **'Choose a Verification Method'** screen, select the **'Use the Salesforce Authenticator mobile app'** option and select '**Continue**'.
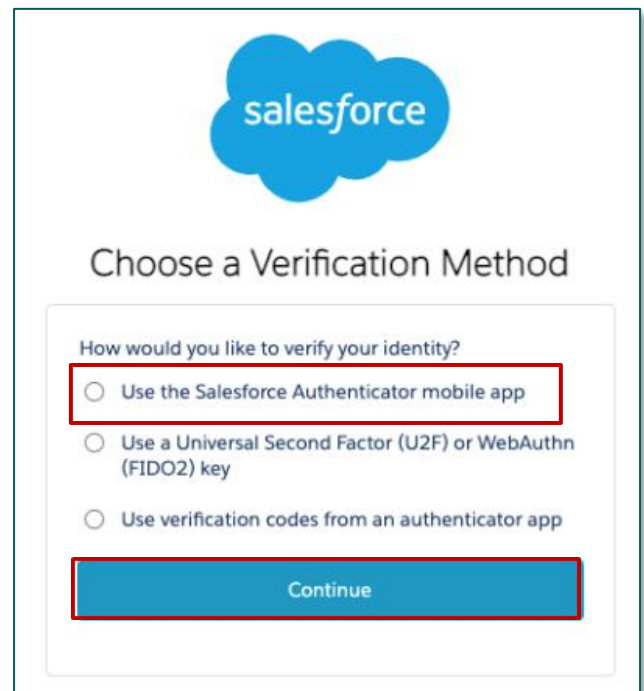
Step 5: Connect the Salesforce Authenticator Mobile App

When users first access the Inclusivity Portal and set up MFA using the Salesforce Authenticator mobile app, they must connect the app to their account. This only needs to be completed once.

Once on the **'Connect Salesforce Authenticator'** screen, open the Salesforce Authenticator mobile app and select the **'Add an Account'** button at the bottom. Obtain the two-word phrase provided and enter it into the **'Two-Word Phrase'** field. When finished, select the **'Connect'** button.
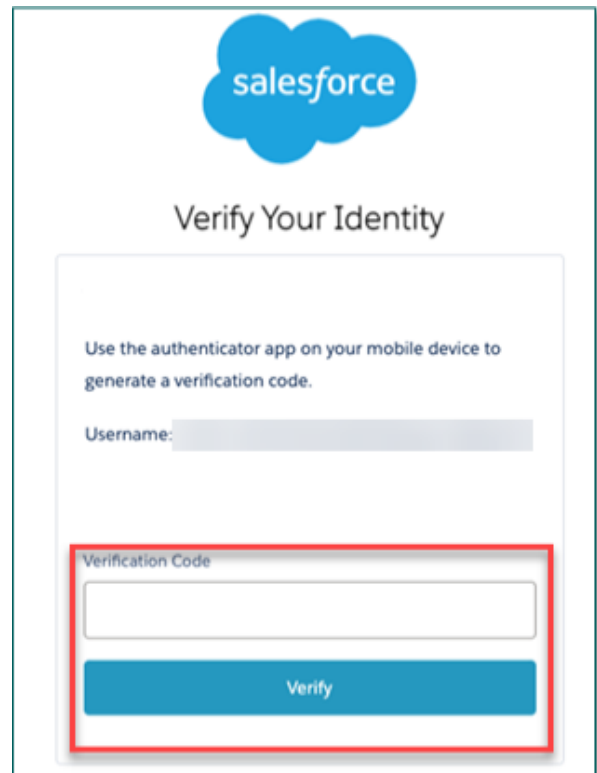
Step 6: Verify Your Identity

On the **'Verify Your Identity'** screen, enter the six-digit code provided by the Salesforce Authenticator mobile app into the **'Verification Code'** field and then select the **'Verify'** button. The six-digit code refreshes every sixty seconds.

If the code is correct, you will be directed to the Inclusivity Portal homepage and can proceed as usual.

Steps to Access the Inclusivity Portal Using the Google, Apple, Microsoft, Okta, or other mobile Authenticator Application for MFA

Note: These instructions will follow the installation and use of the mobile Microsoft Authenticator MFA application, however the process to install the Google / Apple / Okta, or other mobile authenticator applications, follow the same basic steps after accessing the application from the Google Play or Apple App store.

Step 1: Locate a Mobile Non-Salesforce Authenticator MFA Application

If you do not have a mobile MFA application already installed on your mobile device, visit the Google Play or Apple App store and type in "MFA" in the Search box and select the Enter key. Select the Microsoft Authenticator app for this example, but any MFA application will also suffice.

Step 2: Download and Install the Microsoft Authenticator App

Upon downloading the Microsoft Authenticator, click **Install**, then click **Open** and follow the set-up prompts to run Microsoft Authenticator. Note: If the **Camera** controls appears, select "*While using the app*" option
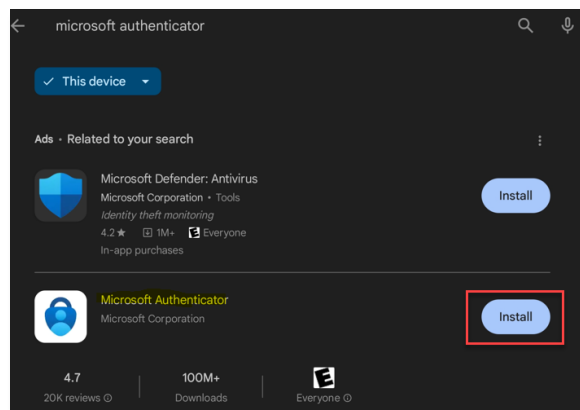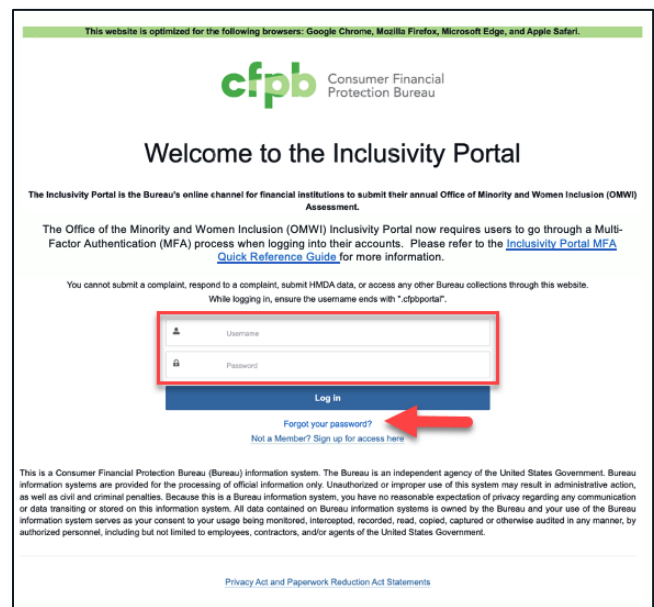

Step 3: Access the Inclusivity Portal

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Inclusivity Portal.

## Step 4: Login with Existing Inclusivity Portal Username and Password

Enter your existing **'Username'** and **'Password'** into the login screen. Ensure the username ends in ".cfpbportal."

If you have forgotten the Password, use the **'Forgot Your Password'** link below the **'Login'** button.
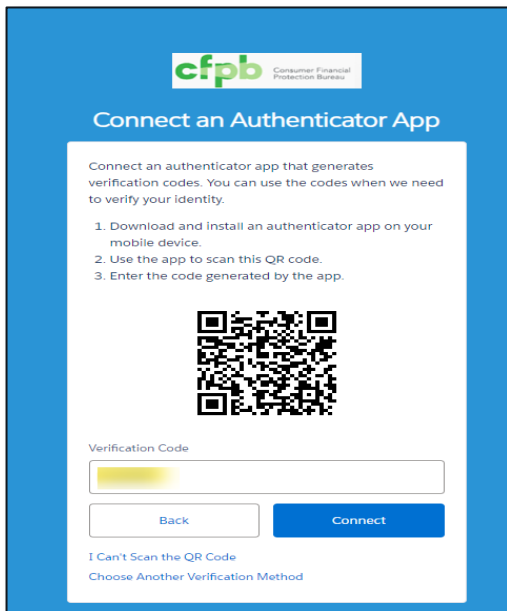
Step 5: Choose the Windows MFA Verification Method

On the **'Choose a Verification Method'** screen, select the **'Use verification codes from an authenticator app'** option. Click **Continue**.
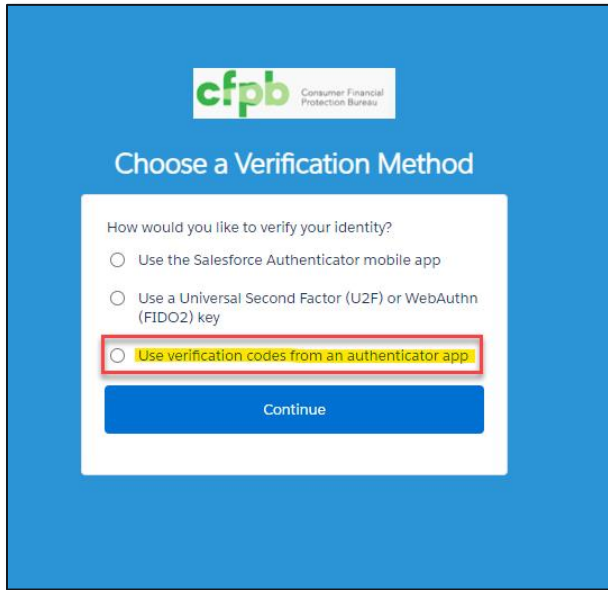
## Step 6: The Connect an Authenticator App Screen Opens

The following screen appears and should remain open.

## Step 7: Return to the Microsoft Authenticator on Your Mobile Device

Open the Microsoft Authenticator app on your mobile device if not still open and select the **Scan a QR Code** option box (see below).

Note: If not previously selected and prompted for Camera options, select "While using the app" option.
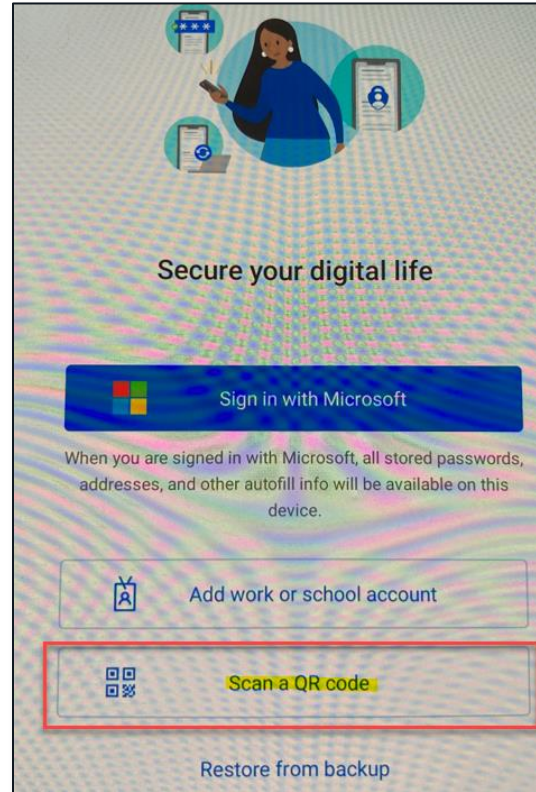
Step 8: Use Your Mobile Device Camera To Scan the QR Code

With the camera on your mobile device open, scan the QR code shown in Step 7 (previous page). Once successfully scanned, the account will register and appear in the Microsoft Authenticator app on your mobile device. Select the Account name in the Microsoft Authenticator app on your mobile device and a One-time password code will appear (see below).
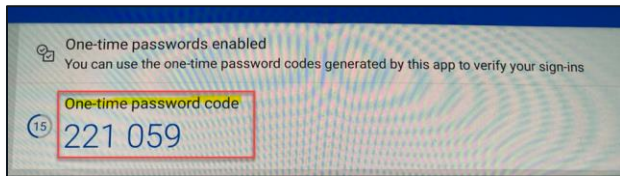
Step 9: Enter the One-time Password Code In Connect an Authenticator App Screen

Return to your browser and enter the code in the Connect an Authenticator App screen (see below: and select **Connect.**
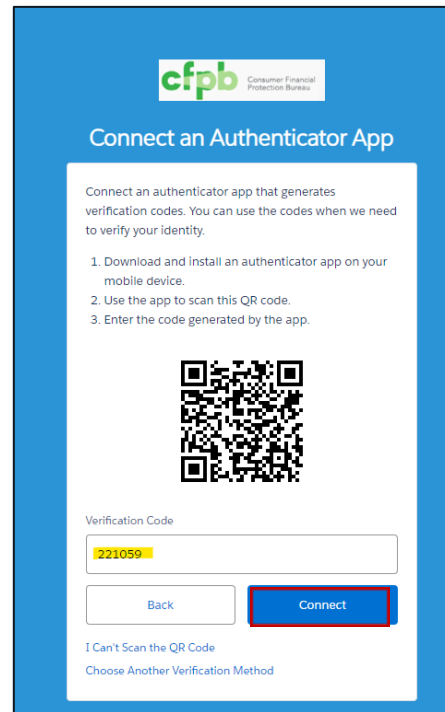
Step 10: Access the Inclusivity Portal

You should now successfully access the site.

Note: In the future, after entering your username and password, you will be prompted to Choose a Verification Method. Again, select the Use Verification Code from an Authenticator app. Return to your mobile device, open the Microsoft Authenticator app (or the app chosen for authentication), select the registered account and generate a new code. Enter that code in your browser and select Connect to finish logging in.

Steps to Access the Inclusivity Portal Using the Windows/Apple (iOS) Desktop Application for MFA

Note: These instructions will follow the installation and use of a Windows MFA application, however the process to install an Apple (iOS) MFA application follows the same basic steps but begins with accessing the Apple store to locate an iOS desktop MFA application.

Step 1: Install a Windows Desktop MFA Application

If you do not have a Windows Desktop MFA application already installed on your desktop/laptop, visit the Microsoft Store and type in "MFA" in the Search box and select the Enter key.

The Microsoft Store will display a range of MFA apps to select (see below). Select the application that your organization's Cybersecurity team has approved. *Note: These instructions depict an example of one Desktop MFA application and CFPB does not endorse any approved application over any other .*

Select the **TOTP Manager** Authenticator and select the **Get** or download button. Follow the prompts to install.
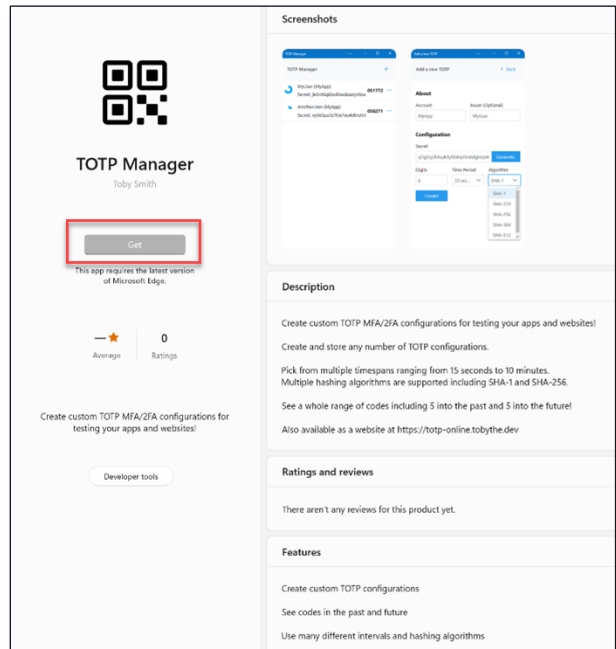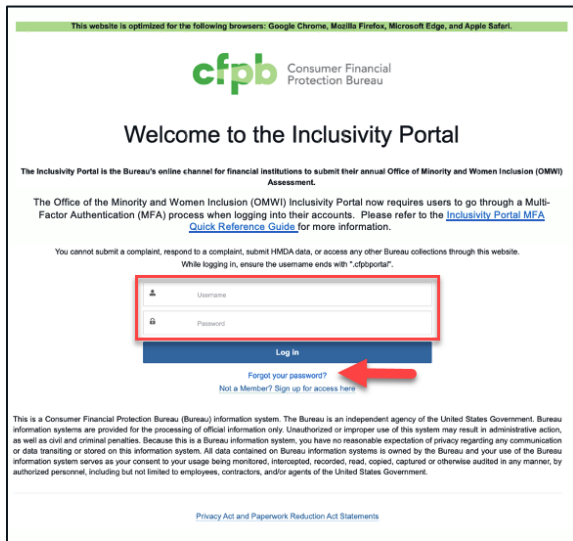

Step 2: Access the Inclusivity Portal

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Inclusivity Portal.
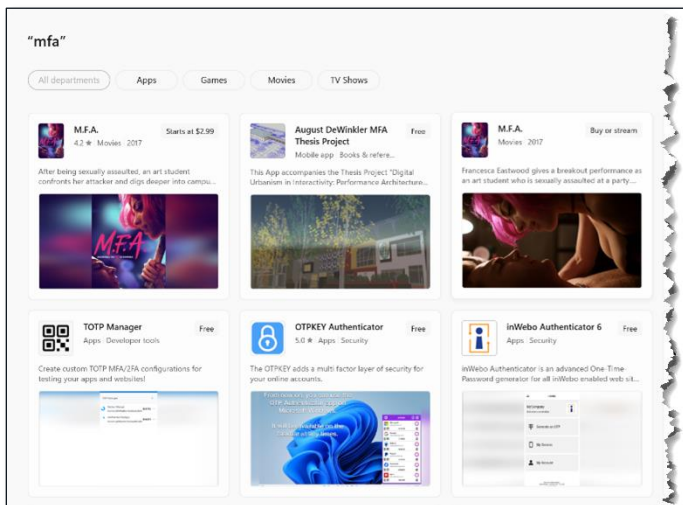
## Step 3: Login with Existing Inclusivity Portal Username and Password

Enter your existing **'Username'** and **'Password'** into the login screen. Ensure the username ends in ".cfpbportal."

If you have forgotten the Password, use the **'Forgot Your Password'** link below the **'Login'** button.

Step 4: Choose the Windows MFA Verification Method

On the **'Choose a Verification Method'** screen, select the **'Use verification codes from an authenticator app'** option and select **Continue**.
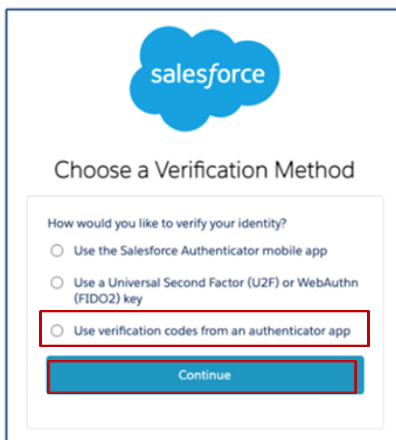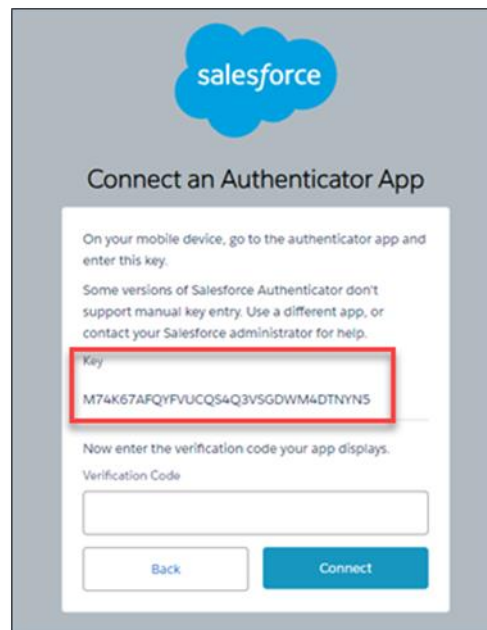

Step 5: Connect an Authenticator App

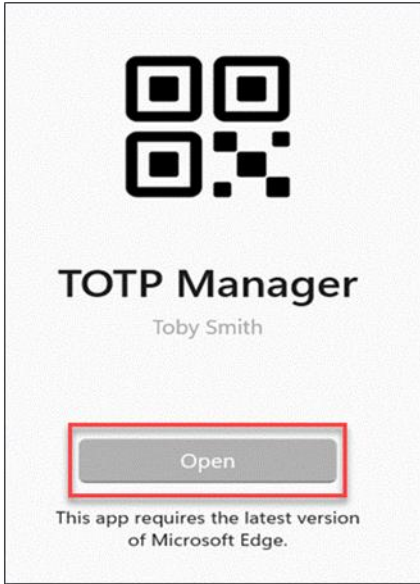When the **Connect an Authenticator App** screen appears, select **I Can't Scan the QR Code**.
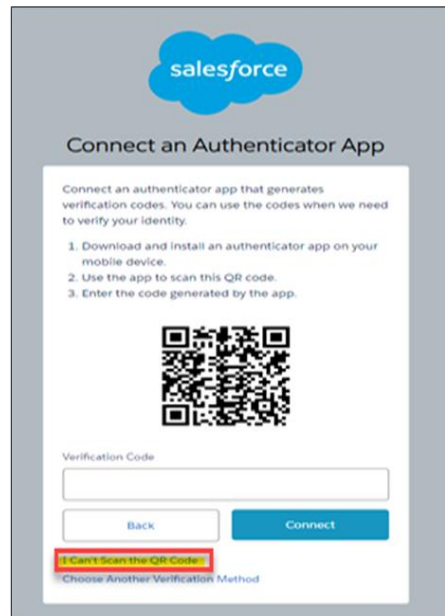
A numeric key will be generated in the **Key** section. Copy this key to be used in a later step.

.

Step 6: Complete Authenticator App Verification

Return to the installed Authenticator application, e.g., TOTP Manager, and follow the prompts.


Select the **+ sign** to add a credential.

On the next screen, enter **Inclusivity** into the **Account** field. Paste the **Key** copied at the end of Step 5 into the **Secret** field and select **Create**.

A six-digit code will be created, e.g., **404140**. Copy the number.

Return to the **Connect an Authenticator App** screen, enter or paste from your clipboard the six-digit code in to the **Verification Code** box and select **Connect**.
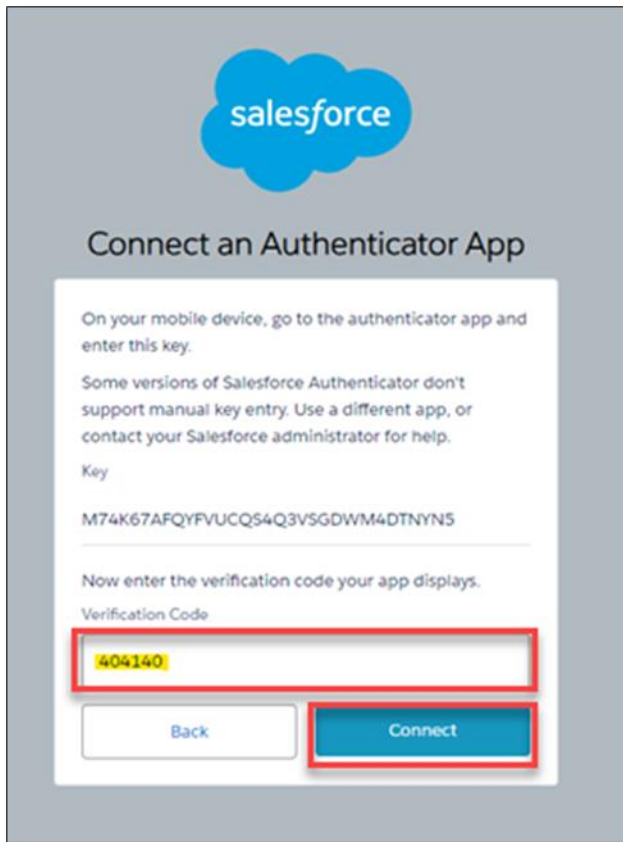
This should complete your MFA authentication process.
Note: Salesforce may ask that you re-login and enter the MFA code during the log-in process.

Steps to Access the Inclusivity Portal Using a Universal Second Factor (U2F) or WebAuthn (FIDO2) Key (e.g., a YubiKey) for MFA

If you wish to use this option, follow the known channels through your Cybersecurity team and/or IT department to request an approved device. Once

approved and received, follow the steps below or as designated by your IT department. The following steps describe the use of a *YubiKey device, but other approved devices follow similar steps.*

Step 1: Access the Inclusivity Portal

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Inclusivity Portal.

Step 2: Login with Existing Inclusivity Portal Username and Password

Enter your existing **'Username'** and **'Password'** into the login screen. Ensure the username ends in ".cfpbportal."
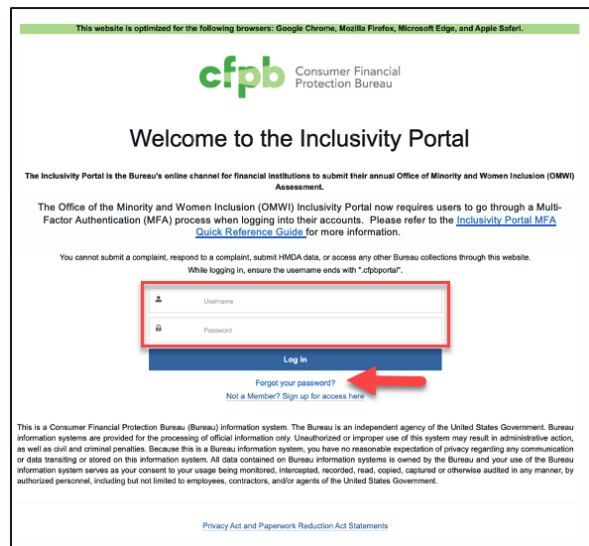
If you have forgotten the Password, use the **'Forgot Your Password'** link below the **'Login'** button.

Step 3: Choose the Universal Second Factor (U2F) or WebAuthn (FIDO2) key method (specifically the use of a YubiKey)

On the Choose a Verification Method screen, select the **Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) Key** option and select **Continue**. You will be directed to the Register a Security Key screen.
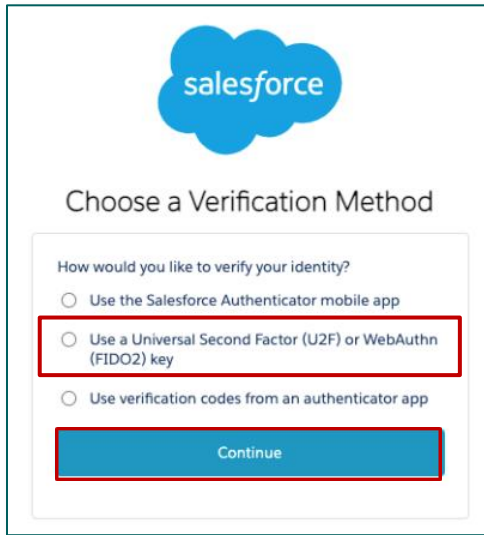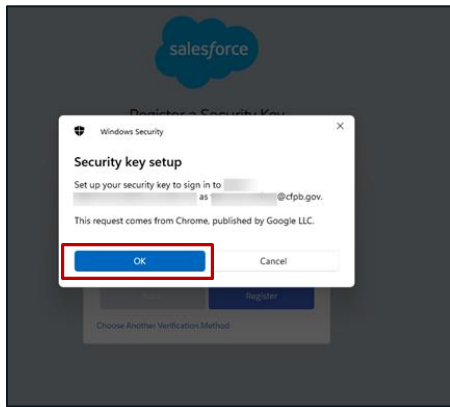

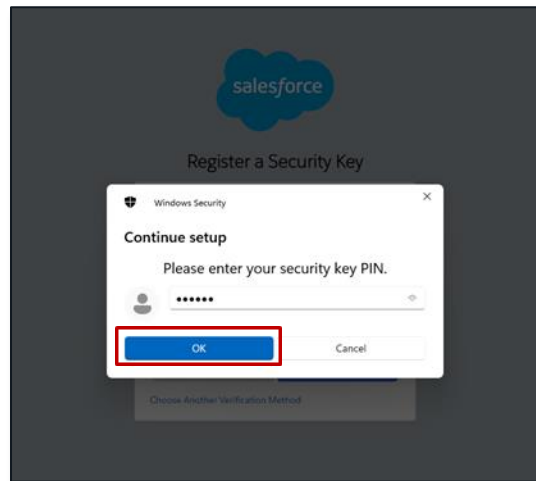## Step 4: Register and Set Up Your Security Key

On the **Register a Security Key** screen Follow the instructions, insert your security key into a USB port, touch a button (if it has one), and then select **Register.**

cfpb Consumer Financial Protection Bureau
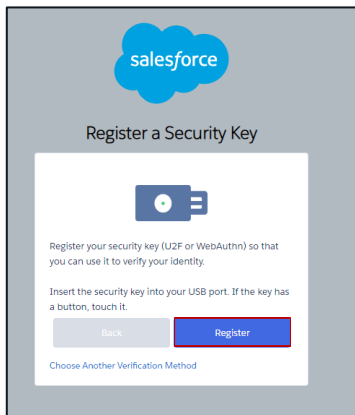
The **Security key setup** screen will appear, with text that advises you are setting up the key to sign-in to the Inclusivity Portal URL with your designated username. Select **OK**.

On the **Continue setup** screen, a confirmation of your security key (i.e., YubiKey) allowing the Inclusivity Portal to see your security key. Select **OK.**


On the next **Continue setup** screen, enter the security key PIN that you created when you obtained your key (i.e., YubiKey). Select **OK**. *Note: The PIN would have been setup by you when you obtained it; contact your Cybersecurity and/or IT department if you have any issues.*
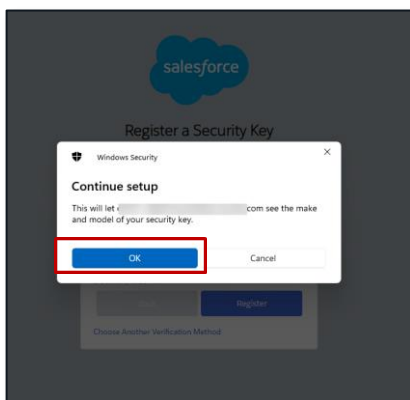
On the next **Continue setup** screen, follow the instructions to "**Touch your security key**".

Consumer Financial
Protection Bureau
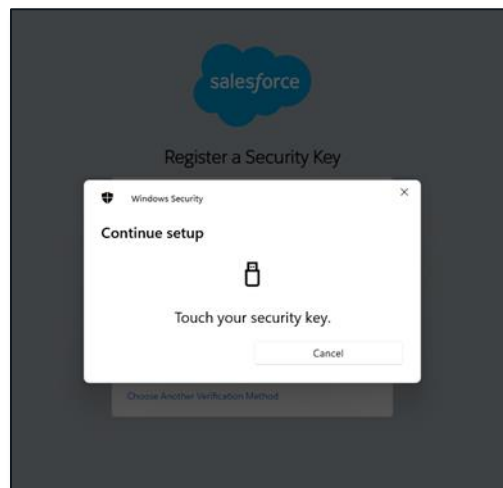
Step 4: Verify Your Identity (with your Security Key, e.g., YubiKey)

The **Verify Your Identity** screen will appear after touching your security key in the previous step. This series of steps verifies you and the security key for future logins. Verify the information presented and select **Verify**.
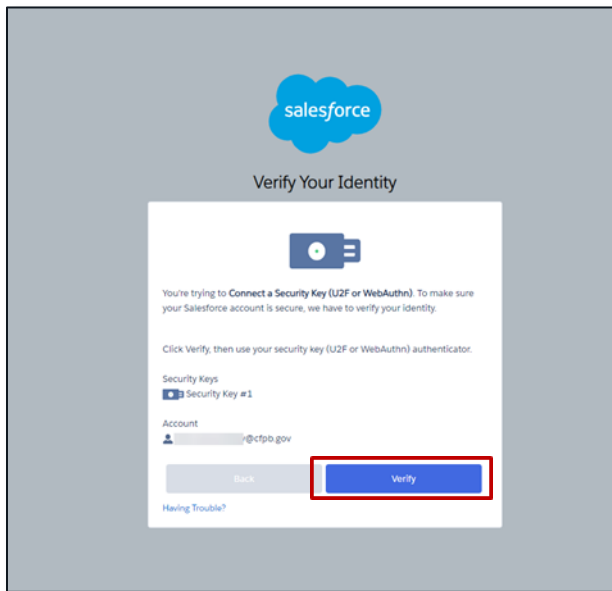
On the **Making sure it's you** screen, re-enter your security key pin. Click **OK**. *Note: Like Step 3 above, the PIN would have been setup by you when you obtained your security key; contact your Cybersecurity team and/or IT department if you have any issues.*
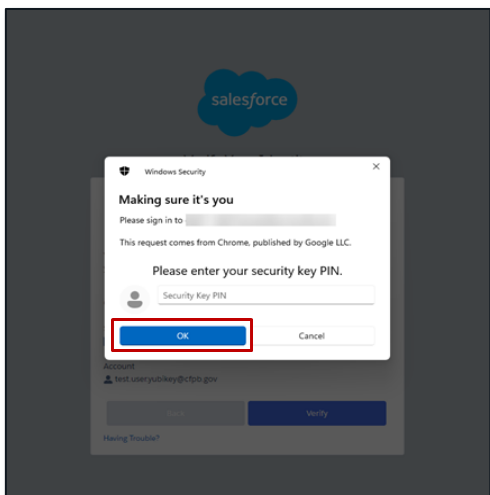
Step 5: Next and Subsequent Logins to the Inclusivity Portal

Upon the next login, and any future logins, to the Inclusivity Portal enter your username and password; you will be prompted to use your security key. Touch the security key, e.g., YubiKey, and you will immediately be logged in.

Inclusivity Portal Support

If you have any questions regarding MFA or experience any issues, please send us an email, detailing the MFA issue in the subject line at OMWI_diversityassessments@cfpb.gov