

Nonbank Registry (NBR) Portal Multi-Factor Authentication (MFA) Quick Reference Guide

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

The NBR Portal will require users to go through an MFA process when logging in. This means that users have to provide additional information or credentials, apart from their username and password, to access the NBR Portal.

MFA is a security technique that verifies a user's identity by requiring them to provide multiple pieces of information or credentials to protect your account from unauthorized access or cyber-attacks. After establishing your NBR Portal password, you will be prompted to set up your preferred MFA method on your next login attempt. In practice, using MFA means that each time you log into the NBR Portal, you will be prompted to enter a code sent to your registered device, answer security questions, or use an authenticator app.

CFPB requires all its users to take advantage of this feature and ensure their accounts are as secure as possible.

MFA Overview

What is MFA?

MFA is a way for NBR Portal users to securely log into the portal that requires using "factors" to verify (authenticate) 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

NOTE: Follow the guidance of your organization's Cyber Security for installing one of these supported MFA methods.

When accessing the NBR 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

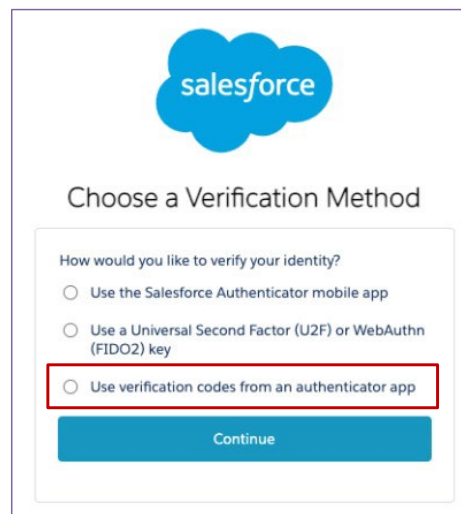
The Salesforce Authenticator mobile app is simple to install, use, and connects to your NBR Portal account. Once set up, you will receive a push notification to your mobile device that can be used to approve the secondary authorization request to login. As needed, the Salesforce Authenticator mobile 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. (See [Steps to Access NBR Portal using the Salesforce Authenticator App](#) for detailed instructions).

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

The NBR Portal also supports a wide variety of 3rd party verification mobile and desktop 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 NBR Portal account.

You can download the 3rd party authenticator mobile apps from the Google Play or Apple App Store. Follow the prompts to install and use the mobile apps. Follow the detailed instructions in [Steps to Access NBR Portal using the Salesforce Authenticator App](#), however when you reach the **'Choose a Verification Method'** screen, select the **'Use verification codes from an authenticator app'** option. (see below)



You can download 3rd party authenticator desktop applications from the Microsoft Store or Apple Store. (See [Steps to Access NBR Portal Using Windows/Apple \(iOS\) Desktop MFA Application.](#))

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.

Steps to Access NBR 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 NBR Portal

Using a compatible browser (Google Chrome, Mozilla Firefox, or Microsoft Edge) access the NBR Portal at <https://nbr.consumerfinance.gov/s/login>.

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 NBR 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.

Step 3: Login with your NBR Portal Username and Password

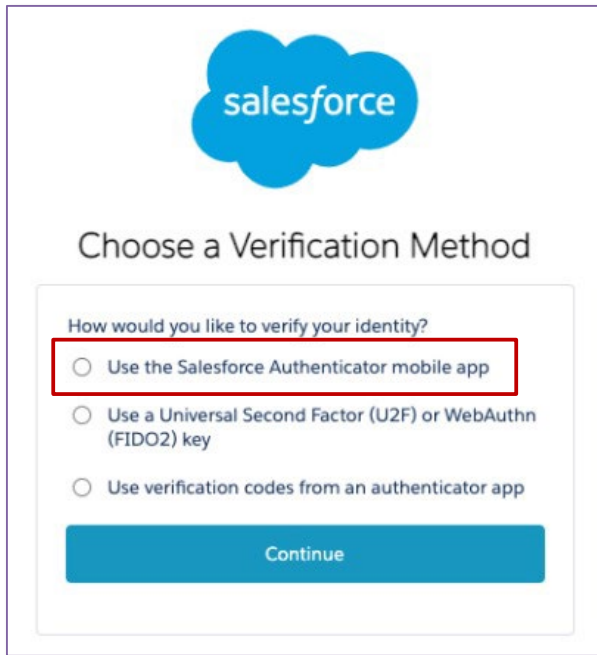
Enter your existing '**Username**' and '**Password**' into the login screen.

The screenshot shows the login interface for the NBR Portal. At the top left is the 'cfpb' logo, followed by the text 'Consumer Financial Protection Bureau'. The main heading is 'Sign in to your account'. Below this are two input fields: 'Username' and 'Password'. Under the 'Password' field is a link that says 'Forgot your password?'. A green button labeled 'Sign In' is positioned below the input fields. At the bottom of the form area, there is a link for 'Privacy and PRA Statements' and a note: 'If you are the point of contact and want to register your company with the NBR, click here'.

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.



salesforce

Choose a Verification Method

How would you like to verify your identity?

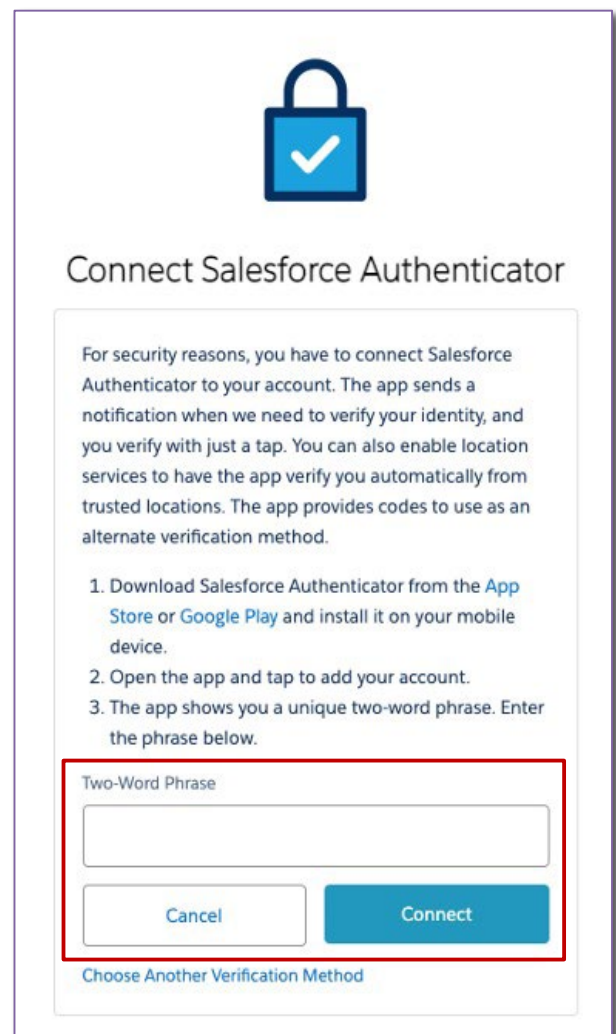
- Use the Salesforce Authenticator mobile app
- Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key
- Use verification codes from an authenticator app

Continue

Step 5: Connect the Salesforce Authenticator Mobile App

When users first access the NBR 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.



Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

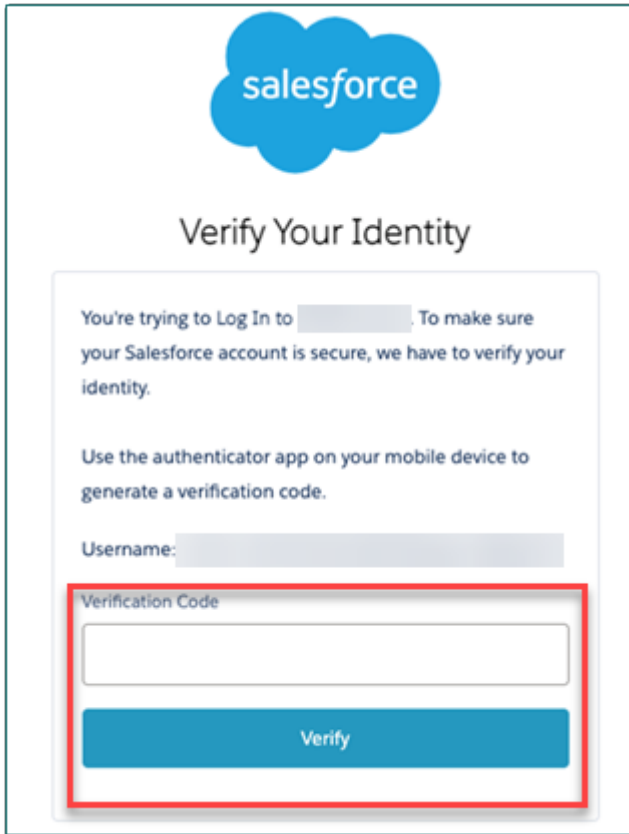
Two-Word Phrase

Cancel Connect

[Choose Another Verification Method](#)

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.



The screenshot shows the Salesforce 'Verify Your Identity' screen. At the top is the Salesforce logo. Below it is the title 'Verify Your Identity'. The main content area contains the following text: 'You're trying to Log In to [redacted]. To make sure your Salesforce account is secure, we have to verify your identity.' Below this is the instruction: 'Use the authenticator app on your mobile device to generate a verification code.' There is a 'Username:' label with a corresponding input field. Below that is a 'Verification Code' label with a large input field, which is highlighted with a red border. At the bottom of the form is a blue 'Verify' button.

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

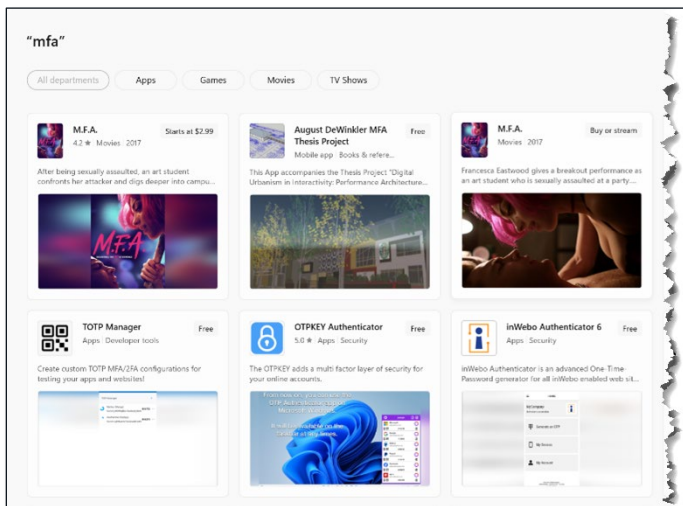
Steps to Access NBR Portal Using the Windows/Apple (iOS) Desktop MFA Application

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

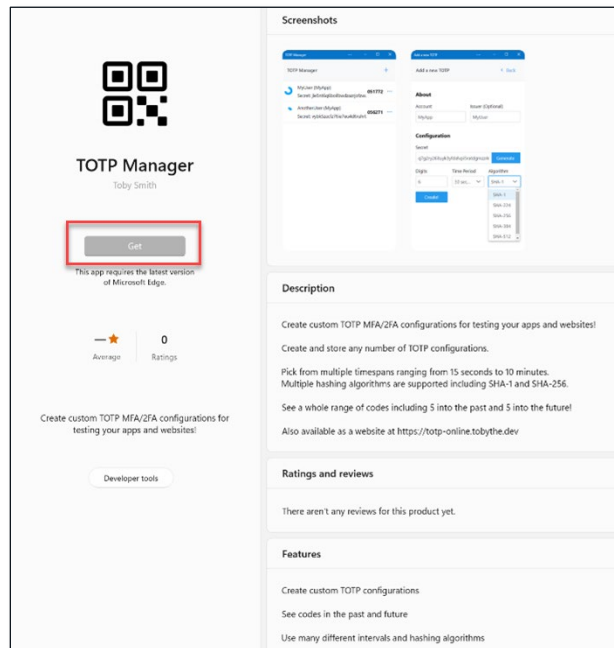
If you do not have a Windows Desktop MFA application already installed on your desktop/laptop, visit the Microsoft Store and type in “MFA” in the Search box and select the Enter key.

The Microsoft Store will display a range of MFA apps to select (see below). Select the application that your organization’s Cyber Security has approved.



[For these instructions, “TOTP Manager” will be used as an example.]

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



Step 2: Access the NBR Portal

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

<https://nbr.consumerfinance.gov/s/login>.

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 NBR Portal users to:

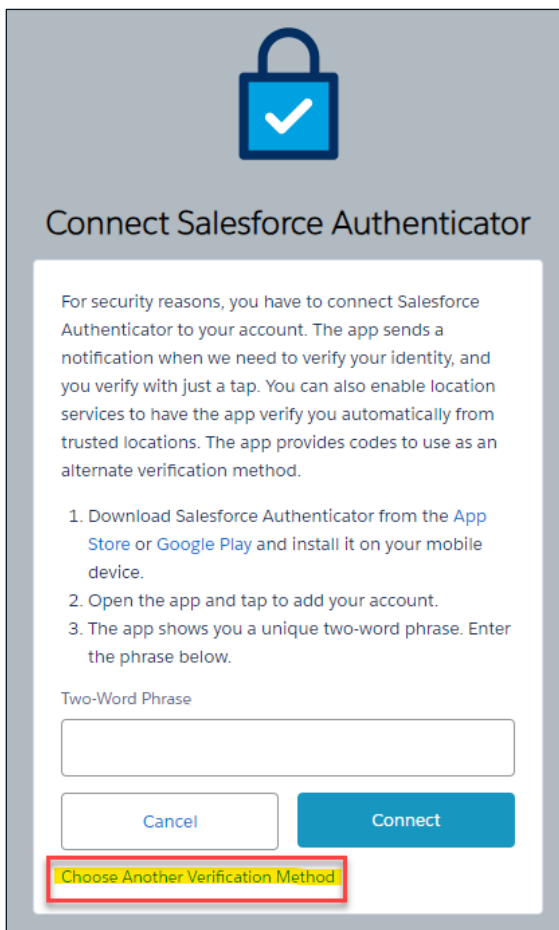
1. Use the most recent version of the browser listed above and keep it up-to-date with the latest security patches and updates;

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.

Step 3: Login with your NBR Portal Username and Password

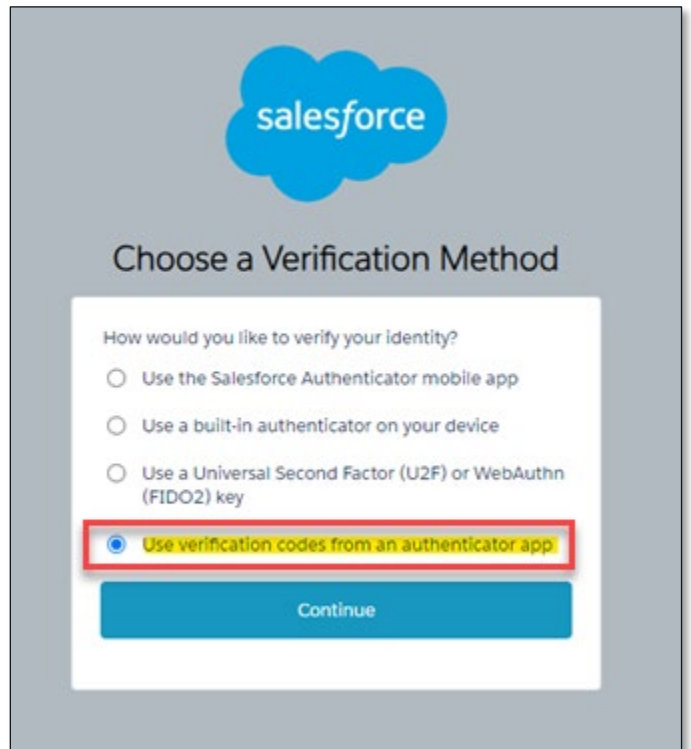
Enter your existing **'Username'** and **'Password'** into the login screen.

After entering Username and Password, Salesforce will prompt you to Connect Salesforce Authenticator. Select "Choose Another Verification Method."



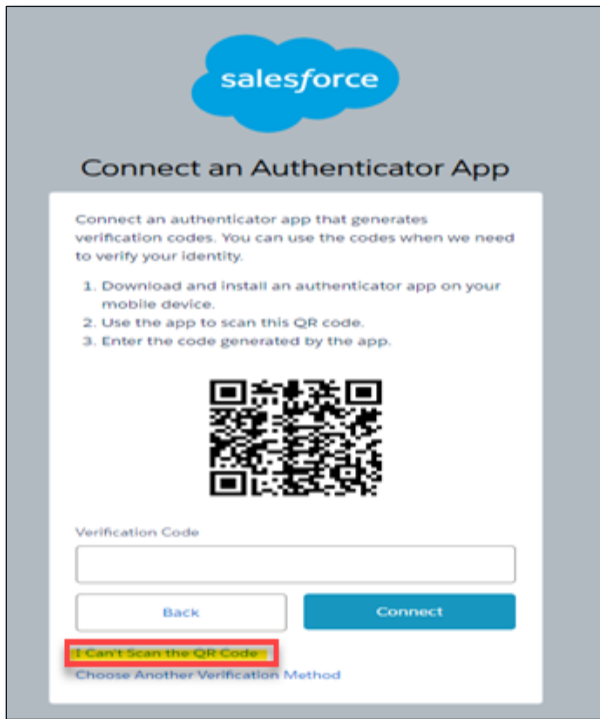
Step 4: Choose a Verification Method

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

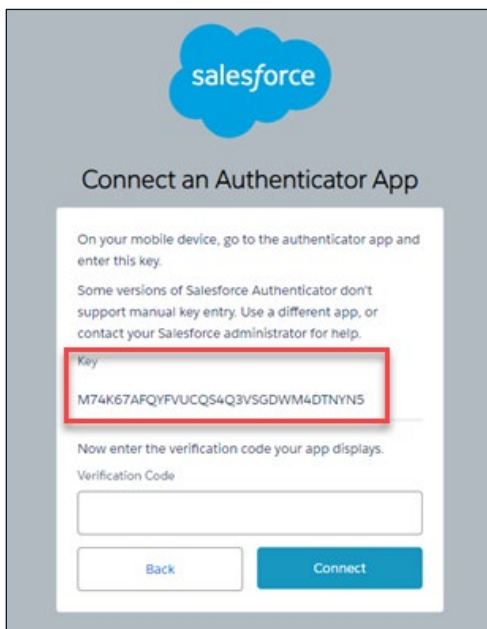


Step 5: Connect an Authenticator App

When the “Connect an Authenticator App” screens appears, select “I Can’t Scan the QR Code”.

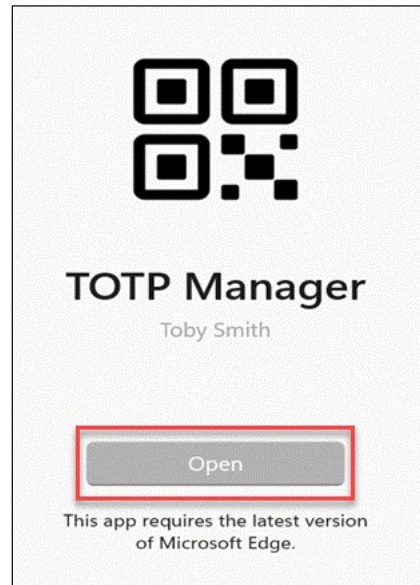


A numeric key will be generated in the “Key” section. Copy this key to be used in a later step.



Step 6: Complete Authenticator App Verification

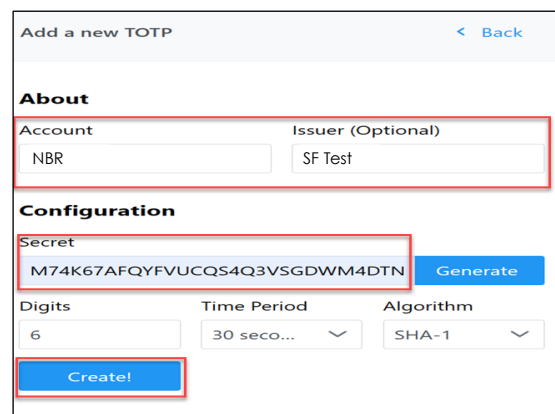
Return to the installed Authenticator application, e.g., TOTP Manager, and follow the prompts.



Select the “+” sign to add a credential.



Enter or paste from your clipboard the “Key” copied at the end of Step 5 into the “Secret” box; enter the Account info as “NBR”, and select “Create”.



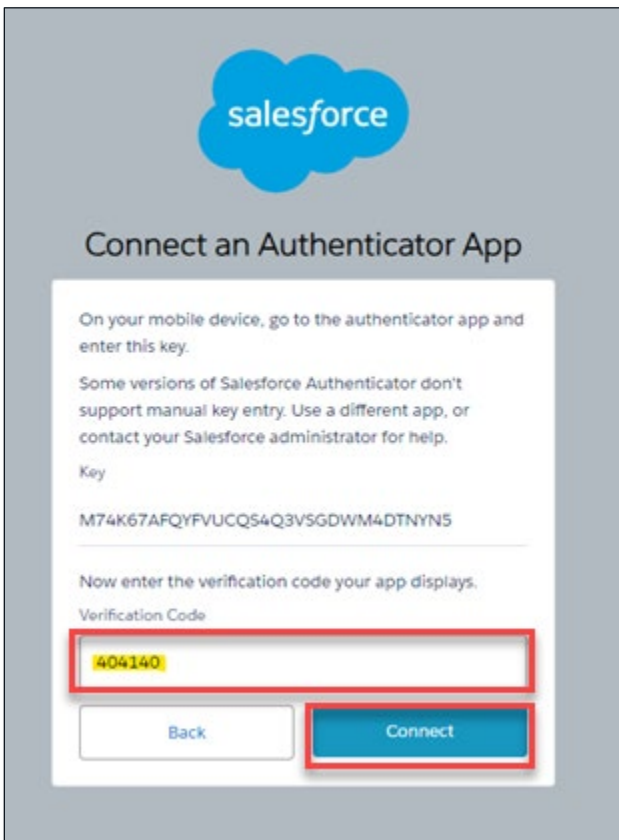
A six digit code will be created, e.g., “404140”; copy the number.



NBR 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 NBRHelp@cfpb.gov.

Returning to the Salesforce 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.