

## Multifactor Authentication (MFA)

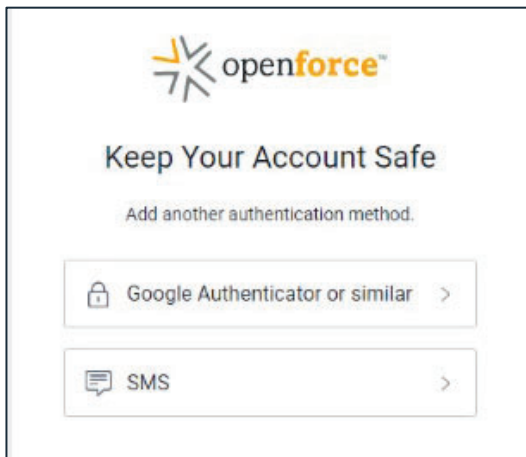
To increase the security of Openforce accounts and personal information, all users are required to enroll in multifactor authentication (MFA).

When logging into your Openforce account, you will be prompted to input a verification code that confirms your identity.

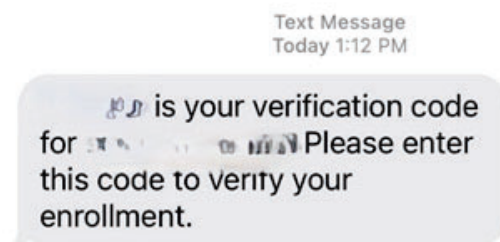
There are two methods for receiving verification codes, SMS (text message) or an authenticator app. Below outlines what to expect when choosing either option:

### Option 1: SMS/Text Message

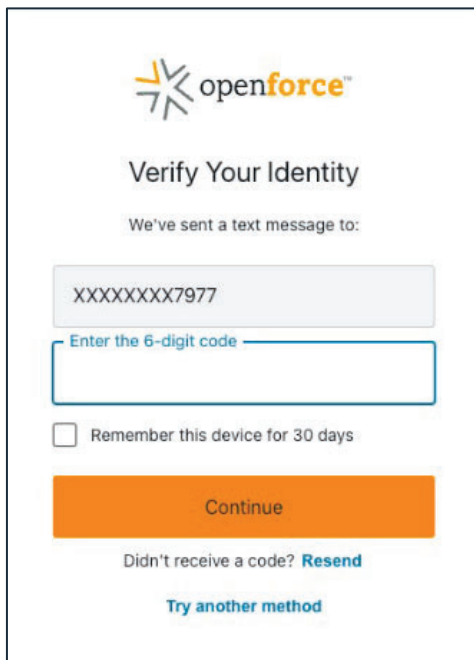
1. Enter your Openforce username and password.
2. You'll be prompted to choose your preferred method of receiving verification codes. For SMS/Text, **click "SMS"**.



3. Enter your preferred mobile phone number. An SMS/Text with a 6-digit code will be sent to the mobile phone number provided.

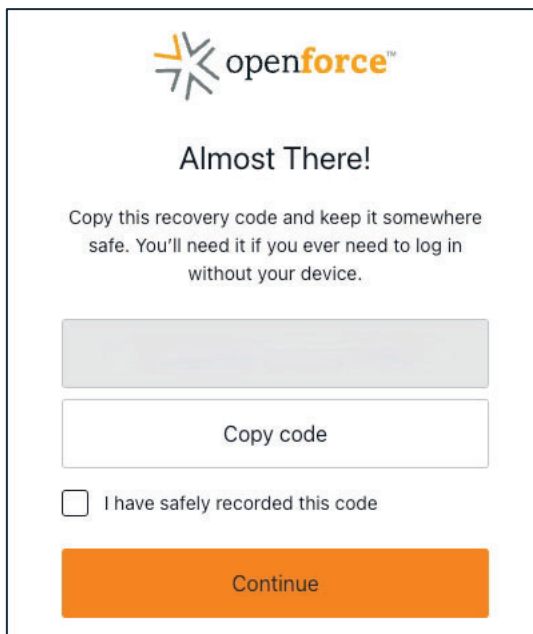


4. Enter the verification code you received via SMS/Text message.



NOTE: Selecting “Remember this device for 30 days” will store your verification data and only prompt you to submit a verification code after 30 days, or if logging in from a device not recognized.

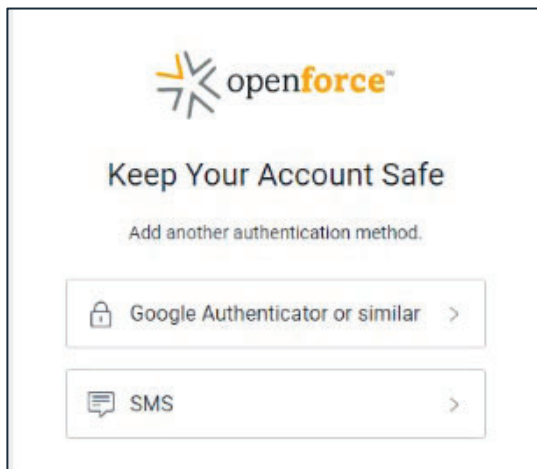
5. You are now enrolled with MFA. Be sure to save and store your MFA recovery code provided in a secure location. You can use this code to access your account in the event you lose access to your previously selected MFA option.



NOTE: Should you lose this recovery code, you will need to contact Openforce Support to restore your MFA settings.

## Option 2: Authenticator App

1. Enter your Openforce username and password.
2. You'll be prompted to choose your preferred method of receiving verification codes. **Click “Google Authenticator or similar”.**

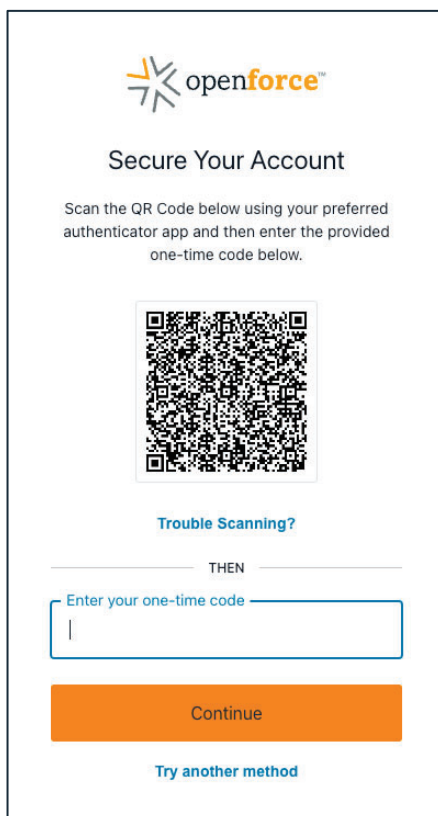


NOTE: You can use any authenticator app, as long as the app can scan QR codes.

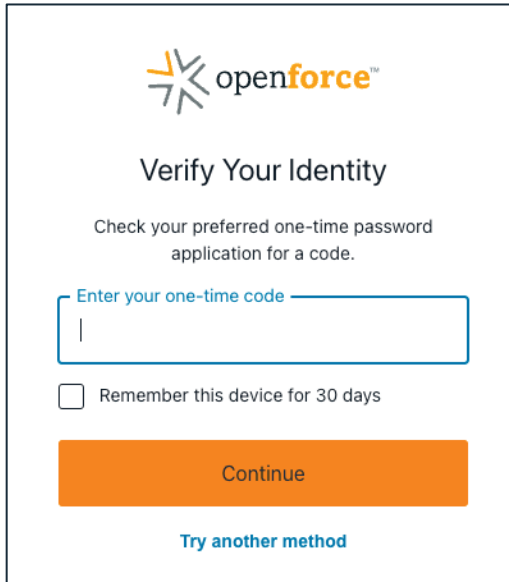
Authenticator apps can be downloaded from the app store on your mobile device.

Commonly used authenticator apps: Duo Mobile, Microsoft Authenticator, Google Authenticator, Authy.

3. Using your chosen authenticator app, scan the QR code provided and enter your one-time verification code.

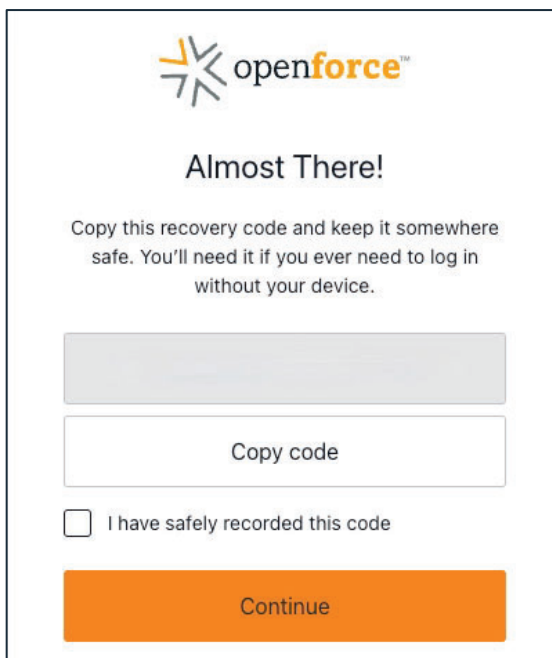


4. Your chosen authenticator app is now saved as your primary MFA method. You will be prompted to provide a new code from that app at each login.



NOTE: At your next login, selecting “Remember this device for 30 days” will store your verification data and only prompt you to submit a verification code after 30 days, or if logging in from a device not recognized.

5. Be sure to save and store your MFA recovery code provided in a secure location. You can use this code to access your account in the event you lose access to your previously selected MFA option.



NOTE: Should you lose this recovery code, you will need to contact Openforce Support to restore your MFA settings.

## Frequently Asked Questions (FAQs):

### **What is multifactor authentication (MFA)?**

Multifactor authentication (MFA) is an electronic authentication method that requires the user to provide two or more forms of identity unrecognized device being used to gain access and asked to confirm the identity via multifactor authentication (MFA), often by providing a code sent to a mobile device or using biometrics through an authentication application.

### **How does MFA work?**

MFA works by requiring two or more verification methods – or factors – to prove you’re whom you say you are before you can log in. By requiring multiple types of evidence to confirm your identity, it’s much harder for a bad actor to gain access to your account. Even if your password becomes compromised, an attacker still needs your other factor to log in. It is widely adopted as a security measure for both personal and business networks; it works by identifying an unrecognized device being used to gain access and asking to confirm the identity via multi-factor authentication (MFA), often by providing a code sent to a mobile device or using biometrics through an authentication application.

### **Who will be required to use MFA to login into the Openforce portal?**

All users accessing their Openforce account will be required to enroll with MFA.

### **What methods can be used for enrolling in MFA?**

There are two methods that can be utilized for MFA, SMS/Text or a preferred Authenticator App.

### **Will I have to authenticate every time they log in?**

No. Selecting “Remember this device for 30 days” on the authentication screen during login saves your verification data and only prompts you to re-authenticate after 30 days, or if logging in from a device not recognized.

### **What if I’m not receiving the SMS code, or my authenticator app isn’t working?**

If you’re unable to gain access to your account with the original option they enrolled with, you can use the recovery code provided at the time of enrolling in MFA.



This code should be saved and stored in a secure location. If the user loses access to their previously selected MFA option, they can use this code to access their account and change the MFA options.

The recovery code is not saved within the portal therefore, it will not be a recovery option if it's not saved by the user in a secure location or is lost.

If you do not have access to the recovery code, contact Openforce Support to have your MFA reset.

### **Can Openforce Support help if I can't log in or lost my recovery code?**

Yes. Openforce Support can assist users that are locked out of their accounts.

### **What happens if my preferred method is SMS/Text, but I change my phone number?**

If you chose the SMS option for MFA and no longer have access to that phone number, call Openforce Support who can assist in resetting your MFA.

NOTE: Openforce Support cannot reset MFA via email requests and must be done over the phone.