# Quick Reference Guide (QRG)

# Step-by-Step
# Multi-Factor Authentication

# Table of Contents

## What is Multi-Factor Authentication (MFA)?

MFA is a two-factor authentication security method used to provider two or more forms of identification before granting access to an account or system.

Examples of identification include:

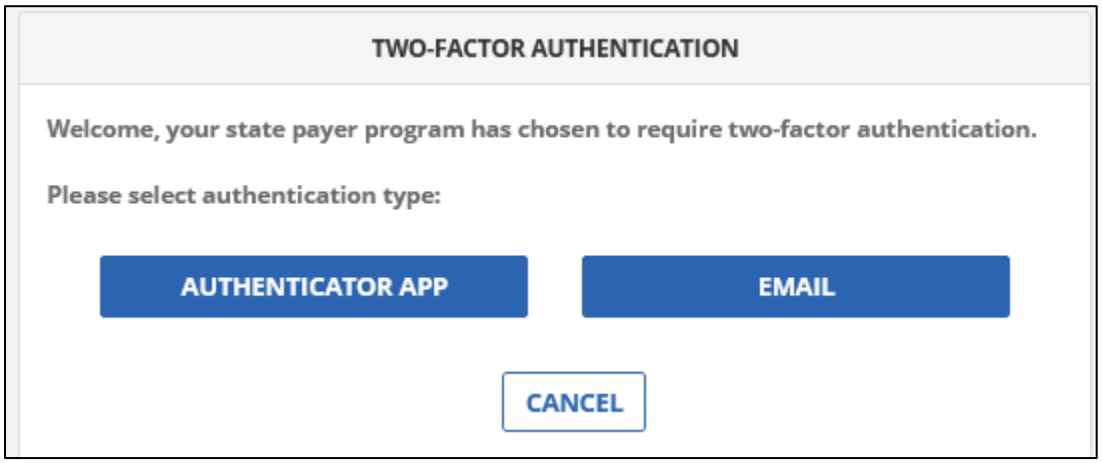
- Personal knowledge: passwords, knowledge-based answers, personal identification numbers (PIN), etc.
- Devices: mobile device, pin code, key fob, etc.
- Biometrics: fingerprint, retinal pattern, voice, etc.

MFA is essential for securing online accounts, particularly those containing sensitive information. MFA adds an extra layer of security protection and makes it more difficult for unauthorized users to access an account even if they have obtained or bypassed the password.

## Enabling MFA for the California Electronic Visit Verification (CalEVV) Portal and Aggregator

Authentication can be validated by using one of the following methods to verify identity:

- Email address associated with your CalEVV user profile
- Google Authenticator application
- Microsoft Authenticator application

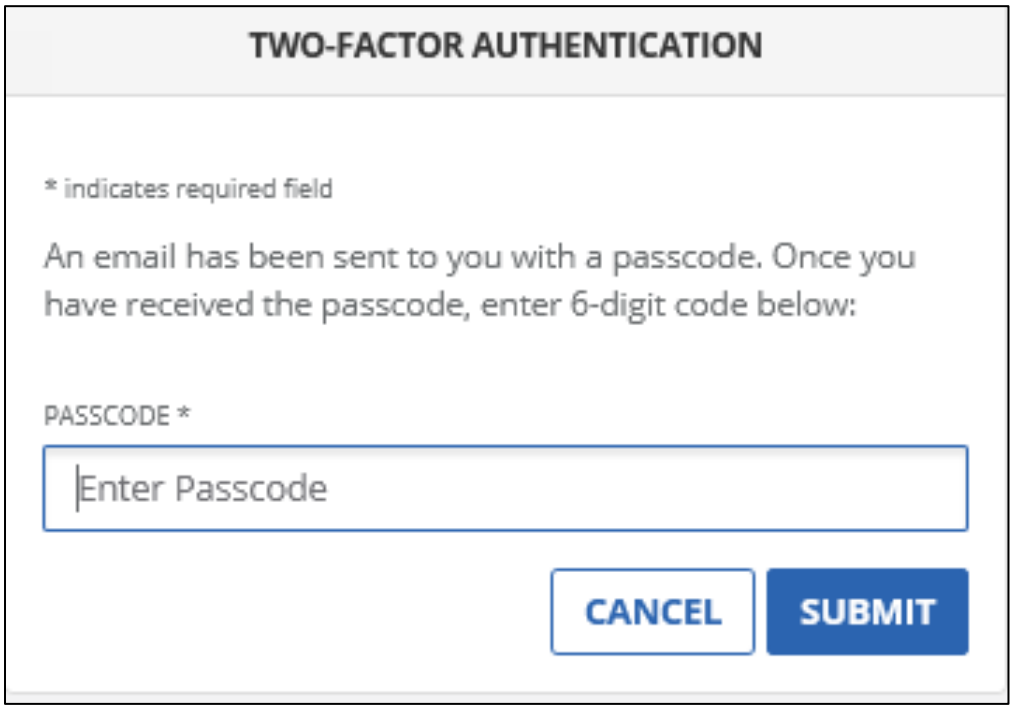



MFA will be required:

- Every 12 hours regardless of activity, or
- Whenever a user logs into the CalEVV system from a new device

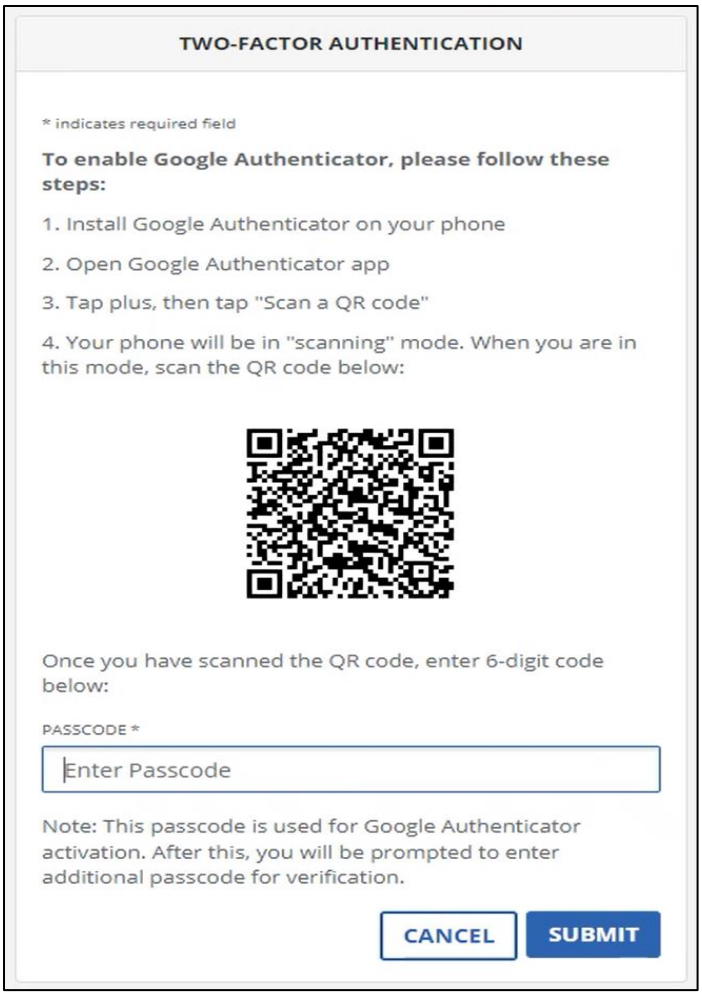
## MFA Using Email

1. You will receive an email from noreply@okta.com.
    - Check your Spam/Junk folder
2. Open the email, scroll down to the one-time verification code.
3. Copy and paste the code into CalEVV MFA when prompted.
4. Click SUBMIT.



## MFA Using Authenticator Application

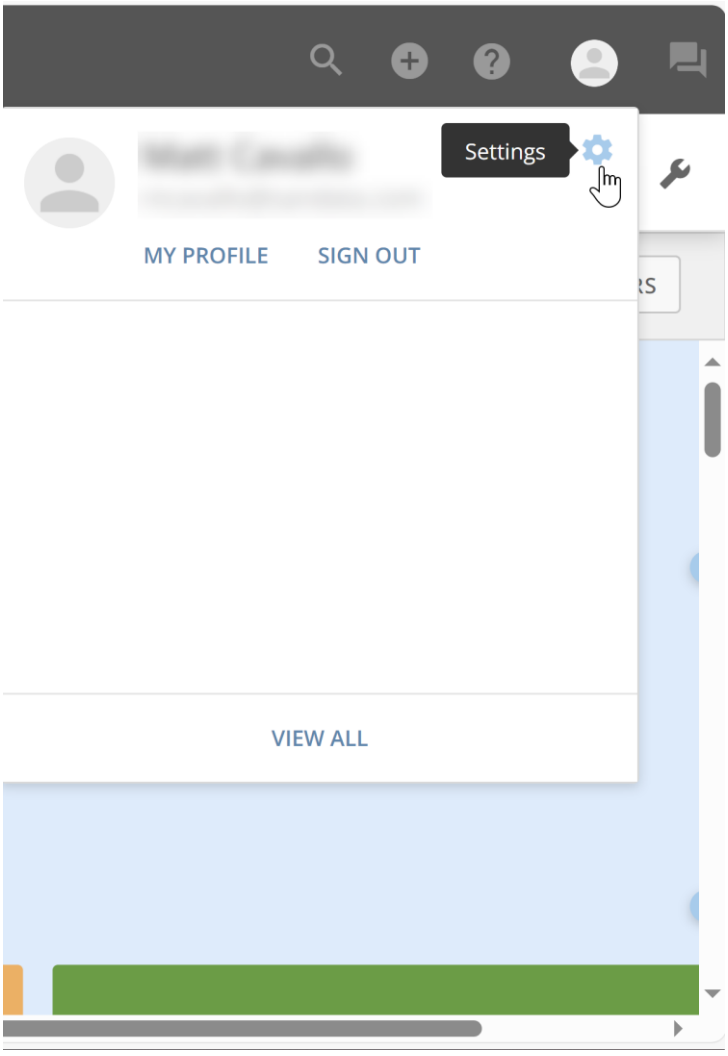
1. Download either the Google Authenticator or Microsoft Authenticator application.
    - Please note the prompts lists Google Authenticator, but CalEVV MFA is compatible with both Microsoft and Google Authenticator.
2. Open the application.
3. When prompted, scan the QR code to link to your CalEVV account.
4. Retrieve the passcode from the application.
5. Enter the passcode into CalEVV MFA when prompted.
6. Click SUBMIT.



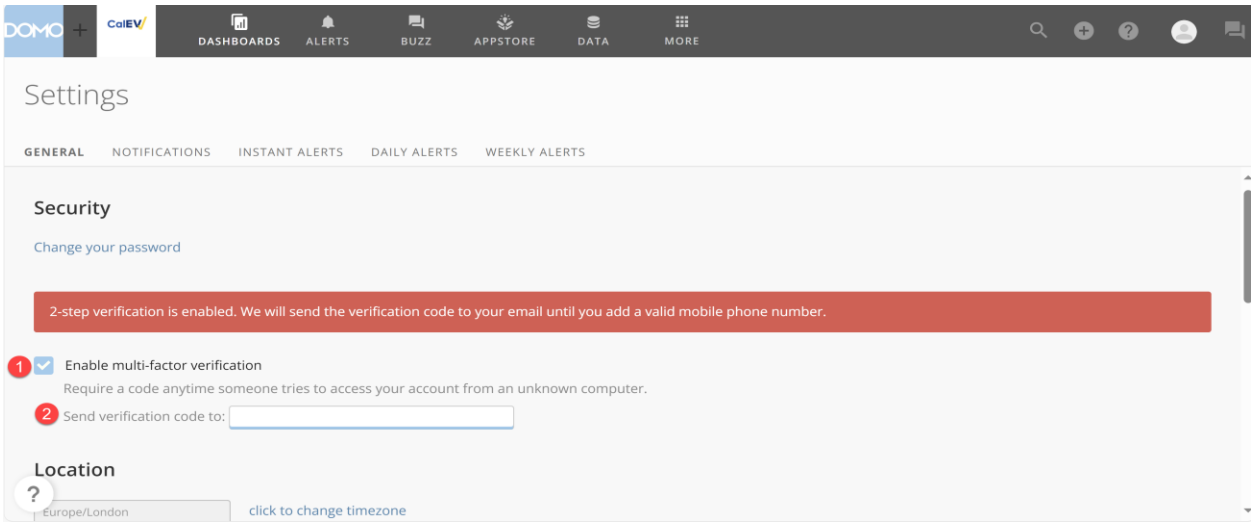

If you get locked out of entering your MFA passcode, please call the Sandata Customer Support team at 855-943-6070 or email CACustomerCare@sandata.com.

# Enabling MFA for the CalEVV Business Intelligence (BI) Tool (DOMO)

1. Log onto the CalEVV BI Tool
2. Click on the Profile icon 
3. Click on the Settings icon 



4. Check the box next to **Enable multi-factor authentication**.
5. Enter your mobile phone number in the **Send verification code to** field.
    - MFA is now enabled and will be required at next login.




6. Once you log into the CalEVV BI Tool, you will be prompted to enter an MFA verification code. This code request will appear prior to each login.
7. The code will be sent via text message to the phone number that was added in the previous step.
8. Retrieve the code from your text message and enter it into the field provided.
9. Click VERIFY.