

Multi-Factor Authentication (MFA) Setup Guide

User Reference Document

This document provides step-by-step instructions for setting up and using Multi-Factor Authentication (MFA) in the CalAmp VDOT System.

1. Overview

Multi-Factor Authentication (MFA) adds an extra layer of security to the VDOT system by requiring a second verification step during login. The VDOT system uses a Time-based One-Time Password (TOTP) mechanism.

Users must download a compatible authenticator application (such as the Microsoft Authenticator app) on their mobile device to generate temporary, secure verification codes.

2. First-Time MFA Registration Flow

This setup happens only the first time a user logs into the VDOT system.

Step 1: Access the Landing Page

- Navigate to the VDOT system login URL.
- Click the SIGN IN button on the right-hand panel of the landing page.

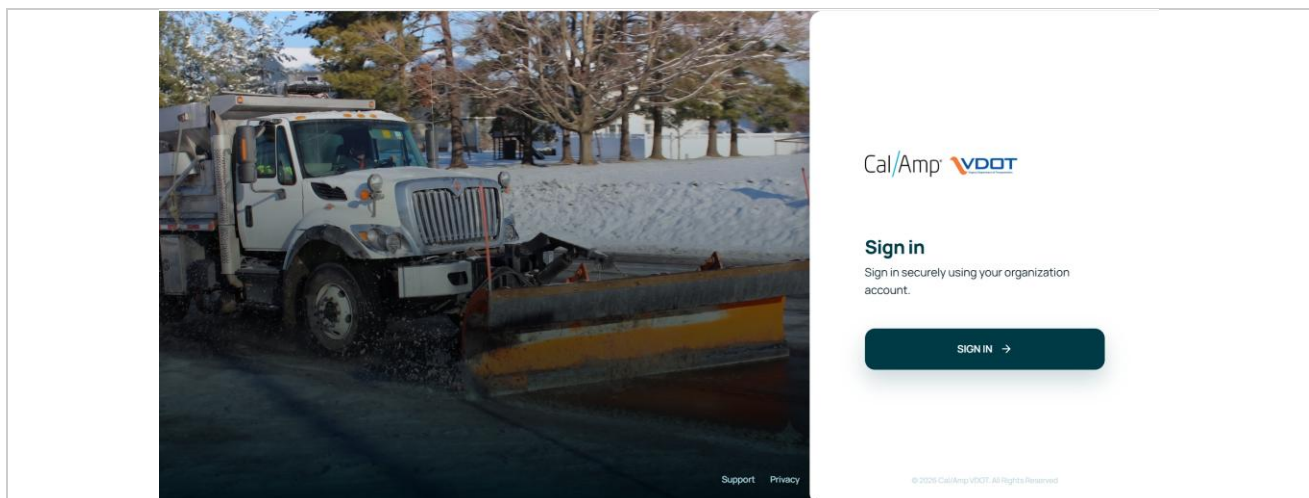


Figure 1 — VDOT Landing Page

Step 2: Enter Account Credentials

- You will be redirected to the authentication page.
- Enter your organization Username / Email and Password.
- Click SIGN IN to proceed.

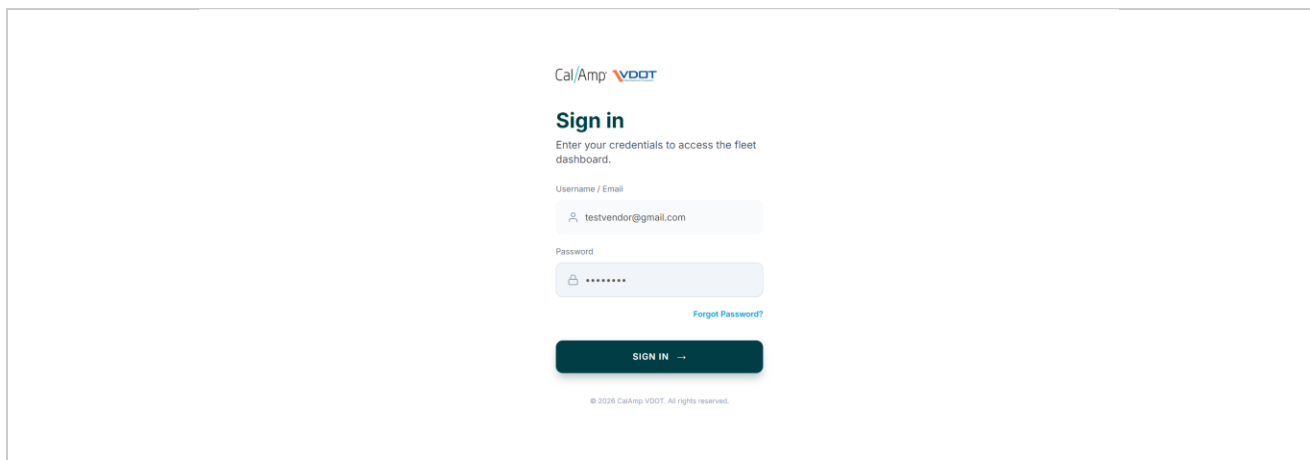


Figure 2 — Auth0 Login Credentials Page

Step 3: Prerequisites for MFA

Before registering for Multi-Factor Authentication (MFA), install a compatible Time-Based One-Time Password (TOTP) authenticator application on your mobile device.

The VDOT System supports any standard TOTP-compatible authenticator application. The following applications are commonly used and recommended:

Authenticator Application	iOS (App Store)	Android (Google Play)
Microsoft Authenticator <i>(Recommended)</i>	Apple App Store	Google Play Store
Google Authenticator	Apple App Store	Google Play Store
Cisco Duo Mobile	Apple App Store	Google Play Store

Recommendation: Microsoft Authenticator is the preferred application for the CalAmp VDOT. However, any authenticator application that supports the **TOTP (Time-Based One-Time Password)** standard can be used successfully.

Note: Ensure the authenticator application is installed on your mobile device before beginning the MFA registration process. During the initial setup, you will use the application to scan the QR code displayed by the VDOT system and generate a six-digit verification code required to complete registration.

Step 4: Register Authenticator via QR Code

- Upon your first successful credential entry, the Secure Your Account screen will appear.
- This screen displays a unique QR code.

Action Required on Mobile Device:

1. Open the Microsoft Authenticator app on your phone.
2. Tap the + or Add Account button.
3. Select Work or school account or Other (Google, Facebook, etc.).
4. Scan the QR code displayed on the screen.

The app will now display a 6-digit one-time verification code that refreshes every 30 seconds.

IMPORTANT — One-Time Registration:

This QR code is only shown during this initial registration process. You will not see this QR code on future logins, preventing the account from being added to another authenticator app unless your MFA is reset by an administrator.

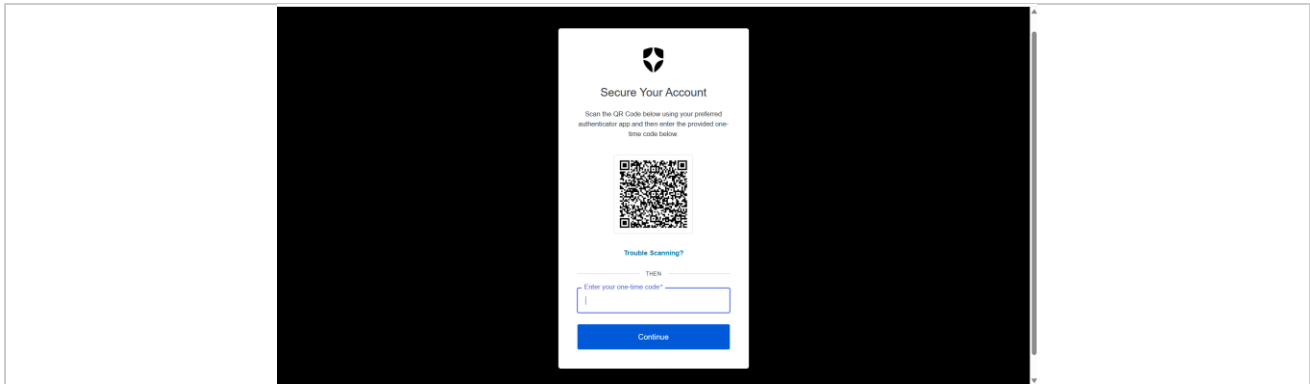


Figure 3 — Secure Your Account (QR Code Page)

Step 5: Complete Registration

- Enter the 6-digit verification code from your authenticator app into the Enter your one-time code field.
- Click Continue.
- Once verified, you will be automatically redirected to the VDOT system dashboard according to your assigned user role.

3. Subsequent Login and Trusted Device Option

After completing the initial MFA registration, Multi-Factor Authentication will be required each time you sign in to the CalAmp VDOT System. To improve the user experience on trusted devices, you may choose to remember your current browser and device for **30 days**.

Step 1 – Sign In

1. Navigate to the CalAmp VDOT System login page.
2. Click **SIGN IN**.
3. Enter your **Username/Email Address** and **Password**.
4. Click **SIGN IN**.

Step 2: Enter Verification Code & Trust Device

After your credentials have been authenticated, the **Verify Your Identity** page will be displayed.

1. Open the authenticator application on your registered mobile device.
2. Retrieve the current **6-digit verification code**.
3. Enter the verification code into the **Enter your one-time code** field.

Remember This Device

To reduce the frequency of MFA prompts on a trusted device:

Select the **Remember this device for 30 days** checkbox.

Click **Continue**.

NOTE:

The **Remember this device for 30 days** option is available only after the initial MFA registration has been completed. It is not displayed during first-time MFA enrolment.

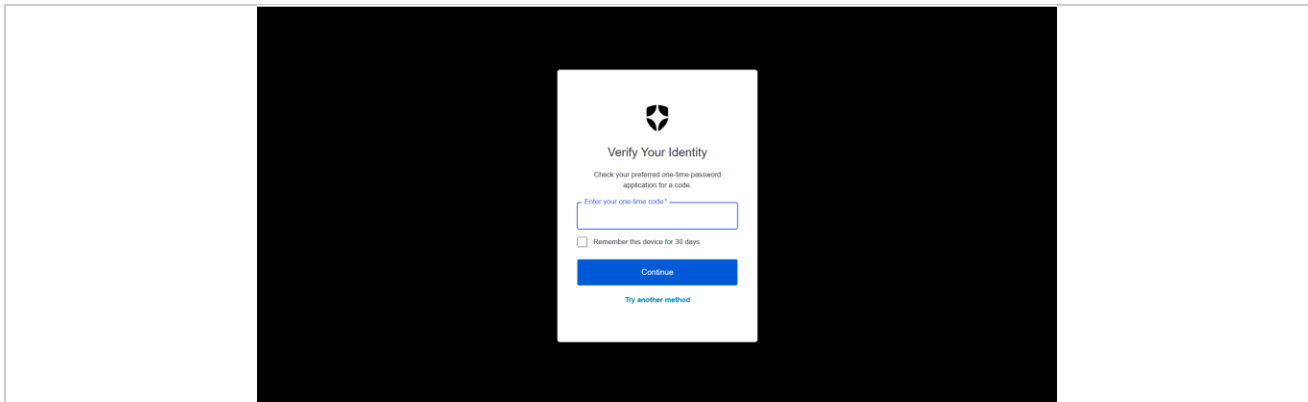


Figure 4 — Verify Your Identity (Remember Device Checkbox)

Alternative Verification Method

If you are unable to access your registered authenticator application (for example, if your mobile device has been lost, replaced, or is unavailable), select Try another method below the Continue button to receive a one-time verification code via your registered email address.

Refer to **Section 4 – Email Verification** for additional information

4. Email Verification

If a user no longer has access to the phone with their authenticator app installed, the VDOT system provides a fallback option to verify identity using email instead of a one-time code from the app.

Step 1: Choose an Alternate Method

- On the Verify Your Identity screen, click Try another method (located below the Continue button).
- The Select a method to verify your identity screen will appear, listing the available verification options for the account.
- Select Email from the list.

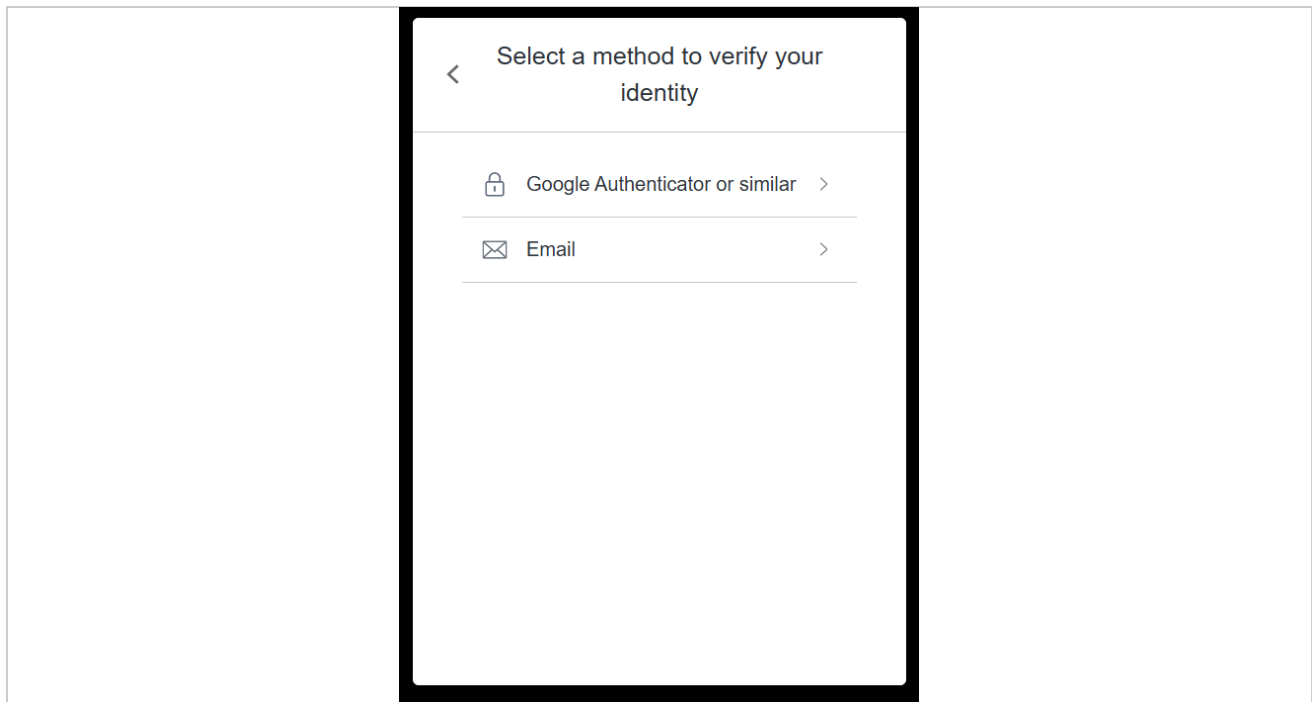


Figure 5 — Select a Method to Verify Your Identity

Step 2: Enter the Emailed Code

- The system sends a one-time verification code to the email address on file, shown in masked form (e.g. `admi*****@gmai*****`).
- Check that email inbox and enter the code into the Enter the code field.
- Optionally, check Remember this device for 30 days to skip MFA on this browser/device for the next 30 days.
- Click Continue to complete sign-in.
- If the email has not arrived, use the Didn't receive an email? Resend link to request a new code.

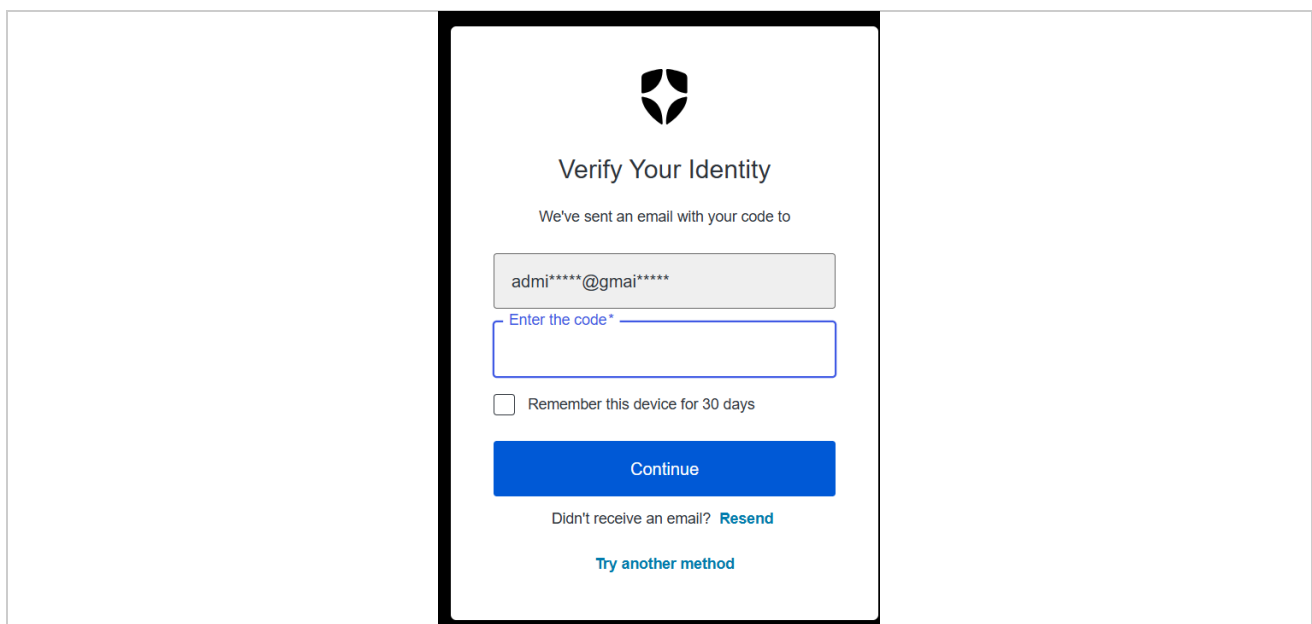


Figure 6 — Verify Your Identity via Email

NOTE:

The **Email** verification option is available only if it has been enabled for your account. If **Email** is not displayed on the **Select a method** screen, email-based verification is not available. In this case, if you are unable to access your registered authenticator application, contact the **VDOT System Administrator** to have your Multi-Factor Authentication (MFA) settings reset.

5. Key Security Rules & FAQ

Can I set up MFA on multiple authenticator apps or devices?

No. MFA enrolment is a one-time process that registers a single authenticator application with your account. After enrolment, the QR code is no longer accessible, preventing additional devices or authenticator applications from being configured.

To register a new device, your existing MFA configuration must first be reset by the **VDOT System Administrator**. Once reset, you can complete the MFA enrolment process again using your new device.

What happens if I change my phone or lose access to my authenticator app?

If you no longer have access to your registered authenticator application, select **Try another method** on the **Verify Your Identity** screen and choose **Email** (if available) to receive a one-time verification code.

If email verification is not available, or you are unable to complete authentication using an alternative method, contact the **VDOT System Administrator** to request an MFA reset.

After your MFA configuration has been reset, your next sign-in will initiate the **First-Time MFA Registration** process, allowing you to register a new authenticator application on your replacement device.