Multi-Factor Authentication

Purpose

The purpose of this document is to describe the .decimal Multi-Factor Authentication (MFA) security features and options available to users of .decimal software applications. This document should provide answers to many of the commonly asked questions regarding MFA and the options available to users.

What is MFA?

Multi-Factor Authentication (MFA) is an extra layer of security to protect an account and confirm an identity when you try to sign in. MFA uses two or more kinds of authentication to verify the user authenticating is who they say they are. Three of the most common kinds of authentication factors are:

- Something you know: Like a password
- Something you have: Like a smart phone
- Something you are: Like a biometric (finger print or facial recognition)

Refer to the cisa.gov or nist.gov articles for more details on what is MFA.

Feature Overview

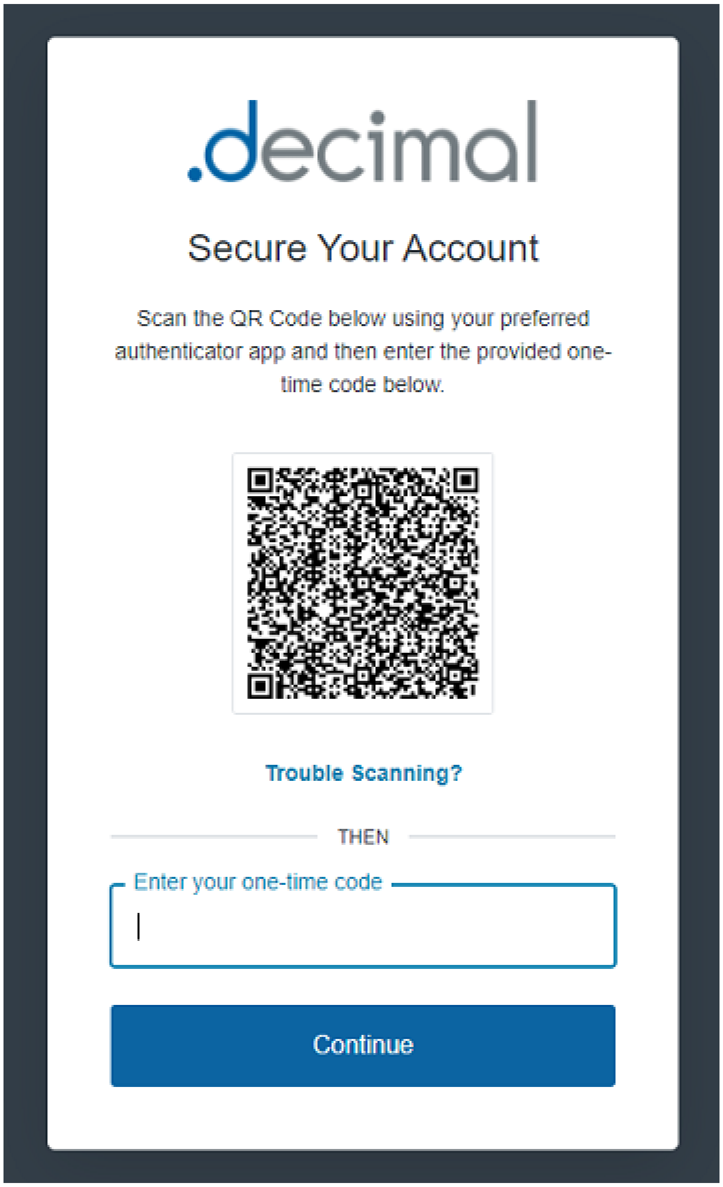
.decimal account logins support enabling MFA for users. The supported MFA types include:

MFA Type	Notes
OTP Code (Time based / Authenticator App)	This includes using apps like Google Authenticator or Authy
Backup MFA: Recovery Code	This is a backup code should the OTP Code / App be lost
Email (coming soon!)	This feature is coming soon - Estimated late 2022

Note: MFA is only available to non 'Legacy' .decimal user logins. If you're unsure if your account supports MFA or wish to be migrated from a 'Legacy' authentication account please contact the .decimal Customer Support team at: Phone: 1.800.255.1613, E-Mail: customersupport@dotdecimal.com.

Enabling/Disabling MFA

Users can enable or disable MFA from within decimal Direct on the user Preferences page. This will allow the user to enroll an OTP application (e.g.: Google Authenticator, Authy, etc) to manage their OPT time based MFA code. Refer to the decimal Direct user guide for detailed instructions.



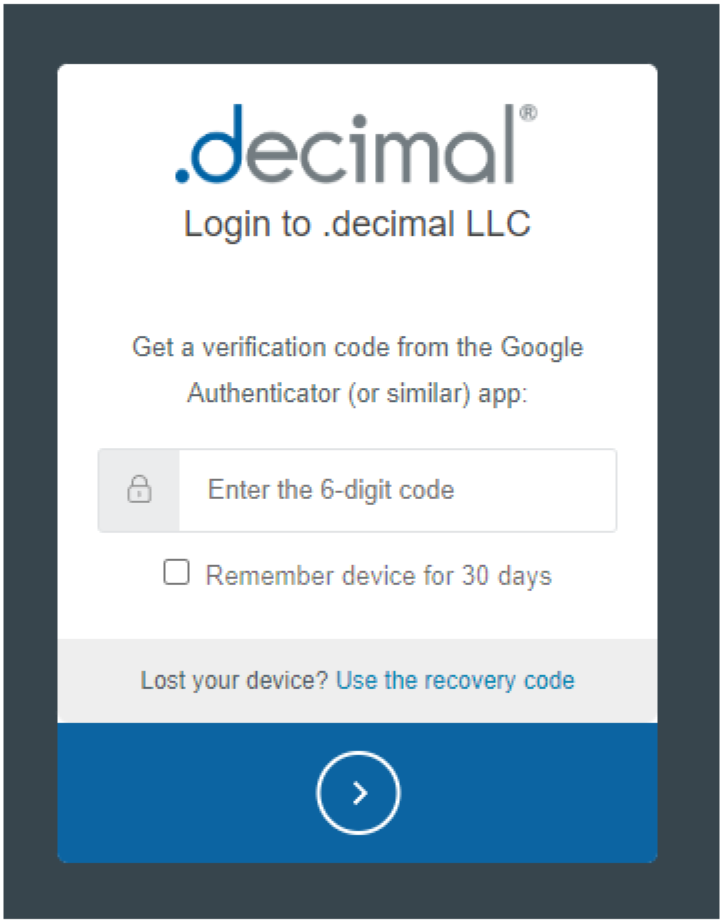
Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

Fig. ##: OPT Registration

Using MFA

Once a user has MFA enabled on their account, the next time they login to a .decimal application they will be required to also provide the MFA code.



.decimal®

Login to .decimal LLC

Get a verification code from the Google Authenticator (or similar) app:

Enter the 6-digit code

□ Remember device for 30 days

Lost your device? Use the recovery code

Fig. ##: OTP Login Prompt

Users can then choose to remember the specific device for 30 days before being required to use the MFA code again.

From:
https://apps.dotdecimal.com/ - **decimal App Documentation**

Permanent link:
https://apps.dotdecimal.com/doku.php?id=support:mfa&rev=1657744751

Last update: **2022/07/13 20:39**