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 describing Multi-Factor Authentication for more details on what is MFA.

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

There are two main use cases for using MFA with your .decimal account:

1. **User Self Management**: Users can elect to enable/disable MFA
2. **Site Manager MFA Management**: Managers can see the status of each user and if they have MFA enabled and choose to force all users to use MFA

Account Compatibility 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.

User Self Management: 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.

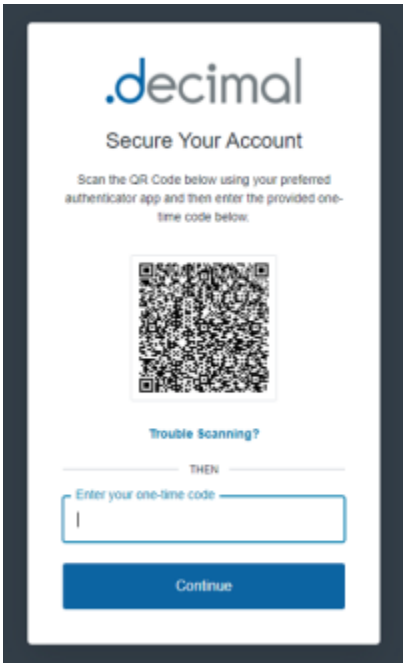

Fig. 1: OPT Registration

Site Managers: MFA Management Options

A Site Manager for a customer organization (e.g.: clinic or hospital IT staff) has a few MFA options for the users they manage:

MFA Status

A Site Manager can view the MFA status of each user within their site within the decimal Direct Site Management → User Management page. Each user will be denoted as whether they have MFA enabled or not.

Require MFA for All Users

A Site Manager or a .decimal employee can require MFA for all users of a specific site within the decimal Direct Site Management → User Management page. Once this option is enabled, the next time each user attempts to login to a .decimal application they will be required to enable MFA for their account. Any additional users added to the site will also be required to set up MFA on their first login. Once a Site Manager has chosen to Require MFA for users within their site users will be unable to manually disable the MFA on their account under the user Preferences page.

Refer to the decimal Direct user guide for detailed instructions.

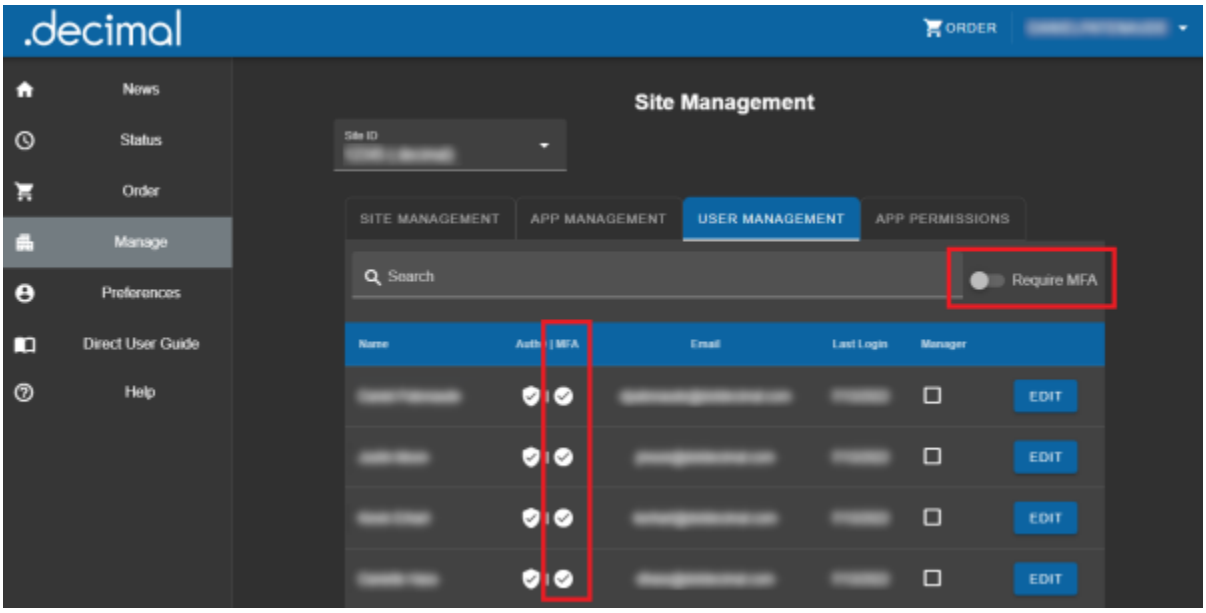

Fig. 2: MFA Management

Logging in with 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.

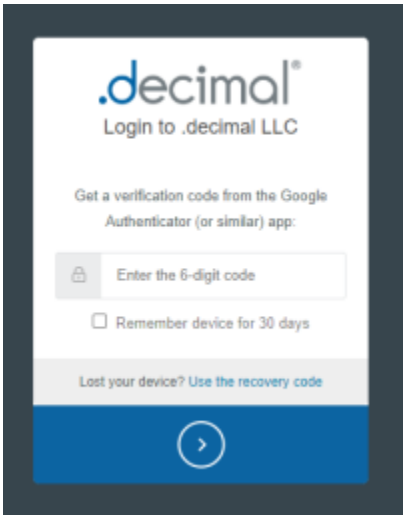

Fig. 3: OTP Login Prompt

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