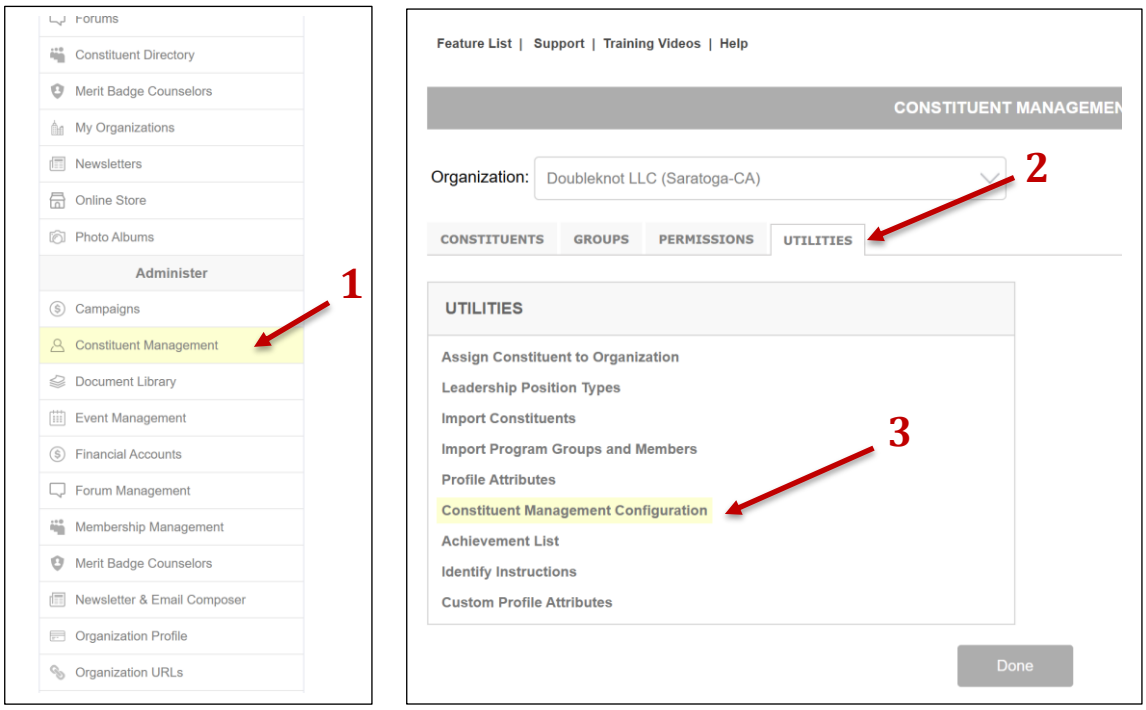
Managing MFA Admin Settings in Doubleknot

This guide provides an overview of the Multi-Factor Authentication (MFA) settings available in Doubleknot's Constituent Management Configuration section. Admins can use these options to customize how MFA is applied across their organization for both administrators and end users.

To configure MFA settings, navigate to: Constituent Management → Utilities → Constituent Management Configuration → Multi-Factor Authentication

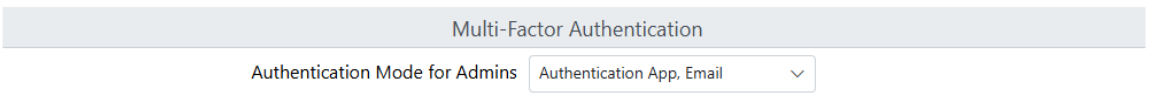


Modes Allowed (Admins)

Select which MFA options are allowed for Admins. At least one option must be selected.

Options:

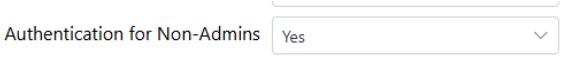
- Authenticator App
- Email



MFA for Non-Admins

Enable or disable MFA for non-admin users (i.e., end users).

Options: Yes / No



Modes Allowed (Non-Admins)

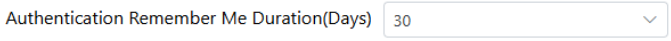
Select MFA modes allowed for end users. This is only active if MFA for Non-Admins is enabled.

Options:
• Authenticator App
• Email

Remember Me Duration (Days)

Controls how long the system should remember a device before prompting for MFA again.

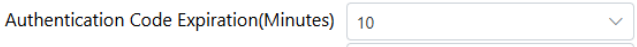
Dropdown values: 30, 60, 90



Code Expiration (Minutes)

Specifies how long an MFA code remains valid once generated.

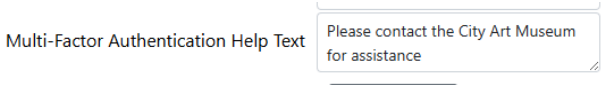
Dropdown values: 10, 15, 20, 25, 30



Help Text

The message shown to users on the Keycloak verification page when a code is requested.

Default text: 'Please contact the “YOUR ORGANIZATION” for assistance.'



Organization’s Logo

Upload a logo that appears on the Keycloak MFA screen for brand recognition.

Upload button + file preview (max file size: 5MB)