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 \rightarrow Utilities \rightarrow Constituent Management Configuration \rightarrow Multi-Factor Authentication

L _v J Forums		
Constituent Directory	Feature List Support Training Videos Help	
I Merit Badge Counselors		
My Organizations		
I Newsletters	Organization: Doubleknot LLC (Saratoga-CA)	
Online Store		
Photo Albums	CONSTITUENTS GROUPS PERMISSIONS UTILITIES	
Administer		
(§) Campaigns	UTILITIES	
Constituent Management	Assign Constituent to Organization	
Document Library	Leadership Position Types	
Event Management	Import Constituents 2	
(\$) Financial Accounts	Import Program Groups and Members	
G Forum Management	Profile Attributes	
Membership Management	Constituent Management Configuration	
Ø Merit Badge Counselors	Identify Instructions	
I Newsletter & Email Composer	Custom Profile Attributes	
Corganization Profile		
% Organization URLs	Done	

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

Authentication for Non-Admins	Yes	~]

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

Authentication Mode for Non-Admins Authentication App, Email \sim

Remember Me Duration (Days)

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

Dropdown values: 30, 60, 90

Authentication Remember Me Duration(Days) 30 \sim

Code Expiration (Minutes)

Specifies how long an MFA code remains valid once generated.

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

Authentication Code Expiration(Minutes)	10 ~	
---	------	--

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.'

Multi-Factor Authentication Help Text	Please contact the City Art Museum for assistance	1

Organization's Logo

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

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

MFA Organization's Logo Select an image