

Two-Factor Authentication (2FA)

OVERVIEW

Two-Factor Authentication (2FA) adds a critical second layer of security to every login. Once enabled, users are guided through a one-time setup using an authenticator app immediately after signing in — ensuring only authorized individuals can access the platform. 2FA can be enforced for all users by an administrator at a site-wide level, or, if not enforced site-wide, can be enabled/disabled individually by each user from their profile settings.

When 2FA is enabled site-wide by an administrator, all users must use 2FA. When it is not enforced site-wide, individual users can enable or disable 2FA for their own account from their profile settings.

WHAT'S NEW

The following capabilities are included in this release:

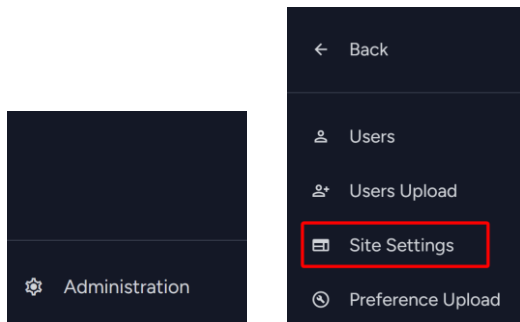
- Site-wide toggle to enforce 2FA for all logins (Administration / Site Settings — first item on the page)
- Individual users can enable or disable 2FA from their own profile settings when it is not enforced site-wide
- QR code setup flow — users scan a QR code with any authenticator app
- 6-digit time-based one-time passcode (TOTP)
- Backup codes displayed after first successful verification — save these for account recovery
- Ability to reset 2FA directly from profile settings

ENABLING 2FA

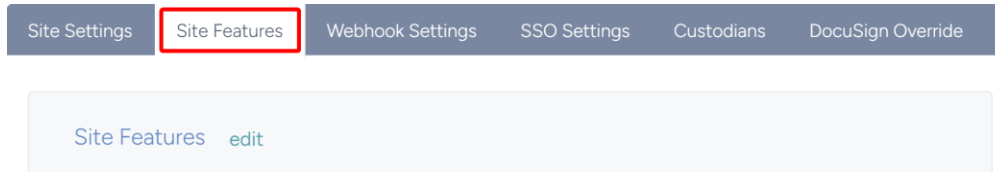
For Administrators — Enabling 2FA

Site Managers and Site Admins can enforce 2FA for all users directly from Site Settings. Once enabled, all users will be required to complete 2FA setup on their next login. Follow these steps to enable 2FA site wide.

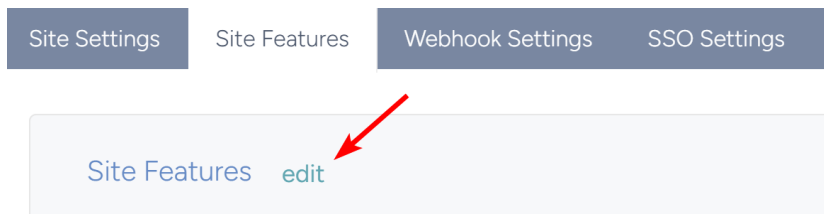
1. Navigate to **Administration** → **Site Settings**.



2. Navigate in the **Site Features** tab at the top



3. Click **edit** next to Site features.



4. Scroll down and locate the **Enforce 2FA for password logins** feature. To enable this feature, toggle it on and click **Save** at the bottom of the page. The setting takes effect immediately for all subsequent logins.



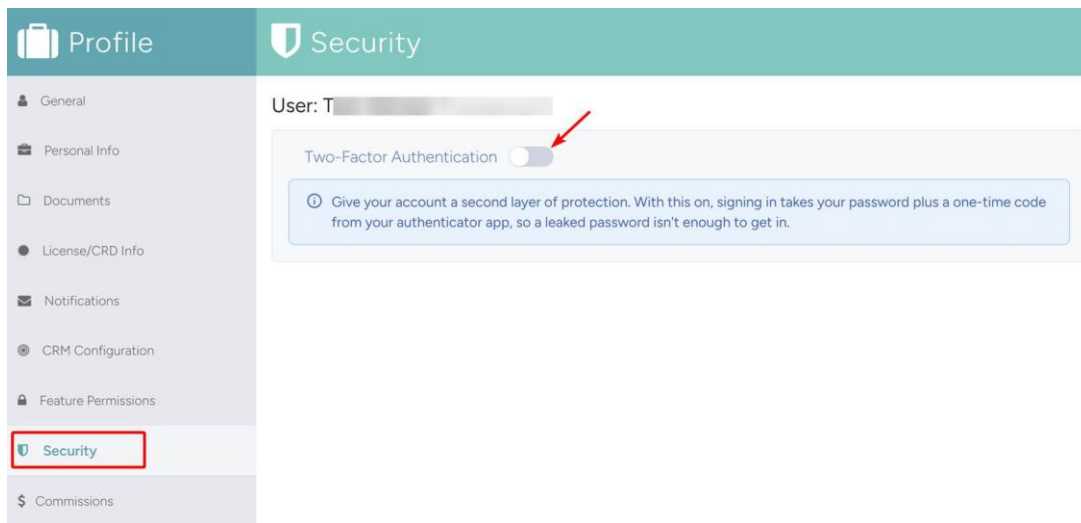
For Users — Enabling 2FA

If your organization **has not** enforced 2FA at a site-wide level, you can still enable or disable it on your own account for added security. If it is enabled site wide, you cannot disable it for yourself.

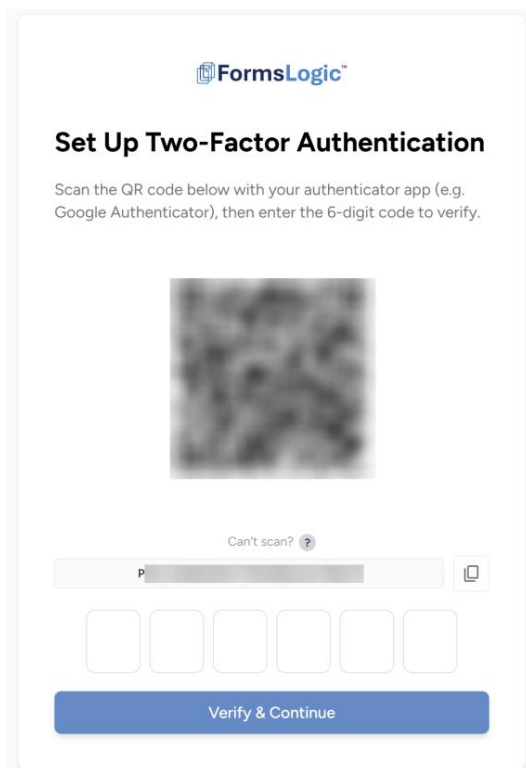
1. Click your name in the upper right and select **Profile** from the dropdown.



2. Navigate into the **Security** Tab and click on the **toggle** to enable Two-Factor Authentication.



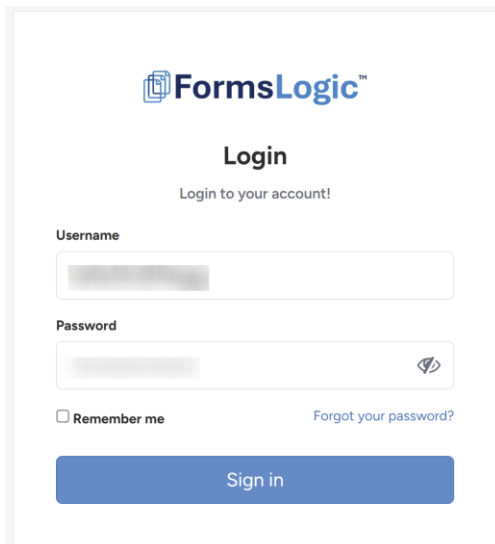
3. Once the toggle is on, you will navigate to the set up screen for 2FA. Here you will set up 2FA for the first time.



FIRST-TIME SETUP – USERS

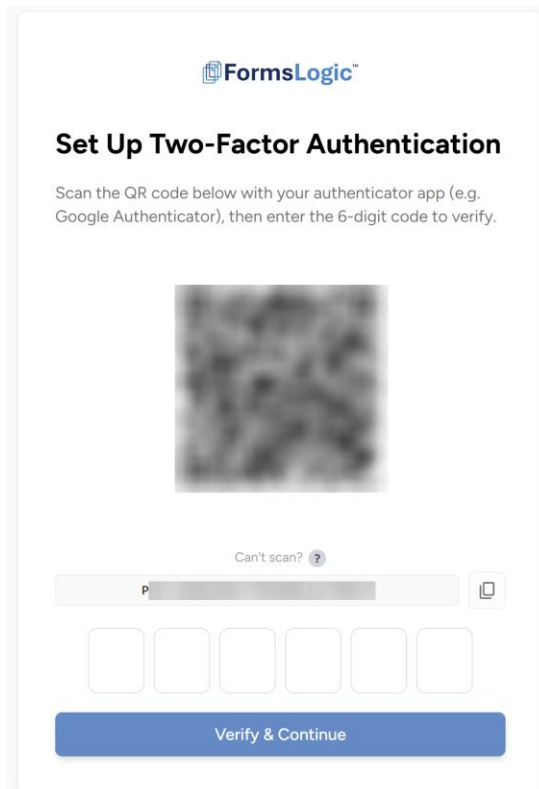
When Two-Factor Authentication is enforced and you log in for the first time on a new device, the following steps occur:

1. In the Login page, enter your username and password as usual and click **Sign In**.



The image shows the FormsLogic login page. At the top is the FormsLogic logo. Below it is the heading "Login" followed by the subtext "Login to your account!". There are two input fields: "Username" and "Password". The "Password" field has a toggle icon for visibility. Below the fields are a "Remember me" checkbox and a "Forgot your password?" link. At the bottom is a blue "Sign in" button.

2. The 2FA setup screen opens, which displays a QR code. **Open your authenticator app and scan the QR code.** Or copy the code if you are unable to scan.



The image shows the "Set Up Two-Factor Authentication" page. It features the FormsLogic logo and the heading "Set Up Two-Factor Authentication". Below the heading is a paragraph: "Scan the QR code below with your authenticator app (e.g. Google Authenticator), then enter the 6-digit code to verify." A large QR code is displayed in the center. Below the QR code is a link "Can't scan? ?". There is a text input field with a "P" placeholder and a copy icon. Below the input field are six empty boxes for entering a 6-digit code. At the bottom is a blue "Verify & Continue" button.

3. In your authenticator app, find the **6-digit code** for Forms Logic. Enter that code into the verification field and click **Verify & Continue**.

1	2	3	4	5	6
---	---	---	---	---	---

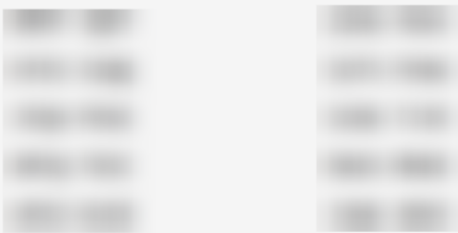
Verify & Continue

4. Your backup codes will be displayed. Save these in a secure location — they can be used to regain access if you lose your authenticator app.



Save Your Backup Codes

Save these backup codes in a safe place. Each code can only be used once if you lose access to your authenticator app.



[Download as text file](#)

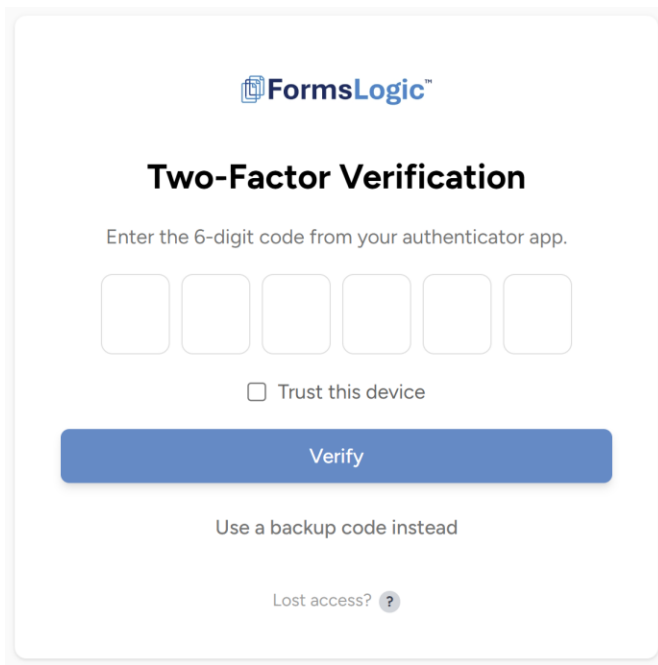
 These codes will not be shown again. Please save them now.

I've saved my codes, continue

5. Click **I've saved my codes, continue** to login and access the platform.

I've saved my codes, continue

6. Whenever you Log-In to Forms Logic after setting it up, you will be prompted to enter a 6-digit code from your authenticator app.



FormsLogic™

Two-Factor Verification

Enter the 6-digit code from your authenticator app.

☐ Trust this device

Verify

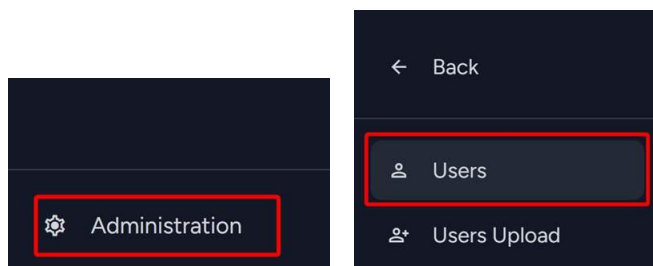
Use a backup code instead

Lost access? [?](#)

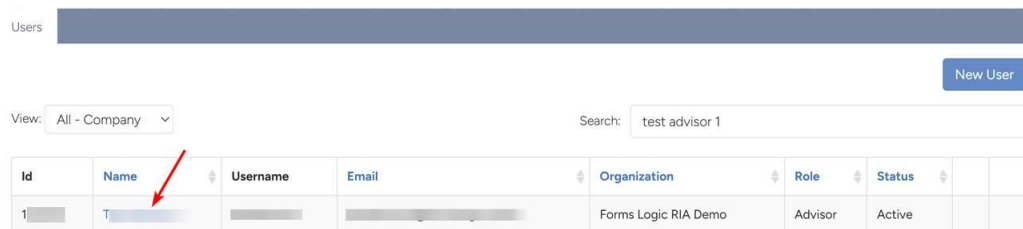
RESETTING USER'S 2FA – ADMINISTRATORS

If you change authenticator apps, get a new device, or need to reconfigure your 2FA for any reason, it can be reset from the profile. This is only available for Site Administrators and Site Managers.

1. From the side navigation menu, navigate to **Administration** → **Users**.



2. Click on the name of the user that needs 2FA reset. This will open their profile.



3. Navigate into the **User Maintenance** Tab.

The screenshot shows the 'User Maintenance' section of a software interface. On the left is a sidebar with a 'Profile' header and a list of menu items: General, Personal Info, Documents, License/CRD Info, Notifications, **User Maintenance** (highlighted with a red box), CRM Configuration, Feature Permissions, DocuSign Override, Preferences, and Commissions. The main content area has a teal header with a 'User Maintenance' title and a 'User: T...' label. Below this are three sections: 1. 'Move User to another Site (current site: Forms Logic RIA Demo)' with a 'Site to Move To' dropdown and a 'Move User' button. 2. 'Change Ownership of User's Work to another User' with a 'Change Owner To' dropdown and an 'Assign User's Work' button. 3. 'Reset Two-Factor Authentication (removes the user's authenticator app, trusted devices, and backup codes)' with a red 'Reset 2FA' button.

4. In the Reset Two-Factor Authentication section, click the **Reset 2FA button**. This will reset that user's 2FA.

This is a close-up of the 'Reset Two-Factor Authentication' section. It shows the text 'Reset Two-Factor Authentication (removes the user's authenticator app, trusted devices, and backup codes)' in blue. Below the text is a red button labeled 'Reset 2FA'. A red arrow points directly to the 'Reset 2FA' button.