Multi-factor Authentication

Download the PDF of this article.

In this Article

Related Articles

Overview

Multi-factor authentication (MFA) is any additional method of authenticating yourself to an application other than your standard username and password combination. These can be tokens you hold, such as security keys, authenticator apps on your mobile device, or biometrics, like fingerprints. When using multiple “factors of authentication” for an online account an extra layer of security is added. If an attacker somehow gets access to your password, an account protected by multi-factor authentication would block the attacker from gaining access to your account as they would also need access to that additional factor.

Requirements

- Multi-factor authentication is available on Essentials plans and up
- An administrator must enable MFA before use is available

Further requirements for each method of multi-factor authentication will differ per method. Refer to the specific documentation pages for each method for more details.

- Time-Based One-Time Passwords
- YubiKey

Enable MFA (Administrator Required)

- Navigate to **Admin Dashboard | Security**

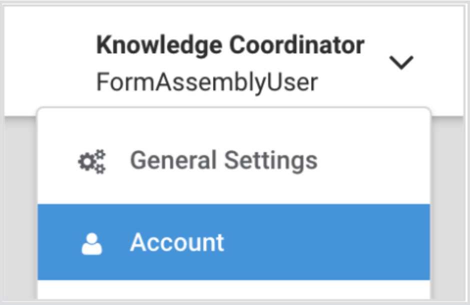
To allow users to manage MFA for their user account

- In the Multi-factor Authentication section, toggle the option to enable MFA for the instance

To force users to authenticate with MFA upon login

- In the Multi-factor Authentication section, toggle the option to Force MFA

Add a Multi-factor Authenticator



- Navigate to the "**Account**" section within your user profile
- Within the **Account Details** section, click the **Configure MFA** button
  - You will be taken to the Multi-factor Authenticators page, which displays all multi-factor authenticators you have set up for your user profile, their status (enabled or disabled), and their order of precedence.
- Click **Add Authentication Method** for a list of available multi-factor authentication options
- Select the authenticator you wish to add
  - A new disabled entry will appear on your timeline with buttons to configure or delete the added MFA method.
- Click **Configure** to continue the setup of the new MFA method.

Enable or Disable a Multi-factor Authenticator

- On the Multi-factor Authenticators page, click **Configure** on the method you wish to enable or disable.
- Within the **Status** section, select the desired option (**Enabled** or **Disabled**)
- Select **Apply** at the bottom of the configuration screen to save the selection.

> Note:
>
> - Some multi-factor authenticators require a "first-time setup" before allowing you to enable or disable them.
> - If the "Force MFA" setting is enabled by your FormAssembly administrator, at least one MFA method must be enabled for your user account. To disable all MFA methods, the "Force MFA" setting must be toggled off first.

Reorder Multi-factor Authenticators on the Timeline

If you have multiple multi-factor authenticator methods set up, the timeline allows you to reorder your methods so one may challenge you before another when logging in.

- Using the drag handles to the left of each entry in the timeline, drag the entries to create your preferred order. The precedence goes in descending order.
- Click **Apply** at the bottom of the timeline to save your changes. The page will refresh and show the new order.

Delete a Multi-factor Authenticator

- On the Multi-factor Authenticators page, locate the multi-factor authentication method you wish to delete
- Click the **Delete** button
- A **Remove Authenticator** confirmation box will ask you to confirm the action. Click **Remove** to confirm.
- The page will refresh with the deleted method removed from the timeline

Note: If the "Force MFA" setting is enabled by your FormAssembly administrator, at least one MFA method must be enabled for your user account. To disable all MFA methods, the "Force MFA" setting must be toggled off first.

MFA Administration

Administrators of a FormAssembly instance can manage MFA configurations for users.

Note: The administrator must have the permission “Can manage multi-factor authentication” enabled for their account.

- Navigate to **Admin Dashboard | User Management | All Users**
- Select a user and navigate to their **Details** tab
- Locate the **Multi-factor Authentication** section
- For each MFA method displayed for the user account, the admin may select to **enable**, **disable**, or **delete**.

FAQs

What’s the difference between disabling and deleting a multifactor authenticator?

- Disabling a multi-factor authenticator authenticator means it will not challenge you to log in to your account. However, it remains set up and associated with your account, so you only need to re-enable the method to activate it again.

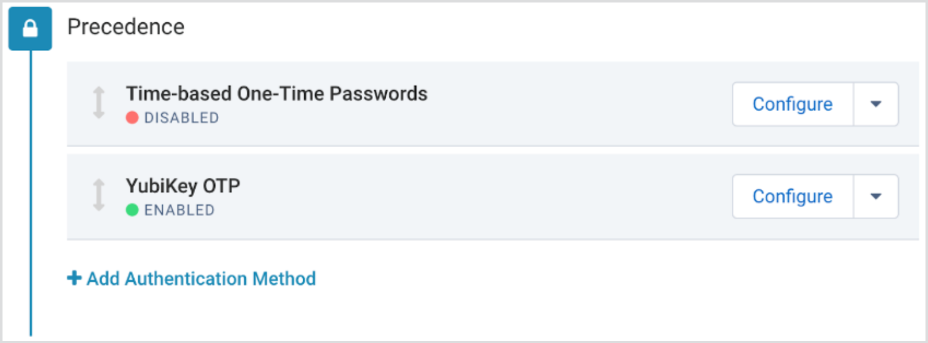
- Deleting a multi-factor authenticator will remove it entirely from your account. If you wish to use that authentication method again, you would completely recreate it and re-configure it from scratch.

If I have multiple multifactor authenticators set up and enabled will I need to complete each one individually before I can log in?

- No, we currently only require the success of one of the authentication challenges you may be presented with. When verified by one of your multi-factor authenticators at login, your account may be accessed.

If I have multiple multifactor authenticators set up and the one at the top is disabled, what authentication challenge will I be presented with when logging in?

- You will be presented with the authentication challenge of the top-most enabled authenticator in your timeline's order of precedence. In the example given below, even though Time-based One-Time Passwords is set to go first, it is disabled, and so the next enabled method will be presented (YubiKey).



Precedence

Time-based One-Time Passwords
● DISABLED

YubiKey OTP
● ENABLED

If I have multiple multifactor authenticators set up, and I'm having trouble with one of them, can I switch to complete another instead?

- Yes. If you have additional multi-factor authenticators enabled on your account, you will see a link to move to the next one if you're having trouble with the current one. Note that choosing to move to the next enabled method cannot be undone, and you cannot return to a previous authentication challenge.

I know my username and password but have lost access to my additional factors, how can I recover my account?

- For our Basic plan customers, you must contact FormAssembly Support and go through a proof of identity process. On completion of that, a FormAssembly Support representative will disable the multi-factor authenticators associated with your account, allowing you to log in without them.
- For our Essentials plan and higher customers, you must contact your FormAssembly instance administrator(s) to disable the multi-factor authenticators associated with your account, allowing you to log in without them.