

Multi-Factor Authentication User Setup

Last Modified on 08/07/2024 1:12 pm EDT

Overview

Once multi-factor authentication (MFA) is [enforced on your Org](#), any user who authenticates with a username and password will be required to configure MFA prior to accessing that Org.

Individual security-conscious users who authenticate with a username and password can also opt-in to MFA.



Note:

Users are required to configure multi-factor authentication for the initial set-up and if an Administrator resets MFA.

User Account Requirements

Only Administrators can enforce multi-factor authentication on their Org.

Related Information/Setup

Please refer to the [Enforcing Multi-Factor Authentication on an Org](#) article for more information on enforcing MFA on an Org.

Setting up Multi-Factor Authentication (Enforced Org)

Once multi-factor authentication (MFA) is enforced on an Org, the next time users log in, the MFA set up page will be displayed.

1. Log in to Resolver to see the **Multi-Factor Authenticator Setup** screen.



Multi-Factor Authenticator Setup

Your organisation has enforced Multi-Factor Authentication for your account. To set it up, please follow these steps:

- 1. Access authenticator app on your phone.**
You can use any authenticator app you choose to.
- 2. Scan the QR code.**
In the authenticator app choose to add an account and scan the QR code.



If you cannot scan the QR code, you can do a manual setup with code
IUSHGLCSGYSSYPCYFBSQ

- 3. Enter the authenticator code.**
Once the new account is configured in your authenticator app, enter the 6-digit code generated by scanning the QR code below:

*

CANCEL

VERIFY

The Multi-Factor Authenticator Setup Screen



Note:

If this is an account activation, create a password prior to configuring MFA.

2. Open your **Authenticator App** and scan the QR code to generate the one-time passcode.



Note:

The Authenticator App is of your choosing. If the QR code fails to scan, complete the manual setup with the code.

3. Input the passcode into Resolver and click the **Verify** button.



Multi-Factor Authenticator Setup

Your organisation has enforced Multi-Factor Authentication for your account. To set it up, please follow these steps:

- 1. Access authenticator app on your phone.**
You can use any authenticator app you choose to.
- 2. Scan the QR code.**
In the authenticator app choose to add an account and scan the QR code.



If you cannot scan the QR code, you can do a manual setup with code
IUSHGLCSGYSSYPCYFBSQ

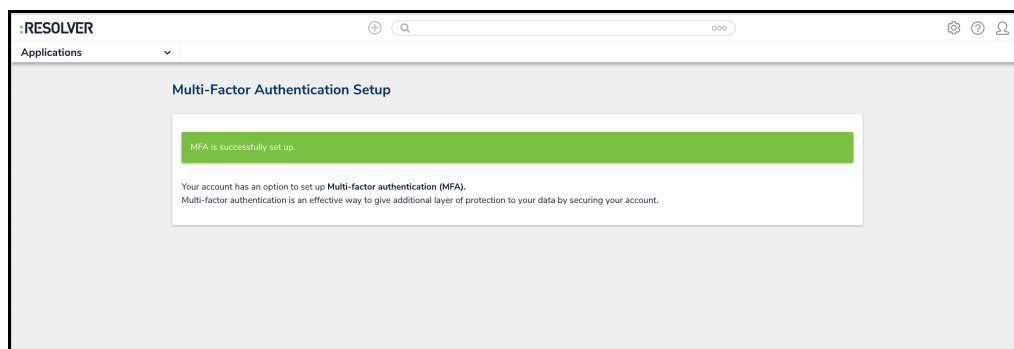
- 3. Enter the authenticator code.**
Once the new account is configured in your authenticator app, enter the 6-digit code generated by scanning the QR code below:

CANCEL

VERIFY

Verify Button

4. A message will appear to indicate the setup was successful.



MFA Success Message

5. **(Optional):** The next time you log in to Resolver, select the **Remember this device for 30 days** checkbox to save your login details for 30 days when using MFA.

Remember This Device for 30 Days Checkbox

Setting up Multi-Factor Authentication (Opt-In)

Any user can set up multi-factor authentication (MFA) on their own account provided that they do not already authenticate with SSO.

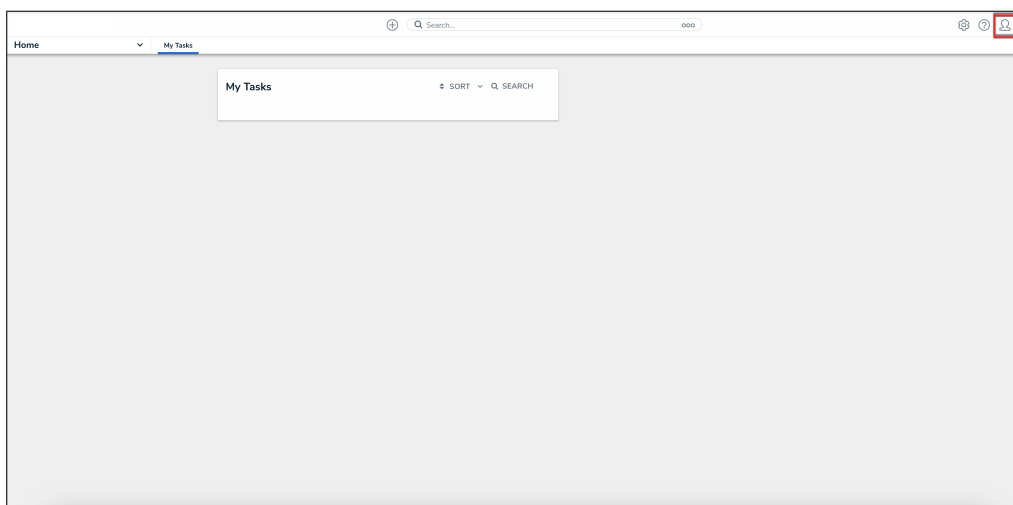
1. Log in to Resolver.



Note:

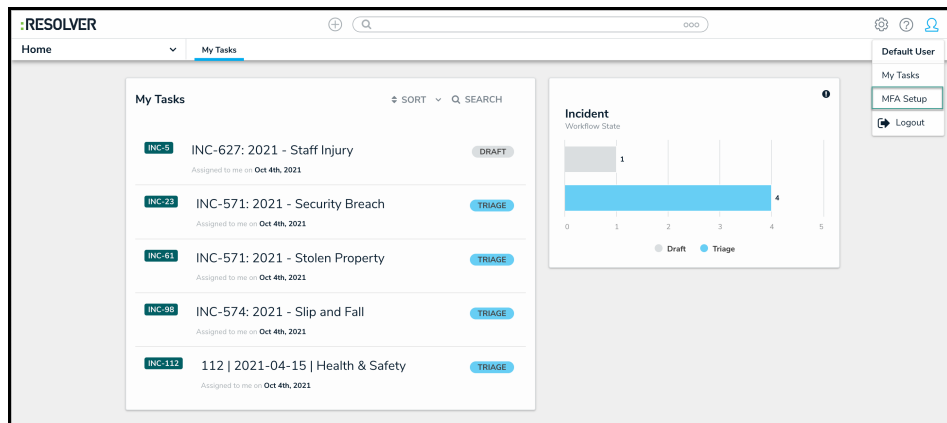
If this is an account activation, create a password prior to configuring MFA.

2. From the **Home** screen, click the **User Profile** icon.



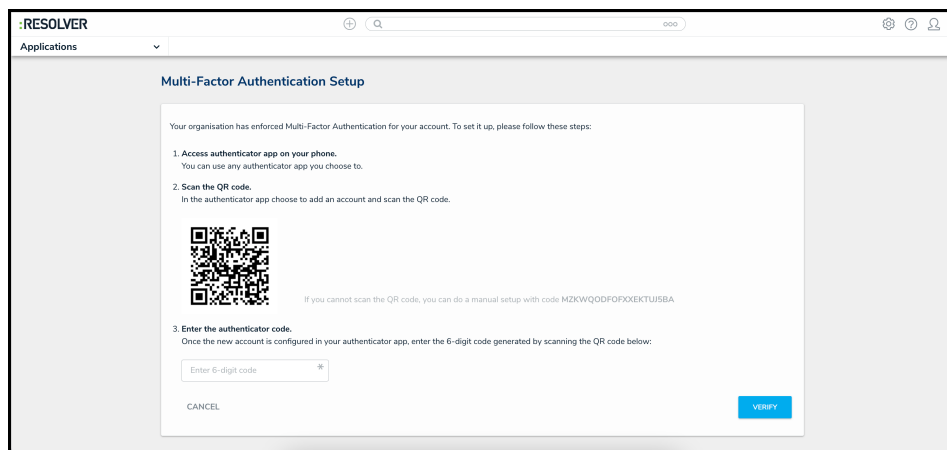
User Profile Icon

- Click the **MFA Setup** button.



MFA Setup Button

- A QR code appears with instructions to complete the setup.



QR Code for MFA Setup

- Open your **Authenticator App** and scan the QR code to generate the one-time passcode.
- Input the passcode into Resolver and click the **Verify** button.

 **Multi-Factor Authenticator Setup**

Your organisation has enforced Multi-Factor Authentication for your account. To set it up, please follow these steps:

- 1. Access authenticator app on your phone.**
You can use any authenticator app you choose to.
- 2. Scan the QR code.**
In the authenticator app choose to add an account and scan the QR code.



If you cannot scan the QR code, you can do a manual setup with code
IUSHGLCSGYSSYPCYFBSQ

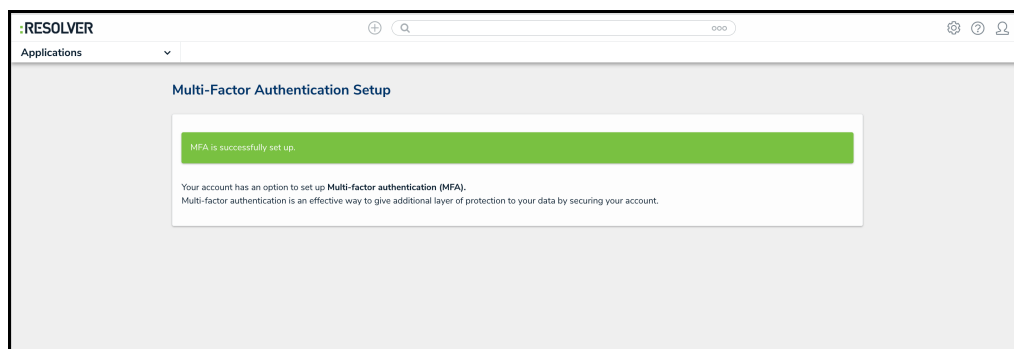
- 3. Enter the authenticator code.**
Once the new account is configured in your authenticator app, enter the 6-digit code generated by scanning the QR code below:

*

CANCEL VERIFY

Verify Button

7. A message will appear to indicate the setup was successful.



MFA Success Message

8. **(Optional):** The next time you log in to Resolver, select the Remember this device for 30 days checkbox to save your login details for 30 days when using MFA.

R.

Multi-Factor Authentication

Enter 6-digit code from your authenticator app.

☐ Remember this device for 30 days

VERIFY

Haven't receive a code? [Resend a new code.](#)

Remember This Device for 30 Days Checkbox