Enforcing Multi-Factor Authentication on an Org

Last Modified on 08/07/2024 9:03 am EDT

Overview

Multi-factor authentication (MFA) adds another layer of security when accessing Resolver using a password. MFA is managed in the Resolver API (Swagger) and Administrators can complete the following:

- Enforce MFA for an Org. The next time users log in to the Org, the MFA set-up page will be displayed.
- Opt-out an individual user from an enforced MFA Org.
- Reset the MFA profile for a user.

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

> ***Note:***
> MFA should only be enforced in Production environments.

User Account Requirements

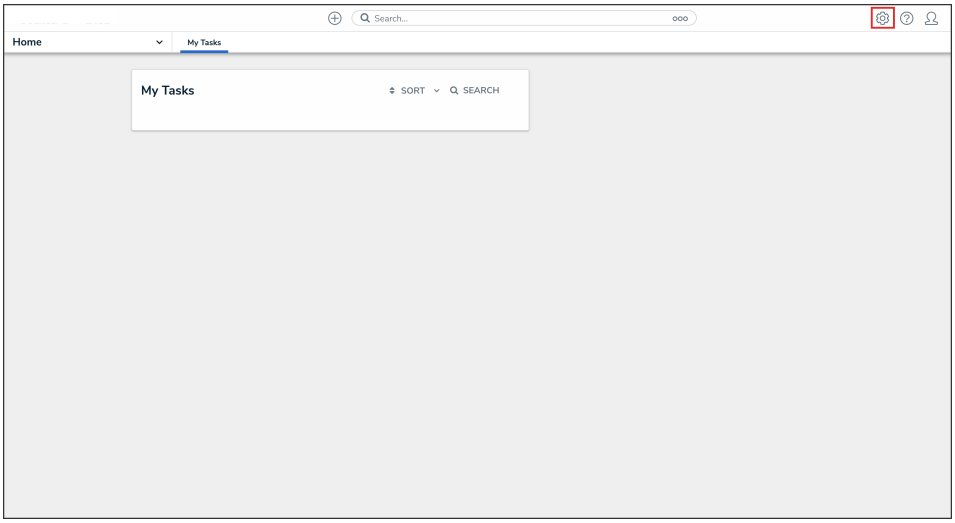
Only Administrators can enforce multi-factor authentication (MFA) on their Org.

Related Information/Setup

Please refer to the Multi-Factor Authentication User Setup article for more information on setting up users with MFA.

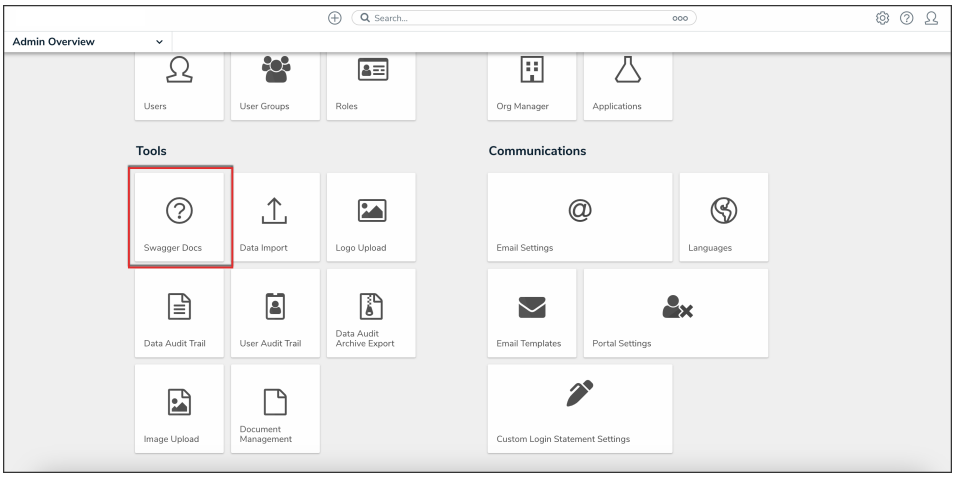
Navigation

1. From the ***Home*** screen, click the **Administration** icon.



Administration Icon

2. From the ***Admin Overview*** screen, click the **Swagger Docs** tile under the **Tools** section.

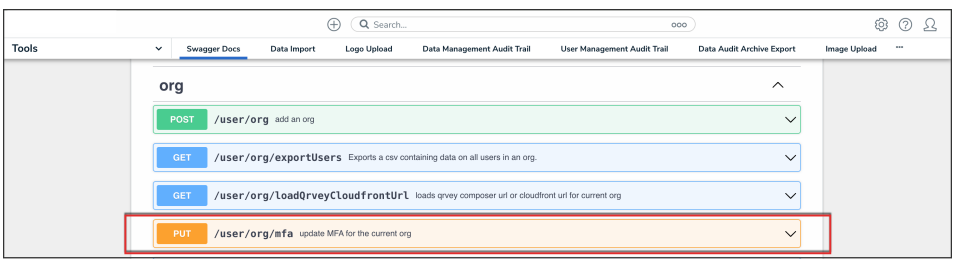


Swagger Docs Tile

Enforcing Multi-Factor Authentication on an Org

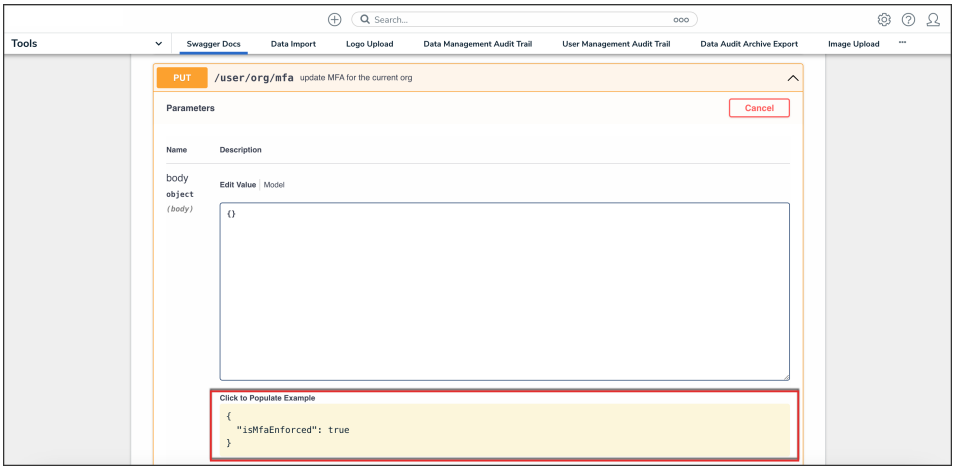
When multi-factor authentication (MFA) is enforced on an Org, all active users will be prompted to use MFA upon their next login. If there are multiple Orgs in your Production environment, MFA will be enforced on all of them.

1. From the ***Admin: Help*** screen, click the **org** topic to expand the list of endpoints and click **Put /user/org/mfa** to open the parameters.



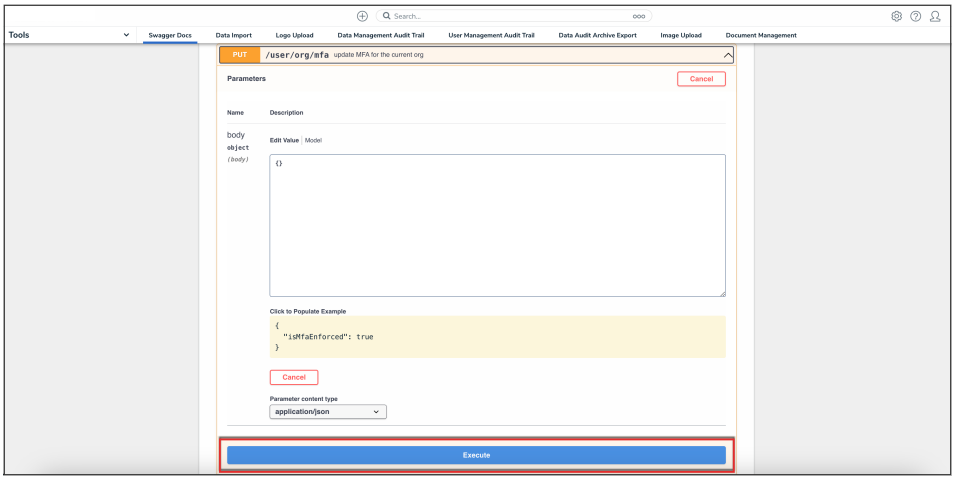
API Endpoint

2. Click the example value to load the call into the body.



Example Value

3. Click the **Execute** button to execute the API call.



Execute Button