

# Log In

Last Modified on 04/12/2023 5:01 pm EDT

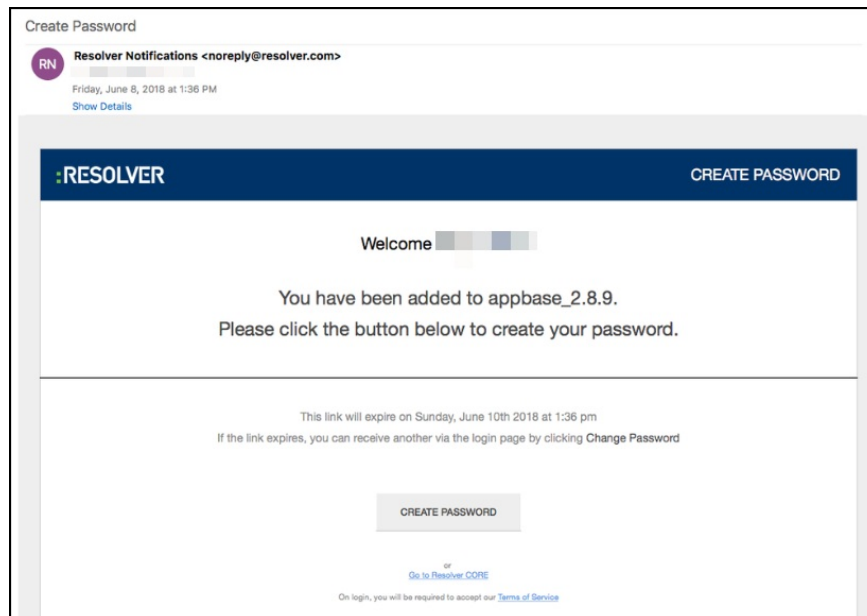
## Overview

The Primary Administrator will receive their login credentials from Resolver®. All other users will receive an automatic email from the **Resolver Notifications <noreply@resolver.com>** address with instructions on creating a password when an Administrator creates an account for you.



**Tip:**

*If you have not received a **Create Password** email, please check your email folders (junk, etc.) for an email from **Resolver Notifications <noreply@resolver.com>**.*



*Example - Create Password Email*



**Note:**

*The login screen indicates which country your data is currently being stored in. See the [Data Region](#) article for more information.*

## Related Information/Setup

### Single Sign-On (SSO) to Log In

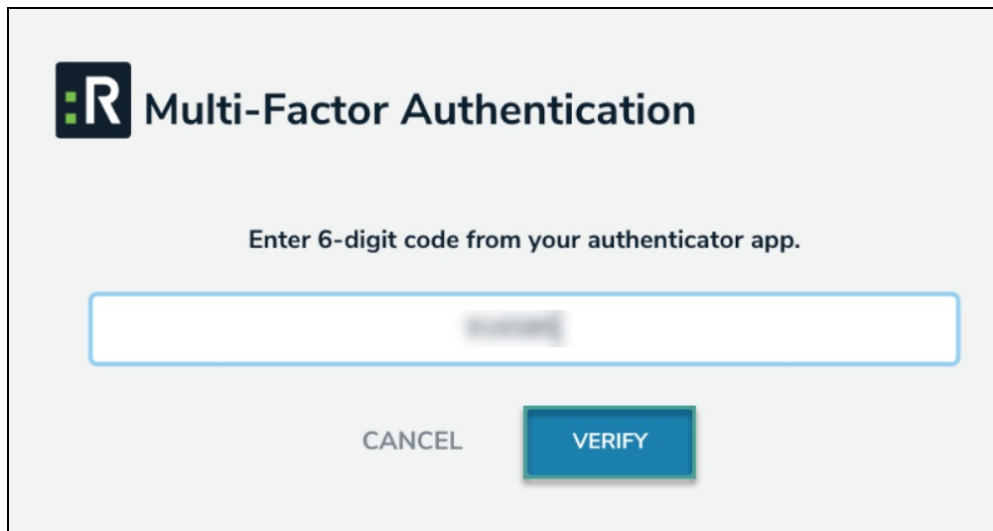
If your organization is uses SSO authentication to log in, please refer to the Single Sign-On (SSO)

category for further information.

- [Single Sign-On \(SSO\)](#)

## Multi-factor Authentication

If multi-factor authentication (MFA) has been configured for your user, open your **Authenticator App**, enter the **6-digit code** into the **Resolver MFA** screen and click the **Verify** button. To set up MFA for the first time or after an MFA reset, review our [Multi-Factor Authentication User Setup guide](#).



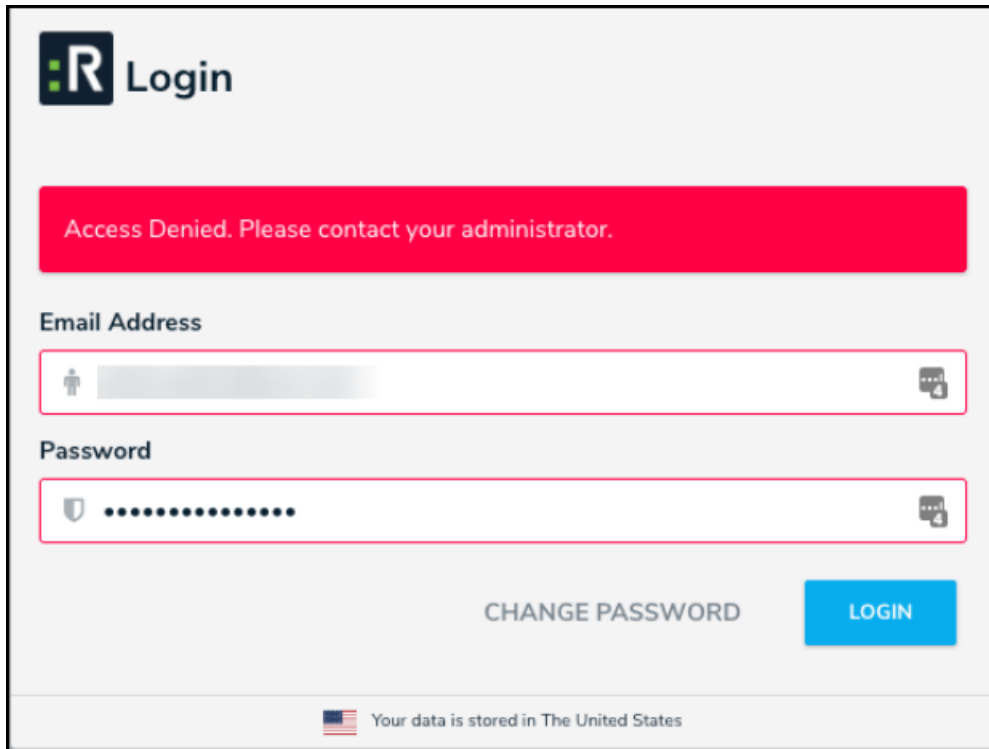
The image shows a screenshot of a web-based Multi-Factor Authentication (MFA) screen. At the top left is the Resolver logo, which consists of a dark square containing a white 'R' with a green dot above it. To the right of the logo is the text 'Multi-Factor Authentication'. Below this, the instruction 'Enter 6-digit code from your authenticator app.' is centered. A large, empty text input field with a light blue border is positioned below the instruction. At the bottom of the screen, there are two buttons: a light gray button labeled 'CANCEL' and a blue button labeled 'VERIFY'.

*Multi-Factor Authentication Screen*

## IP Authorization Control

IP authorization helps Administrators control who is accessing specific Orgs based on their IP address. It can be configured to validate all users, including SSO or users signing in with a username and password.

If IP Authorization Control is enabled, your IP address will be validated against the entries on the Org's IP allow list. If your address doesn't match any of the entries, that Org will not be accessible after login. You will see an Access Denied error after you login if you don't have access to any Orgs due to failed IP address validation.



*Access Denied Login Error*

Please refer to the IP Authorization category for more information, including functionality for additional login scenarios.

- [IP Authorization Control](#)

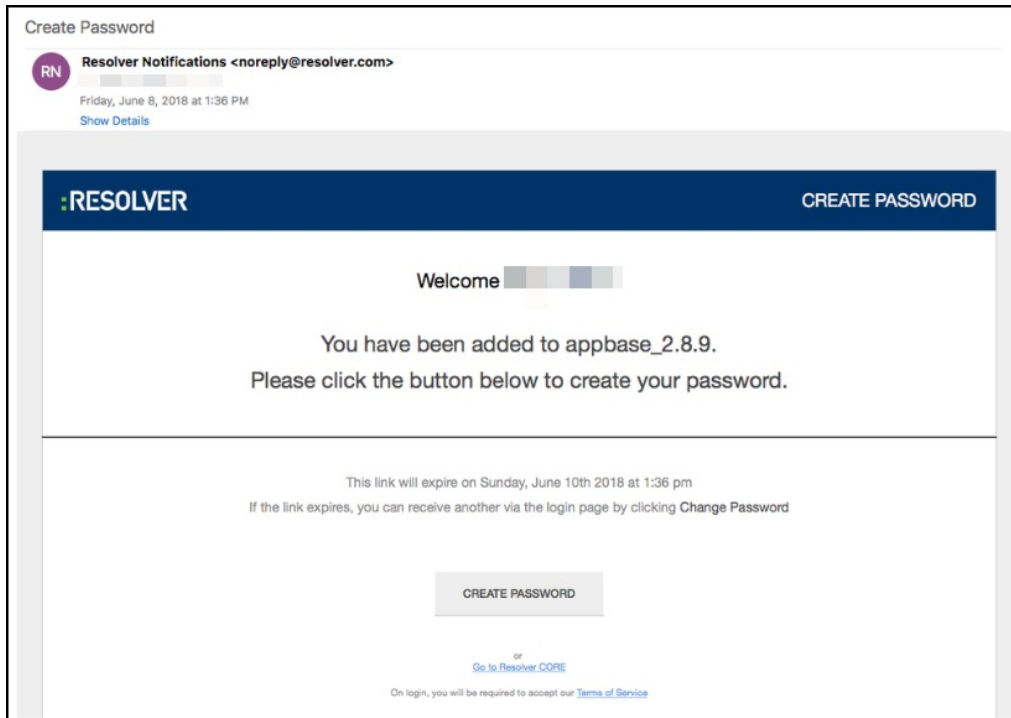
Please refer to the Password Requirements article for more information on the password conditions.

- [Password Requirements](#)

---

## Logging In

1. Open the email sent from **noreply@resolver.com**.



*Example - Create Password Email*

2. Click the **Create Password** button.
3. Enter your password in the **New Password** field. Your password must be at least 9 characters and contain alphanumeric characters; spaces are also permitted. Please refer to the [Password Requirements](#) article for more information on the password conditions.
4. **(Optional)** Click the **Show Password** icon to confirm the password entered is correct.
5. Click **Set Password**.
6. Review the **Terms of Service**, then click **Accept Terms**. All new users must accept the Terms of Service before continuing.
7. From the **Password Confirmation** screen, click the **Login** link.
8. From the **Login** screen, enter the **email address** that received the create password email in the **Email Address** field.
9. Enter your password in the **Password** field.

**R** Login

Email Address

user@domain.com \*

Password

Password \*

CHANGE PASSWORD LOGIN

Your data is currently being stored in Canada

*Login Screen*

10. Click the **Login** button.



**Note:**

*If your implementation includes multiple Orgs, select the organization you'll be working in before the homepage displays*