

# IP Authorization Logins

Last Modified on 02/10/2023 9:42 am EST

Depending on the org's settings, all users logging into Core (including users making API requests through an API key) are subject to the following rules:

- If IP authorization is **off**, users can log in without IP validation.
- If IP authorization is **on**, users' IP addresses are validated against the org's IP allow list. This applies to both SSO and basic access authentication requests (i.e., usernames and passwords).



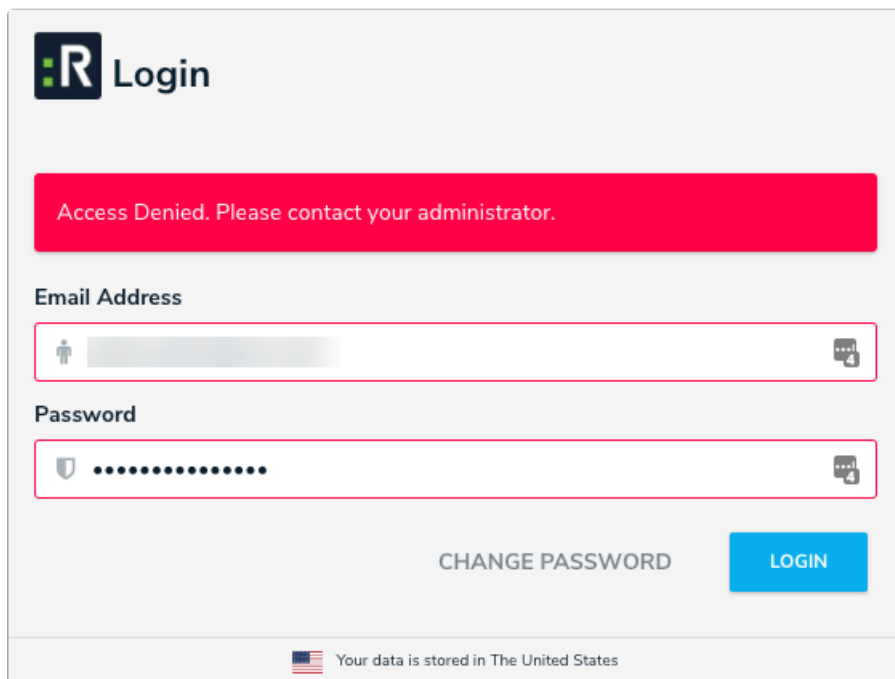
IP token validation must be enabled separately from IP authorization.

- If IP authorization is set to **bypass\_sso**, SSO users can log in without IP validation, but basic access authentication requests are validated against the IP allow list.

The above options can be enabled and disabled by [Resolver Support](#). See the [IP Authorization Overview](#) and [IP Token Validation](#) articles for more details and important notes.

## Multi-Tenancy (Multiple Orgs)

If a user is a member of multiple orgs but does not have access to an org because their IP address wasn't validated against the allow list, that org will not display after successful login. If no orgs are accessible under IP authorization control, an **Access Denied** error is displayed after login.

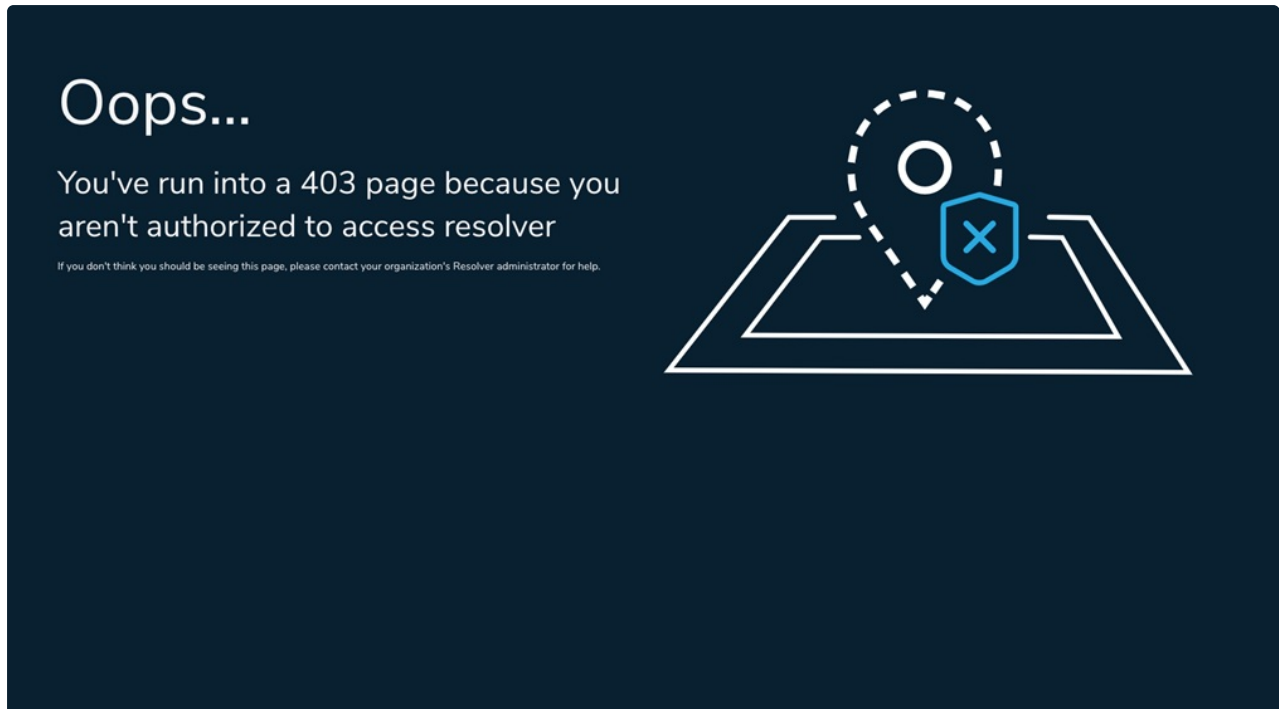
A screenshot of a web login interface. At the top left is the Resolver logo (a black square with a white 'R' and a green dot) followed by the word 'Login'. Below this is a red rectangular banner with the text 'Access Denied. Please contact your administrator.' in white. Under the banner are two input fields: 'Email Address' with a person icon and 'Password' with a shield icon. Both fields have a red border and a small speech bubble icon with the number '4' on the right. Below the password field are two buttons: 'CHANGE PASSWORD' in grey and 'LOGIN' in blue. At the bottom of the form is a small American flag icon followed by the text 'Your data is stored in The United States'.

*The error message displayed to users who can't access any orgs under IP authorization control.*

## Confidential Login

If enabled on the org, admins can enable IP authorization control on individual Confidential [Login](#) URLs. If the user's IP address doesn't match an entry in the list, a 403 error is displayed.

This is captured in the [User Audit Trail](#) as an **Unsuccessful Confidential Login** event.



*The error message displayed to unauthorized users attempting to access an Confidential Login URL.*

## Impersonation

Admins will have their IP addresses revalidated when initiating [Impersonation Mode](#) and when terminating it. If validation fails, the admin is logged out, which is captured in the [User Audit Trail](#) as an **Unsuccessful Impersonate User** event.



Session expired or invalid. Please re-login.

Email Address

Password

[CHANGE PASSWORD](#)

[LOGIN](#)

 Your data is stored in The United States