Resolver.
A KROLL BUSINESS

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).

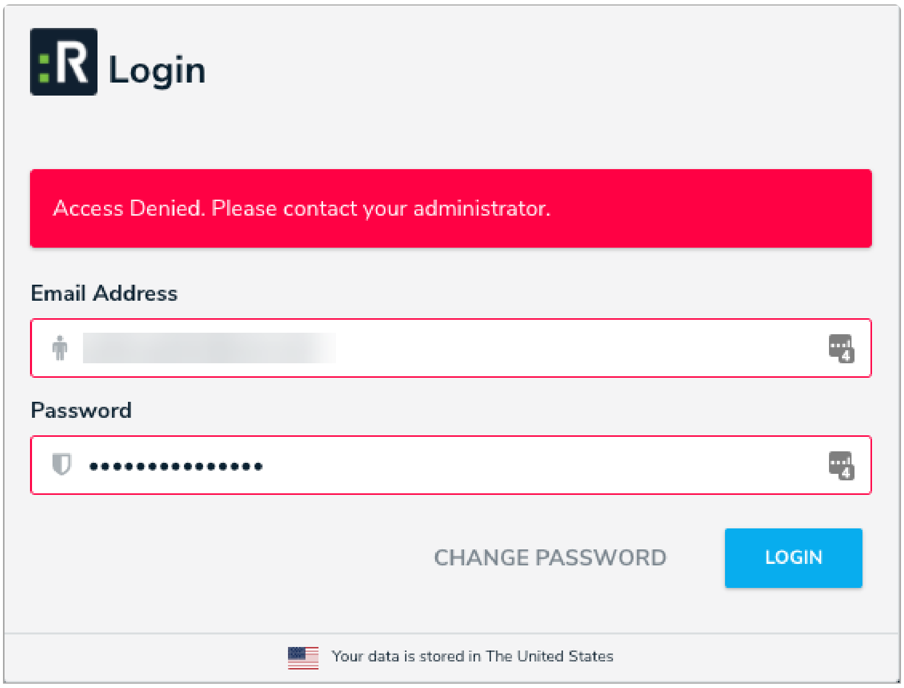
> IP token validation must be enabled separately from IP authorization.

- 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.


Login

Access Denied. Please contact your administrator.

Email Address

Password ●●●●●●●●●●●●●●●

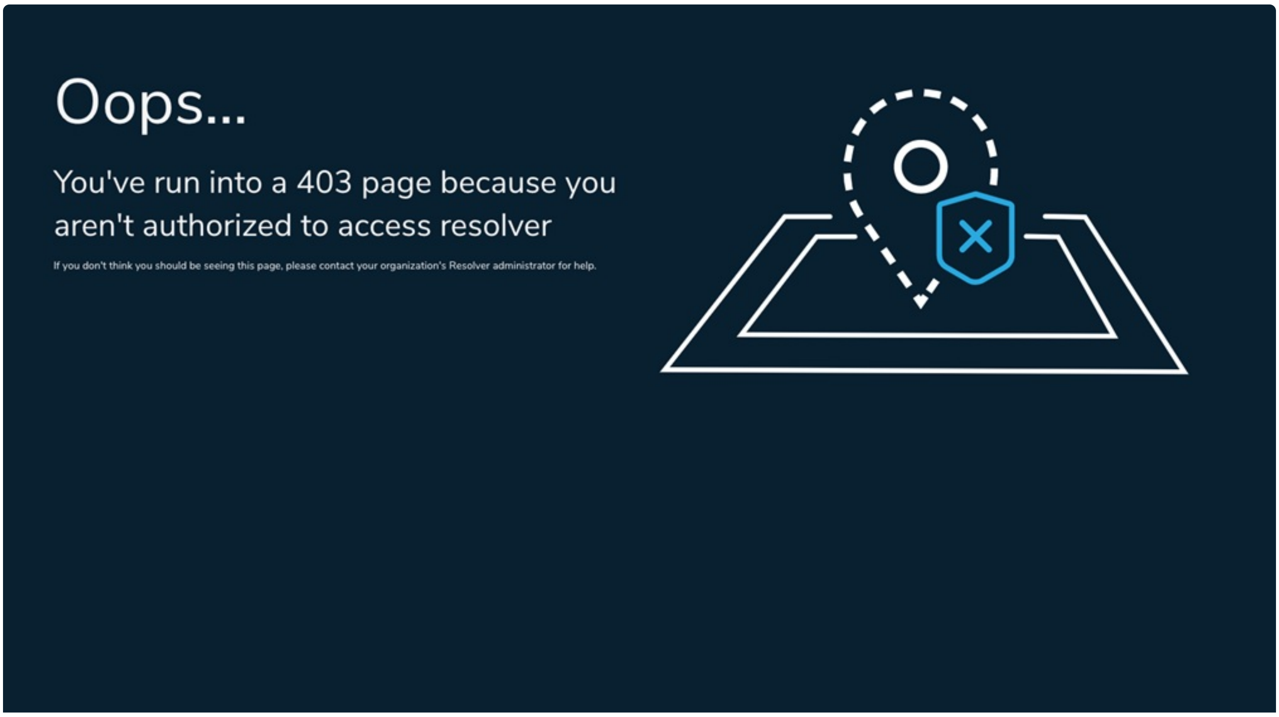
Your data is stored in The United States

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.



Oops...

You've run into a 403 page because you aren't authorized to access resolver

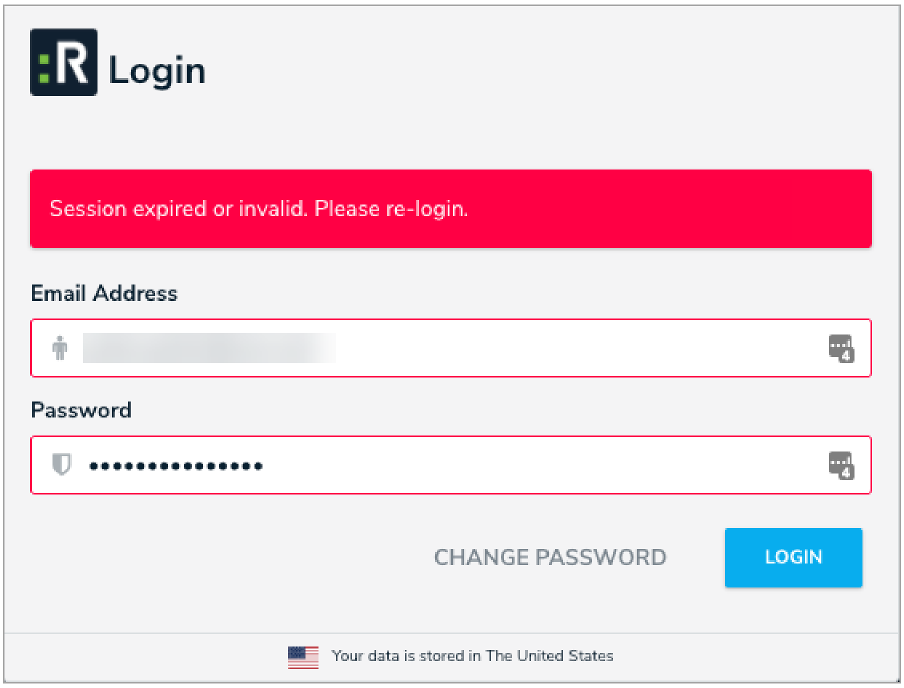
If you don't think you should be seeing this page, please contact your organization's Resolver administrator for help.

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.

Resolver.
A KROLL BUSINESS



Login

Session expired or invalid. Please re-login.

Email Address

[redacted]

Password

•••••••••••••••

Your data is stored in The United States