Log In with SSO

Last Modified on 04/11/2025 1:39 pm EDT

Overview

If single sign-on (SSO) is enabled, entering your email address on the login page will redirect you to your identity provider, where you'll need to enter the login credentials configured for your SSO account.

> ***Note:***
> Users must be logged into SSO in order to access email object links, embedded within system email notifications.

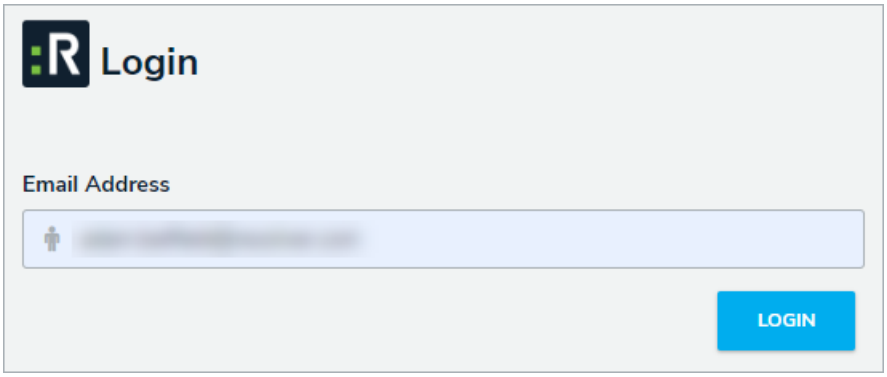
Related Information/Setup

For additional information and help with using SSO, please refer to the Single Sign-On (SSO) Frequently Asked Questions or the Troubleshoot Login Issues: Single Sign On (SSO) Users articles.

Logging into SSO for the First Time

If you're logging in with SSO for the first time, you must accept the **Terms of Service** before you can successfully log in. New users will not be required to create a password, nor will they receive an email with a link to log in. As such, Administrators should provide new users with the URL to access their organization.

1. From the SSO ***Login*** screen, enter your email address in the **Email Address** field.



SSO Login Screen

2. Press **Tab** on your keyboard to disable the **Password** field and complete the login process. If you have trouble with this step, review Troubleshoot Login Issues: Single Sign On (SSO) Users.

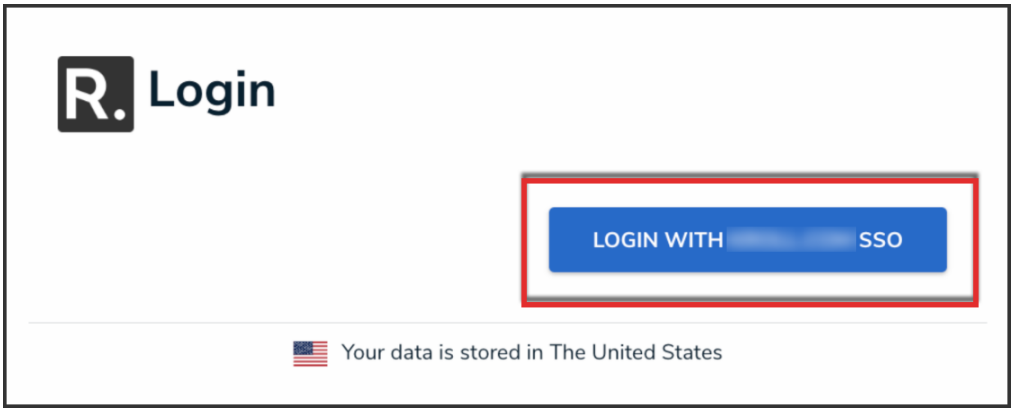
Enabling One-Click SSO Log In

Users have the option of logging into Resolver with SSO with one click of a button, skipping the need to provide an email address.

For additional information and help with using the one-click SSO log in feature, please refer to the Single Sign-On (SSO) Frequently Asked Questions article.

To enable one-click SSO log in:

1. Add the following syntax to the login URL: `?domain=<CustomerDomain.com>`
2. Click the **Login with SSO** button.



Login With <Domain Name> SSO Button

> ***Note:***
> The system can support domain names on the login button to a maximum of 40 characters. Beyond this, the login button will display as **Login with SSO**. Any typos in the URL or invalid domain names will redirect users to the non-domain URLs, and will prompt users to enter emails for SSO logins, as before.

IP Authorization Control and SSO

If your admin has enabled IP authorization control for SSO on an org you have access to, your IP address will be validated against the org's IP allow list when logging in. If your IP address can't be validated, that org will not be accessible. See the IP Authorization Control section for more details.

Logging Out Using SSO

Logging out will end your SSO session. Additionally, after 10 minutes of inactivity, you'll be prompted to refresh your session. If, after 5 minutes, you haven't refreshed the session, you'll be logged out automatically.

Resolver.
A KROLL BUSINESS