Log In with SSO

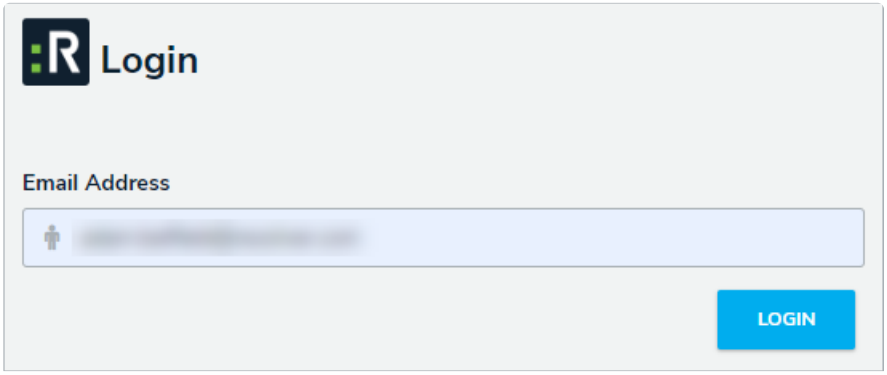
Last Modified on 10/03/2019 12:47 pm EDT

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.

If you're logging in 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.

To log in using SSO, enter your email address, then 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.

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.



The login screen with SSO enabled.

Admins can disable SSO for individual users.

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.