Request SSO for Your Account

Last modified on 10/06/2025 3:24 pm EDT

Single sign-on (SSO) and force SSO | Request SSO for your account | Why you should use SSO

Single sign-on (SSO) and force SSO

SSO

Single sign-on (SSO) is an authentication method that allows you to access multiple applications or services with a single set of login credentials. Instead of remembering and entering separate usernames and passwords for each application, you can log in once and access all connected systems without needing to log in again for each one.

Force SSO

Force SSO is a setting or policy within an SSO system that requires users to authenticate exclusively through SSO when accessing protected resources or applications. Even if you're already logged in somewhere else, force SSO ensures that you always use your SSO login to access certain applications. This enforces consistent authentication, strengthens access control, and enhances overall security by centralizing user login management.

How force SSO works in DrChrono

- You can turn on force SSO for your practice group. Once it's enabled, everyone in the practice group must log in with SSO.
- You will no longer be able to use a username and password.
- This setting applies to the entire practice group, not just some users.

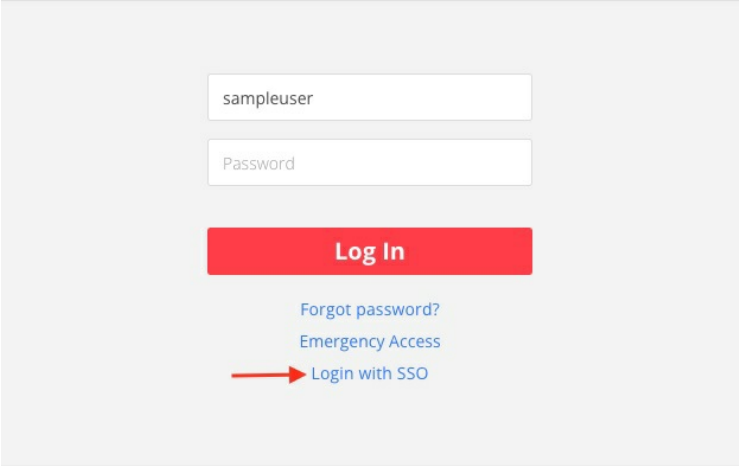
Before force SSO is turned on, make sure that:

- Everyone in your practice group has SSO set up for their account.
- Your login request is linked to an existing user. If this isn't done first, you won't be able to log in to DrChrono after force SSO is enabled.

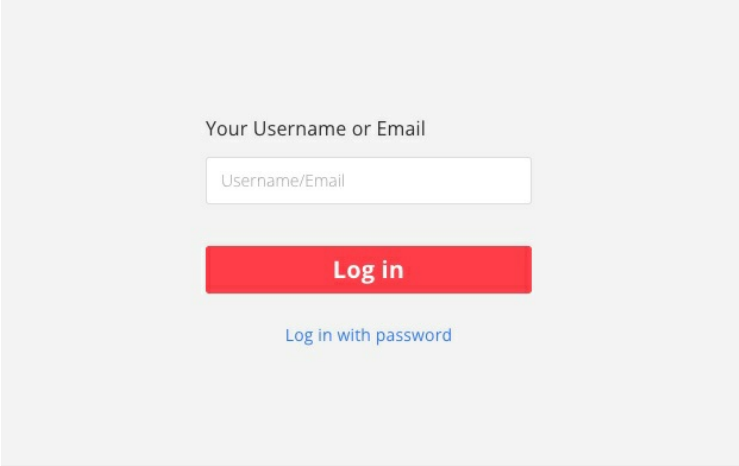
To turn on force SSO for your practice group, create a support case.

Request SSO for your account

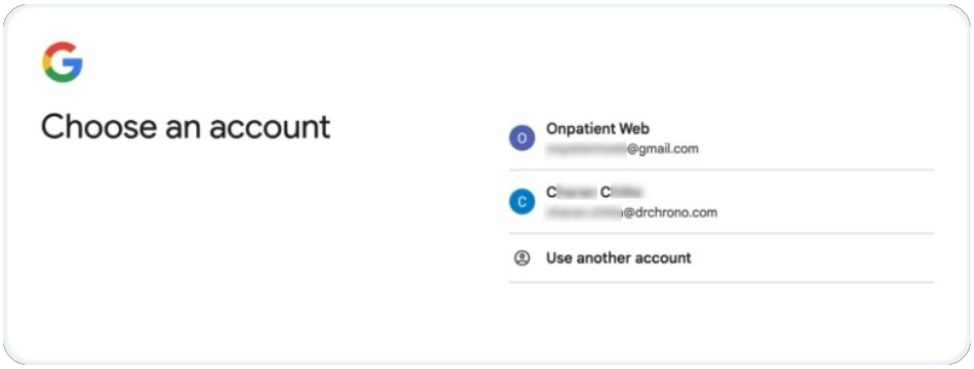
1. You must set up your practice group and email with an identity provider.
2. On the login page, enter your username and select **Log in with SSO**.



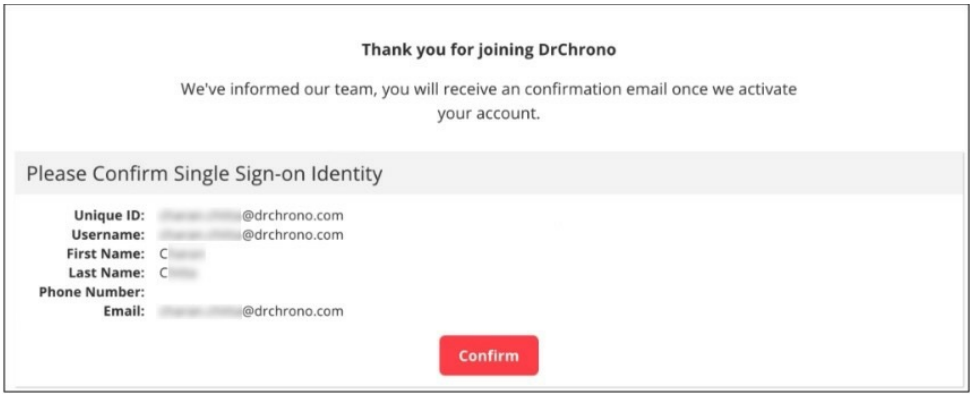
3. Enter your username or email and select **Log in**.



Once you log in, you're redirected to select your account. The image below is an example using Google as the identity provider.



4. After you select your account, you see the screen below to confirm your SSO Identity. Select **Confirm**.



After confirming, your request appears on the **SAML SSO Dashboard**, where the practice group administrator can link the user's request to an existing user.

> Until the request is linked to an existing user, your users will continue to see the confirmation message when attempting to log in using SSO.

Once your request is accepted, you will receive a confirmation email and be able to use the SSO login workflow.

Why you should use SSO

Enabling SSO in DrChrono offers several key benefits for your practice.

- **Improved security:** SSO (using the SAML standard) centralizes and secures the login process, reducing the chances of unauthorized access and potential data breaches.
- **Simpler user logins:** With SSO, users only need to log in once to access DrChrono and other connected systems without needing to remember or enter multiple sets of credentials.
- **Regulatory compliance:** SSO supports secure, centralized access control and auditing, helping you meet compliance and security standards.
- **Increased productivity:** By removing the need to log in multiple times or manage various passwords, users can get to work faster and more efficiently.
- **Easier user management:** SSO streamlines user access management by allowing administrators to manage user access from one dashboard.