How to Request SSO for Your Account

07/24/2024 4:55 pm EDT

SSO and Force SSO

Single Sign-On (SSO) is a method of authentication that enables users to access various applications or services using only one set of login credentials. Rather than having to remember and enter separate usernames and passwords for each application, users can log in once and gain access to all the connected systems without having to log in again for each one.

"Force SSO" is a setting or policy in a Single Sign-On (SSO) system that requires users to authenticate through the SSO mechanism whenever they try to access protected resources or applications. Even if they are already logged in to other systems or applications within the organization, Force SSO mandates users to log in using their SSO credentials whenever they attempt to access a designated application or service. This approach ensures consistent authentication and access control across all integrated systems, enhancing security by centralizing user authentication and reducing the risk of unauthorized access. The "Force SSO" setting is available in DrChrono, and can be applied to an entire practice group. This means that all users within the group will be required to log in exclusively with SSO (Single Sign-On). It's important to note that "Force SSO" cannot be applied to some users and not others within the practice group.

Before enabling Force SSO in DrChrono for your practice group, please make sure everyone in your PG has SSO set up for their login and that their request is linked to an existing user. If this step is not completed before Force SSO is enabled, users whose requests are not linked to an existing user will be unable to log in to DrChrono. If you want to set up Force SSO for your entire practice group, please enter a ticket here so our team can assist.

Why You Should Consider Using SSO

Enabling SSO within DrChrono for your practice can bring several benefits:

1. Enhanced Security: SAML SSO ensures that user authentication is centralized and standards-based, reducing the risk of unauthorized access and data breaches.

2. User Convenience: SAML SSO allows users to log in once and seamlessly access DrChrono without repeatedly entering credentials.

3. Compliance Requirements: SAML SSO provides a secure authentication mechanism for centralized access control and auditing, which helps meet regulatory requirements.

4. Efficiency and Productivity: SAML SSO streamlines user authentication by eliminating the need to manage

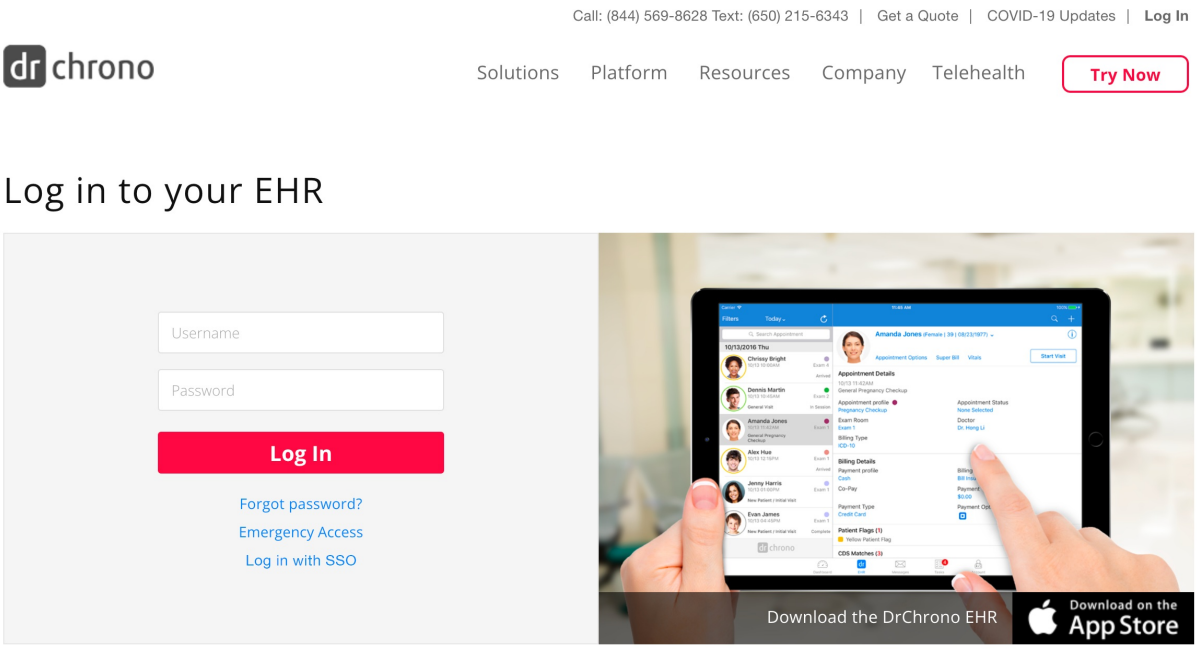
multiple credentials.

5. Streamlined Administration: SAML SSO streamlines user access management by allowing administrators to centrally manage user access from one dashboard.

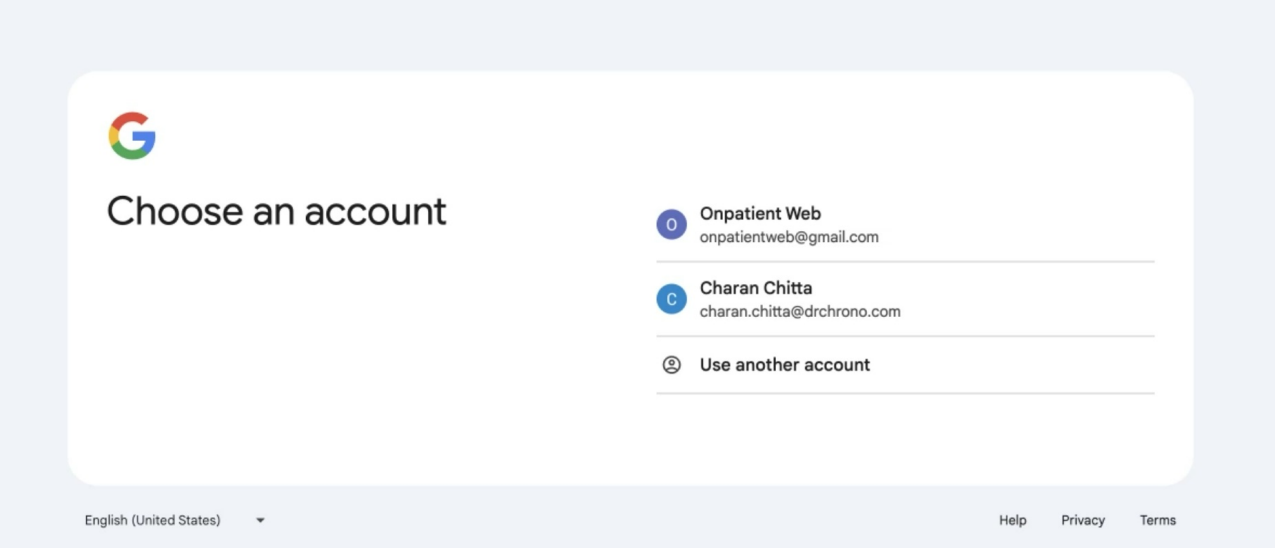
Requesting SSO for Your Account

First, you will need to set up your practice group and email with an Identity Provider. To learn more, visit Setting up an Identity Provider for SSO.

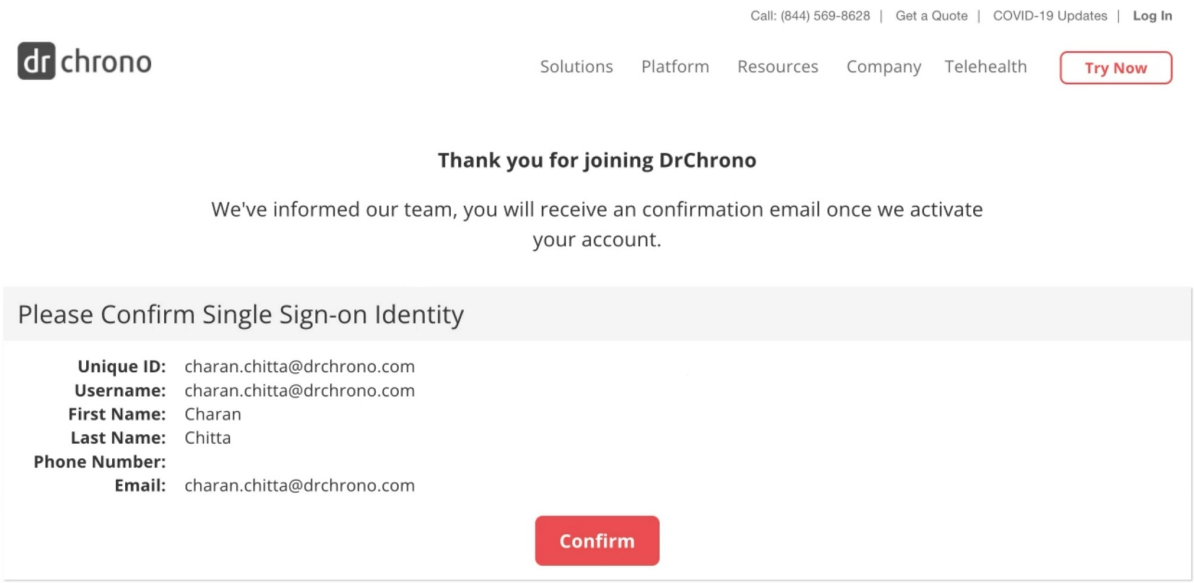
To make an SSO request, have the user log in to DrChrono by selecting "Log in with SSO."



Once the user logs in, they will be redirected to select their account. This screenshot below is an example using Google as the Identity Provider.



After the user selects their account, they will see the screen below to confirm their SSO Identity. Select "Confirm."



After confirming, your request will be visible on the SAML SSO Dashboard, where the practice group admin can link the user's request to an existing user. Please note that 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. Your request must be linked to an existing user to use SSO.

Once your request is accepted, you will receive a confirmation email and be able to use the new login workflow. For more information on the new login workflow, please visit SSO New Login Workflow.