Utilizing the New SSO Dashboard

The new SAML SSO (Security Assertion Markup Language Single Sign-On) Dashboard in DrChrono is a centralized place for managing users and their SSO access within DrChrono. Its primary purpose is to allow practice administrators to oversee user authentication, authorization, and provisioning of SSO to users in their practice, ensuring a smooth and secure user experience within DrChrono. The SSO dashboard was created to empower practice administrators with the autonomy to manage their practice's access and authentication needs independently and improve operational efficiency.

Accessing the New SSO Dashboard

To view the new SAML SSO Dashboard in your account, please contact your office manager or administrator to ensure the **SAML SSO Admin Dashboard** permission is selected. We recommend turning on this permission only for users who will need to approve SSO requests.

To access the new SSO dashboard, hover over Account and select SAML SSO under Practice Settings.
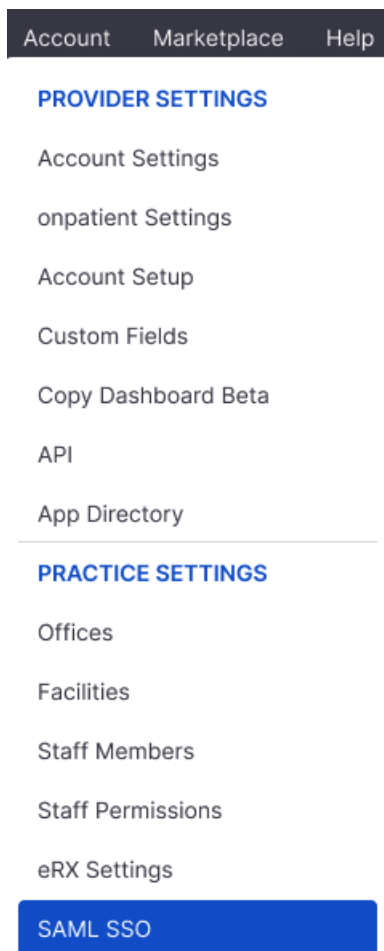
The SAML SSO Dashboard will show all SSO requests for your practice group and SSO Users.

The IDP (Identity Provider) will be specific to the IDP you chose for your practice group. While you may see all

users with the same IDP in the dashboard, you can only take action on users who are part of your practice group and location.

Approving an SSO Request

The SAML SSO Request page is where you can manage new SSO requests that require verification and linking to an existing user account before users can log in through SSO. Once you approve an SSO request, the user can log in through SSO successfully. If you don't approve the request, even if the user's credentials are valid, the user won't be able to log in through SSO. This list is populated the first time a user attempts to log in via SSO. Their request is sent to the SSO dashboard, where a practice admin verifies the user and links them to an existing account.

Users can generate requests by following these steps.

To approve an SSO Request, select "Link to Existing User" on the SAML SSO Request page.

A pop-up will appear, asking you to select a user. Search for the user to whom you would like to link the request and select "Activate."

Once you've linked a request to a user and activated the request, you can view the user under the SAML SSO Users.

If you want to remove a request at any time, you can select the red trashcan icon under Remove Request on the SAML SSO Request page.

Please ensure that every PG member has SSO set up for their login and that their request has been linked to an existing user before enabling force SSO for their practice group. 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.

Removing a User from the Dashboard

By removing a user from the SSO dashboard, you revoke their SSO access to DrChrono. This means they can no longer log in to DrChrono using single sign-on.

To remove a user from the dashboard, navigate to the SAML SSO User page. Find the user you want to remove and select the red "Remove User" button.

You'll then see a confirmation message at the top left of your screen, indicating that the user has been deleted successfully.
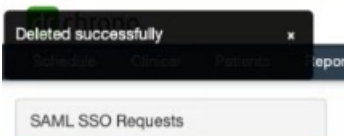
We recommend regularly looking at your existing users and removing anyone who may no longer work for your practice.

If you accidentally revoke a user, they'll reappear in the SAML SSO Request page list the next time they try to log in via SSO. This means that the user will need to go through the verification process again before gaining access.

Adding an SSO Request from the Dashboard

If you want to add an SSO user from the dashboard, navigate to the SAML SSO User screen and select "+SSO for Existing User."

A pop-up will appear, asking you to enter the required information to create a user. "Select User" indicates the username of the provider or staff member you are creating SSO for; "SSO Unique ID" indicates the username's email address, and the SSO Identity Provider would be the Practice Group Name or email domain. Users can search using partial keywords on all pages of the dashboard.

Once you select "Create," the user will appear in the User list without further action. The user can then log in via SSO.