Setting up an Identity Provider for SSO

07/08/2024 7:15 pm EDT

First, you will need to set up your practice group and email with an Identity Provider. We support many different Identity Providers. Below, you can find helpful references for setting up SSO with some of the Identity Providers we support, such as Google, Microsoft Azure, and Okta.

Google SAML SSO
Microsoft Azure SAML SSO
Okta SAML SSO

Download the IDP Metadata, send it in a support ticket to DrChrono, and include the IDP Metadata, routing name, and email domain name. We support multiple domains. The subject line of the support ticket should be "SSO Dashboard."

DrChrono will send back some information:

a. entityID: https://app.drchrono.com/sso/saml/{routing_name}/metadata/

b. ACS URL: https://app.drchrono.com/sso/saml/{routing_name}/acs/

c. Initial User/Start URL: https://app.drchrono.com/sso/saml/{routing_name}/login/

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL
ACS URL is required

Entity ID
Entity ID is required

Start URL (optional)

☐ Signed response

Name ID

Defines the naming format supported by the identity provider. Learn more

Name ID format
UNSPECIFIED ▼

Name ID
Basic Information > Primary email ▼

BACK   CANCEL   CONTINUE

User Setup

a. `username` : The unique identifier for this user. It can either be their email address or their DrChrono username.

b. `email` : The user's email address. This must be passed separately even if you used it as the `username` .

c. `first_name` : The user's first name. It's best if this and `last_name` match DrChrono's records, but they don't have to.

d. `last_name` : The user's last name.

e. `phone` : The user's phone number (optional).
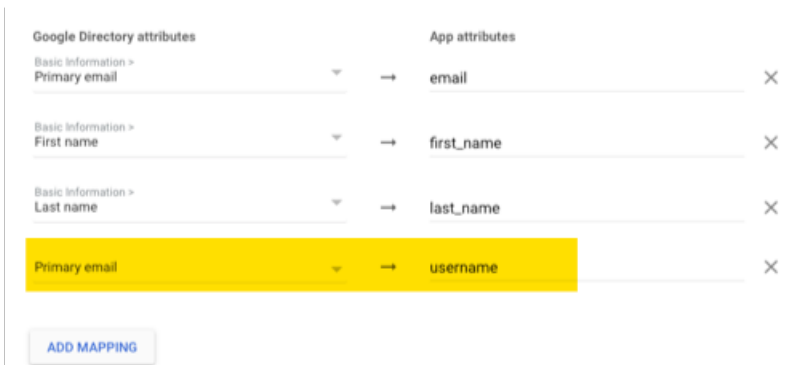
Once this is set up, your users can make SSO requests to DrChrono. Visit How to Request SSO for Your Account to learn more.