Set Up an Identity Provider for SSO

Last modified on 09/10/2026 3:46 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 are links to each vendor's own general documentation for creating a custom SAML app. These are vendor background reading, not drchrono-specific instructions — required attribute names and mappings vary by app, so use the attribute names in the **User Setup** section below (and the **Microsoft Entra (Azure AD) attribute mapping** section, if applicable) rather than any attribute names shown in the vendor's own examples.

- Google Workspace: Set up your own custom SAML app — Google's generic instructions for creating any custom SAML app in the Google Workspace admin console.
- Microsoft Entra (Azure AD): Add an enterprise application and configure single sign-on — Microsoft's generic tutorial for enabling SSO on any application in Entra.
- Okta: Create an app integration — Okta's generic developer guide for building an app integration. Use for background only.

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:

1. `entityID` : https://app.drchrono.com/sso/saml/{routing_name}/metadata/
2. `ACS URL` : https://app.drchrono.com/sso/saml/{routing_name}/acs/
3. `Start URL` (optional): Leave this field blank, or set it to `https://app.drchrono.com/sso/saml/login` (no routing name needed — DrChrono determines the correct practice from the user's email domain).

Once your IdP is configured, users sign in by going to the drchrono login page and selecting **Log in with SSO**, as described in How to Request SSO for Your Account.

User Setup

1. `username` : The unique identifier for this user. It can either be their email address or their DrChrono username.
2. `email` : The user's email address. This must be passed separately even if you used it as the `username` .
3. `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.
4. `last_name` : The user's last name.
5. `phone` : The user's phone number (optional).

Note: The attribute names above (`username` , `email` , `first_name` , `last_name` , `phone`) are correct for Google Workspace and most identity providers. If your identity provider is **Microsoft Entra (Azure AD)**, do not use these short names — see Microsoft Entra (Azure AD) attribute mapping below instead.

Microsoft Entra (Azure AD) attribute mapping

DrChrono accepts user attributes in two formats: the short names used in the User Setup section above, or the Microsoft claim URIs below. **Microsoft Entra requires the claim URI format.** Entra sends the username and email claims as claim URIs by default, so following the short-name instructions above for a Microsoft Entra app will produce a mixed configuration that fails sign-in.

Claim name	Entra value
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`	`user.userprincipalname`
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`	`user.mail`
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`	`user.givenname`
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`	`user.surname`

In Entra, these are configured under **Enterprise applications > [your drchrono app] > Single sign-on > Attributes and Claims**.

Important:

- All four attributes must use the *same* format — either all short names or all claim URIs. Do not mix the two formats. If some attributes arrive as claim URIs and others as short names, the short-name values are discarded and sign-in fails with a message saying the first and last name fields are required, even if they've already been added.
- Each attribute must have an actual value populated on the user's Entra profile. An empty first name or last name field in Entra produces the same error as a missing attribute mapping.

Troubleshooting

If a user sees an error like this when signing in with SSO:

```
{'user_attributes': {'first_name': [ErrorDetail(string=u'This field is required.', code=u'required')], 'last_name': [ErrorDetail(string=u'This field is required.', code=u'required')]}}
```

SAML authentication itself succeeded — the issue is with attribute configuration on the identity provider side, not with account setup in DrChrono. Specifically:

- This error is **not related to whether the user has been linked in the drchrono SAML SSO Dashboard**. Attributes are validated before the user link is checked, so this error can appear even when the user's SSO Dashboard link is correct.
- Check that `first_name` and `last_name` (or the equivalent Microsoft claim URIs, if using Microsoft Entra) are mapped and that they are not mixed with the other attribute format — see Microsoft Entra (Azure AD) attribute mapping above.
- Confirm the attribute has an actual value on the user's profile in the identity provider, not just a mapping with no data behind it.