Single Sign-On

Introduction

MedProctor's web product at https://secure.medproctor.com can function as a service provider (SP) for your SAML2 asserting federated identity provider (IdP). This document should answer most questions for a standard implementation of single sign-on using SAML2 assertions and workflows of a pre-defined scope. Any assertions, workflows, or scopes not covered in this document are unavailable at this time. This is a very technical document. Experience with the SAML2 SSO protocol will make reading it much easier.

Metadata

The URL for our SAML2 metadata endpoint is unique to your configuration and is available from MP support at dev@medproctor.com

Security

All assertions send to MedProctor MUST BE signed and encrypted. If your IdP cannot provide an XML assertion with both a signature digest AND a signed and encrypted assertion body, then let us know. We can update your configuration to accept an encrypted assertion without signature until you've updated your IdP to support this important part of the SAML2 specification.

Key pairs used by MedProctor's SAML response endpoints in our metadata are unique to your configuration. The public keys provided in the metadata link provided to you are configurable. You must use the provided, public keys at the metadata URL that MedProctor gives you to encrypt and sign your assertions to us. There are default keys provided with your configuration.

We support custom key pairs for signing and encrypting of assertions. We can verify or decrypt assertions with custom private keys and we will provide the paired public key at your metadata URL. Contact support at dev@medproctor.com to securely send your key pair.

We will need your metadata document and public key for signing and encryption if you use the SP-initiated web flow.

Attributes

We will resolve your assertion's attributes **only by full, SAML NameFormat**. We cannot map assertion attributes without the full NameFormat of the attribute. Consult your IdP for information on retrieving these values.

We can use your assertion attributes to provide required and some optional data for your authenticated users. The attributes you provide must be resolvable to the following list of accepted MedProctor claims and attributes.

- **username** – the assertion's subject name identifier will be used as the user's MedProctor UserName. **This attribute is required. If you do not provide one then the SAML Subject NameID will be used instead.**
- studentId – some unique ID. This attribute is useful for reporting processes where username might not be unique to your organization.
- emailPrimary – the user's primary email address
- emailSecondary – the user's primary email address
- telephone – the user's telephone number
- firstName – the user's given name
- lastName – the user's surname

Web flows

MedProctor supports an IdP-initiated web flow. You will need to provide us with a link to your IdP's SAML2 profile /Unsolicited/SSO endpoint. That link should be included on some student facing page that you host. A student clicks the link and authenticates with your IdP as needed. After authentication you will send a valid assertion to our ACS.

MedProctor supports an SP-initiated web flow. MedProctor will provide you with a link and logo for your page that will submit a properly signed and encrypted SamlResponse to your IdP's authn endpoint. You can include this logo and link on some student facing page that you host. A student clicks the link, we send your IdP a valid authn request, and you redirect the user to authenticate as needed. After authentication you will send a valid assertion to our ACS.

User Membership Scope

MedProctor uses roles to manage access control to resources at https://secure.medproctor.com. If an SSO user has been granted admin role membership by MP Support, then that user will be redirected to the admin dashboard by the SP. For assigning admin roles to users please contact MP support at dev@medproctor.com

Supported Protocols and Identity Providers

MedProctor only supports the SAML2 protocol for SSO. Many identity providers also support SAML2. You will need to consult your identity provider for information on integrating a SAML2 service provider like MedProctor. There are many different identity providers. MedProctor is not able to help with debugging or configuring your identity provider. Once your identity provider is ready to integrate with MedProctor using the technology outlined in this document, then we'll be happy to help.