Single Sign-On Overview

Updated September 2, 2021

Overview

Single Sign-On integration allows a customer's end-users to log into the NovoEd platform using their identity-provider, instead of maintaining a NovoEd password. If you are interested in SSO integration for your organization, please contact your Customer Success Manager to kickstart the process.

How does SSO work with NovoEd?

The NovoEd platform uses the SAML 2.0 protocol for single sign-on integration. For the SAML 2.0 protocol, the following roles are defined:

- SAML Authority: The Customer's Identity-Provider
- SAML Consumer: Service-Provider (NovoEd)
- Principal: End-User (Learners, Administrators)

SP-Initiated Workflow:

NovoEd prefers to utilize an SP-initiated workflow to provide end-users with access to the NovoEd platform.

1. End-user accesses a URL to the customer's NovoEd institution.
2. NovoEd redirects the end-user to the identity-provider login page with a SAML Request asking the identity-provider for a SAML Assertion.
3. The end-user logs into the identity provider with their credentials.
4. The end-user returns to NovoEd with a SAML Assertion that confirms their identity.

NOTE: An IdP-initiated workflow can be set up by request.

Common Identity Providers

For SSO integration, a customer's identity provider must support the SAML 2.0 protocol. Below is a list of common identity providers our customers have used for SSO integration with NovoEd:

- Active Directory Federation Services (ADFS) - Microsoft
- Auth0 - Auth0
- Azure Active Directory - Microsoft
- Okta - Okta
- PingFederate - Ping Identity