Using Snyk with SAML Single Sign-on (SSO)

The process of establishing trust between your identity provider and Snyk requires a few separate steps. Read Introduction to Snyk Single Sign-On for more information.

Snyk details you need to set up in your identity provider

Entity ID	**urn:auth0:snyk:saml-{customer_name}** (Replace {customer_name} with your value.)
ACS URL	**https://snyk.auth0.com/login/callback?connection=saml-{customer_name}** (Replace {customer_name} with your value.)
Signing certificate	**https://snyk.auth0.com/pem**

Name your user attributes as follows (using the same capitalization and spelling):

Attribute	Definition
email	The user email address
name	The name of the person to be authenticated
username	The person's username for the identity provider

SAML information to provide to Snyk:

Obtain the following information from your identity provider and organization. You'll provide this information to Snyk in order to establish trust on the service-provider side.

Sign-in URL	The URL for your identity provider sign-in page
X509 Signing Certificate	The identity provider public key, encoded in Base64 format
Sign-out URL	Optional, but recommended - The URL for redirect whenever a user logs out of Snyk
User ID attribute	Optional (default) **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier**
Protocol binding	HTTP-POST is recommended, HTTP-Redirect is also supported
IdP initiated flow supported?	Recommended
Email domains and subdomains	The email domains and subdomains that need access to the SSO