Snyk Customer Onboarding

Thank you for signing up to Snyk!

This guide has been designed to get you up and running with Snyk SSO as quickly and as easily as possible.

SSO

Setting up Single Sign On allows your developers and teams to easily login to Snyk to see the status of their projects, view reports, resolve vulnerabilities etc, using your corporate Sign On Provider.

Snyk can integrate with any SAML based SSO or ADFS.

Snyk has two environments where we would like to set up SSO. Please let us know if you cannot accommodate this ask.

Ideally we would also like a user account (username and password) that we can test with, as this generally makes set up faster. But we understand if this is not possible.

SAML settings

Snyk details you need to set up in your identity provider

1. snyk env:

Entity ID - urn:auth0:snyk:saml-{customer_name}

ACS URL -

https://snyk.auth0.com/login/callback?connection=saml-{customer_name}

Signing cert - https://snyk.auth0.com/pem

Set the following user attributes:

email - the user email address

name - the user name

username - the user username

Information we need from you

1. Sign-In URL
2. X509 Signing Certificate (Identity Provider public key encoded in PEM or CER format)
3. Sign-Out URL (optional, recommended)
4. All email domains and subdomains that need access to the SSO
5. User id attribute (optional, default is http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)
6. Protocol binding (HTTP-POST is recommended, HTTP-Redirect is also supported)
7. Whether or not IdP-initiated flow is supported (recommended)

   **Need to ensure you are exposing the email attribute for us to pick up in the payload for access to both the Snyk platform and support website.

Azure AD Non Gallery App settings

Snyk details you need to set up in your identity provider

Redirect URIs - https://snyk.auth0.com/login/callback

Information we need from you:

1. Client ID
2. Client Secret

3. Microsoft Azure AD Domain (numbers and letters): Azure portal -> App registrations -> Open the Snyk app that you created -> Overview → please send us the value of "Directory (tenant) ID"

ADFS configuration details

Snyk details you need to set up in your identity provider

1. snyk-test env:

Realm Identifier: urn:auth0:snyk-test

Callback URL - https://snyk-test.auth0.com/login/callback

2. snyk env:

Realm Identifier: urn:auth0:snyk

Callback URL - https://snyk.auth0.com/login/callback

Information we need from you

1. ADFS URL or Federation Metadata XML file

User Assignment

There are different options we can apply to how a user gets access to Snyk organisations when they sign up to Snyk for the first time. Please choose one of the following and let us know your preference:

- Option 1 - Open to all
  All users are added to all organisations either as an admin or a collaborator.

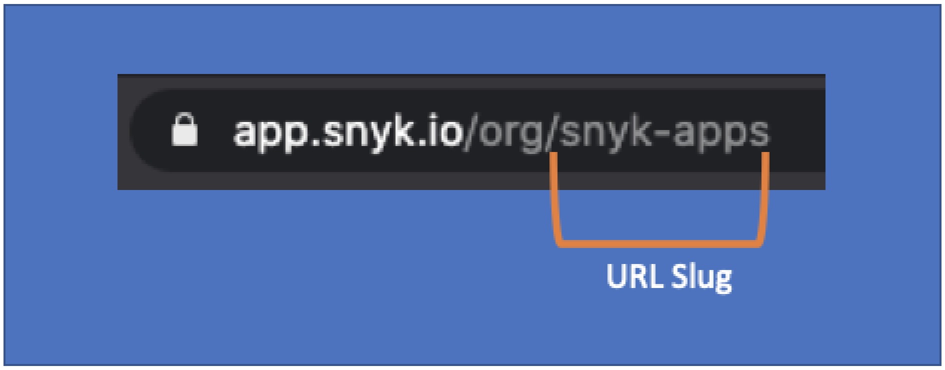
  If selecting this option please let Snyk know the role you would like users to be added as.

- Option 2 - Closed - requires invitation
  The user gets added to an organisation either by receiving an invitation which has been sent by an organisation admin or by the admin adding the user to an organisation after they have signed in for the first time. When the user signs in to Snyk for the first time without receiving an invitation they will see a list of all the orgs and the email addresses of admins who they can contact to request access.

- Option 3 - Org assignment based on information from your identity provider.

  Snyk can map the user to an organisation if you pass an attribute which includes the org name. These attributes must be in an array attribute called `roles` and each element's attribute name will need to adhere to the following pattern: `snyk-{orgName}-{role}`

  - `{orgName}` must match the org slug which appears in the url for each organisation in the Snyk UI. Please note this may differ from the display name for the organisation



app.snyk.io/org/snyk-apps

- {role} must be one of "admin" or "collaborator"

  Example:

```
{
        "roles": [
                "snyk-my-org-admin",
                "snyk-my-other-org-collaborator",
        ],
}
```

- To assign group admin privileges via this mechanism, apply the attribute name as: `snyk-groupadmin`

  Example:

```
{
        "roles": [
                "snyk-groupadmin",
        ],
}
```

Personal Orgs

As well as having access to your company’s Snyk organisations you can also allow them to have access to a personal organisation which they can use for their personal projects. By default we disable this feature.

Should users have a personal organisation as well as having access to the company’s snyk organisations? [**Y / N]**

Once an SSO config is enabled to a group, members’ invitation will redirect the invited user to the SSO tenant page and will prevent them from using the social logins