A black and white logo

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Document name | DevSecOps Tool: Snyk User Guide |
| Version no. | 1.0 |
| Release date | 12th oct 2023 |
| Document ID | *1* |
| Classification | Internal |

|  |
| --- |
| DevSecOps Tool: Snyk User Guide |

# Document History

| Ver. No | Release Date | Created By / Modified By and Date | Reviewed By and Date | Approved By and Date | Remarks and Changes Made |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 8th February 2023 | Ruturaj Sunil Kharde/ 12th Oct 2023 | Prasad Gattetwar and Rajanigandha Gaikwad /5th Dec 2023 |  |  |

# Table of Contents

[Document History 2](#_Toc152677009)

[Table of Contents 3](#_Toc152677010)

[1. scaN and Code Coverage using cli 4](#_Toc152677011)

[1.1 WHAT IS SNYK ? 4](#_Toc152677012)

[1.2 THE SNYK DEVELOPER-FIRST APPROACH 4](#_Toc152677013)

[1.3 USE SNYK IN YOUR WORKFLOW 4](#_Toc152677014)

[2. Implementation steps with Repos 5](#_Toc152677015)

[2.1 INTEGRATION WITH AZURE DEVOPS REPOSITORY 5](#_Toc152677016)

[2.2 ADD PROJECT TO SNYK FROM AZURE REPO 6](#_Toc152677017)

[3. Implementation steps with AZURE DEVOPS BUILD PIPELINE 7](#_Toc152677018)

[3.1 INTEGRATION WITH AZURE DEVOPS CI PIPELINE 7](#_Toc152677019)

[4. Implementation steps with CLI (LOCAL SCANNING) 9](#_Toc152677020)

[5. References 11](#_Toc152677021)

# scaN and Code Coverage using cli

## WHAT IS SNYK ?

Snyk is a platform allowing you to scan, prioritize, and fix security vulnerabilities in your code, open source dependencies, container images, and infrastructure as code configurations

## THE SNYK DEVELOPER-FIRST APPROACH

Developers now assemble applications with a combination of proprietary and open-source code, run that code in containers, and then deploy with infrastructure as code configurations using technologies like Kubernetes and Terraform.

A good security process secures each of these components where they are built and maintained. Snyk integrates into DevOps processes to work with developers using the methods each prefers, while following and supporting industry best practices. Snyk integrates directly into your IDEs, workflows, and automation pipelines to add security expertise to your toolkit.

## USE SNYK IN YOUR WORKFLOW

* **Secure your code**: use [Snyk Open Source](file:///C:\scan-applications\snyk-open-source) to fix vulnerabilities in your open source dependencies and [Snyk Code](file:///C:\scan-applications\snyk-code) to fix vulnerabilities in your source code.
* **Secure your containers**: use [Snyk Container](file:///C:\scan-applications\snyk-container) to fix vulnerabilities in container images and Kubernetes applications.
* **Secure your deployment**: use [Snyk Infrastructure as Code (IaC)](file:///C:\scan-infrastructure\snyk-infrastructure-as-code) to fix misconfigurations in Terraform, CloudFormation, Kubernetes, and Azure templates. Use IAC to fix misconfigurations in Amazon Web Services accounts, Microsoft Azure subscriptions, and Google Cloud projects.

# Implementation steps with Repos

## **INTEGRATION WITH AZURE DEVOPS REPOSITORY**

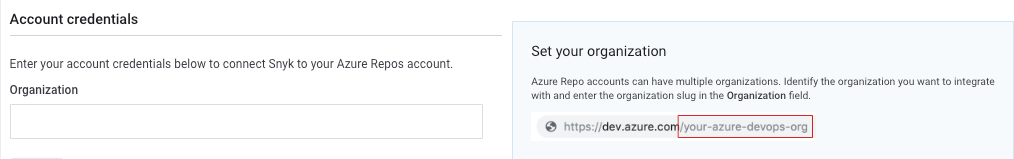
**Step 1**: Log/signup in to your Snyk account and navigate to Integrations tab/section

(You can do the signup using Google account or GitHub account on its official link https://snyk.io)

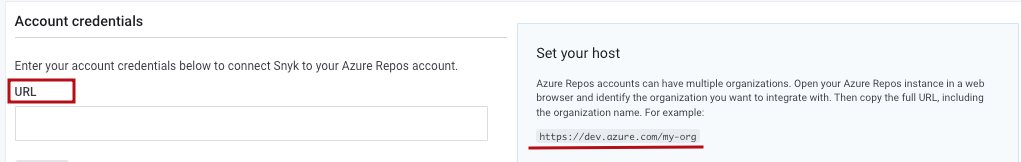
**Step 2**: On Snyk account dashboard, click the *Settings* > *Integrations* > *Azure Repos* ‘Edit setting’ > we need to focus on the *Account credentials* section.

**Step 3**: Pay special attention to the instructions given on the Account Credentials section. Depending on your plan, you may need to enter just the Azure DevOps Organization name, or you may need to enter the entire URL.

* **Set your host**: enter the name of your organization, for example, almvsts1 and the hit NEXT button



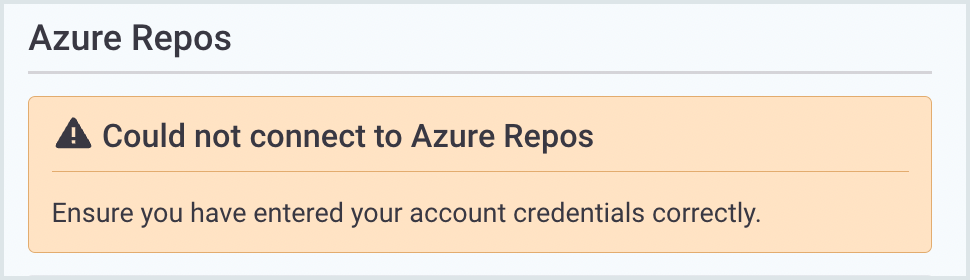
* **Or, you may get the below interface to input your organization url. Set your host**: enter the entire url, for example, enter https://dev.azure.com/your-azure-devops-org Alternatively, you may enter a custom url that is publicly reachable



**Step 4**: Enter the PAT that you generated from your Azure DevOps Service/Server and then hit Save button

**Step 5**: Snyk tests the connection values and the page reloads, displaying the Azure Repos integration information. A message to confirm that the details were updated appears at the top of the screen in green color with CONNECTED keyword

If the connection to Azure fails, a notification appears under the Azure Repos card title in red color, as shown in below image



## **ADD PROJECT TO SNYK FROM AZURE REPO**

To add a default Project:

**Step 1**: Go on Snyk dashboard, navigate to the following setting , *Projects 🡪 Add projects.*

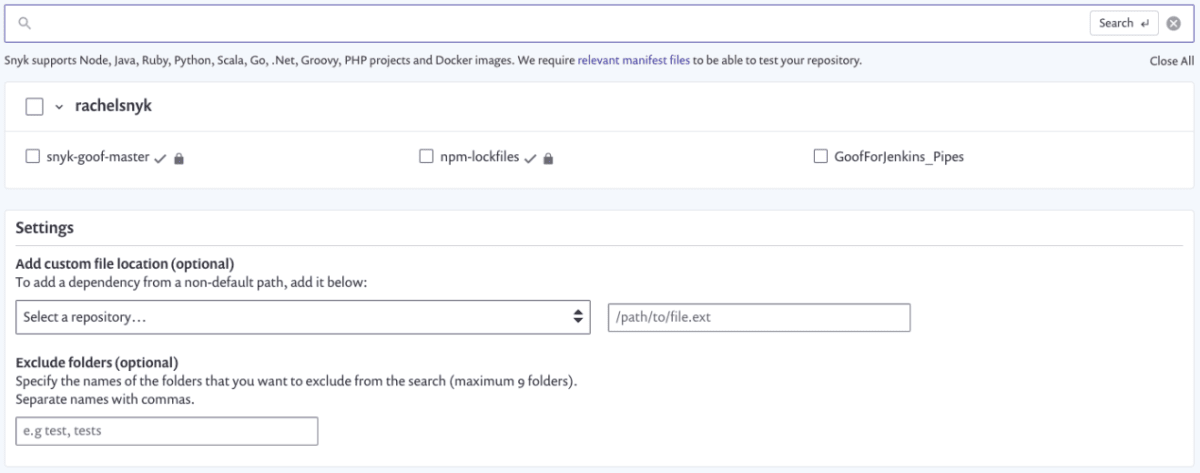
**Step 2**: Choose the relevant repository from which your projects needs to be imported.

**Step 3**: The available repositories for the integration you chose are displayed in a new window.

**Step 4**: Select the repositories that you want Snyk to monitor for security and license issues.

**Step 5**: To import the repos for a specific Organization, enable the check box.

**Step 6**: Click *Add selected repositories* button. Snyk scans the projects from selected respective repos and imports them to Snyk as project on dashboard.



# Implementation steps with AZURE DEVOPS BUILD PIPELINE

## **INTEGRATION WITH AZURE DEVOPS CI PIPELINE**

**Step 1**: Access your Snyk account.

**Step 2**: Token:

**2.1** For free plans, go to your *Account setting* from left bottom panel by clicking on user name> locate *General* tab >locate the Auth Token section >locate the key text box .Copy it on note pad

**2.2** For paid plans, navigate to the Organization where you want to integrate; then go to Settings to create a new service account token. Copy and save it on the side.

**Step 3**: Access your Azure DevOps Server/Services account and navigate to the Extensions -> Browse marketplace.

**Step 4**: Search for the Snyk Security Scan extension and click Get it free.

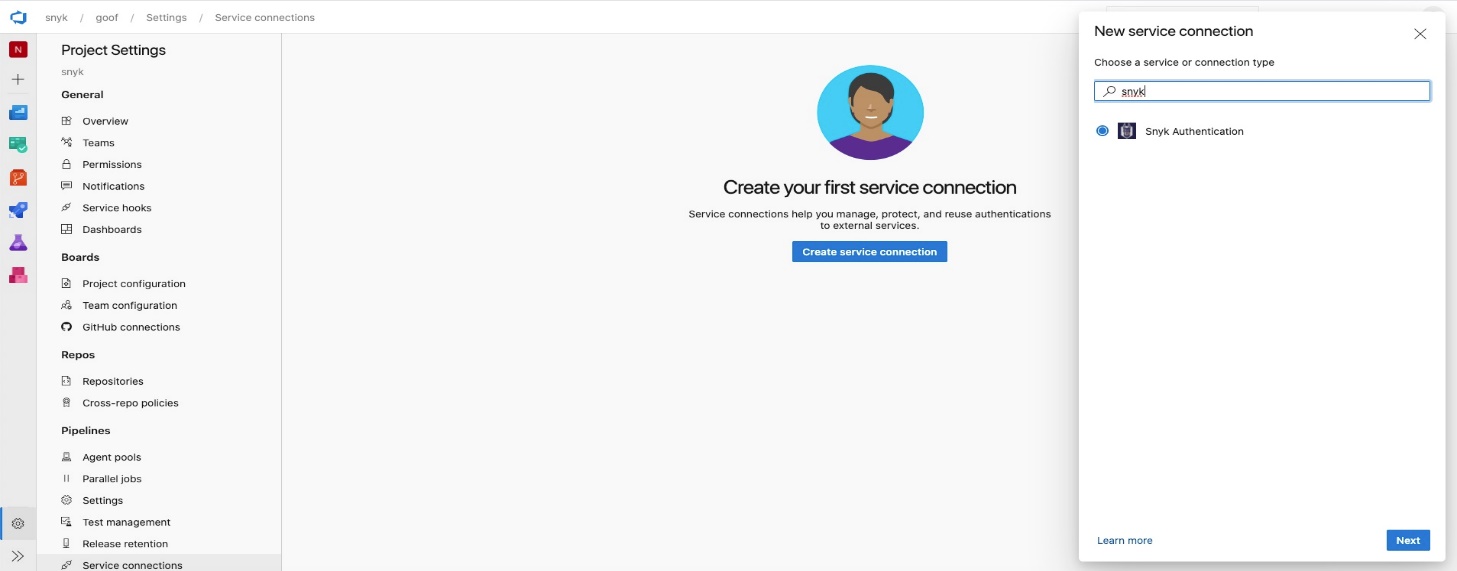
**Step 5**: Create a new Service Connection in your Project via *Project Settings —> Pipelines —> Service Connections* and click on *New service connection*

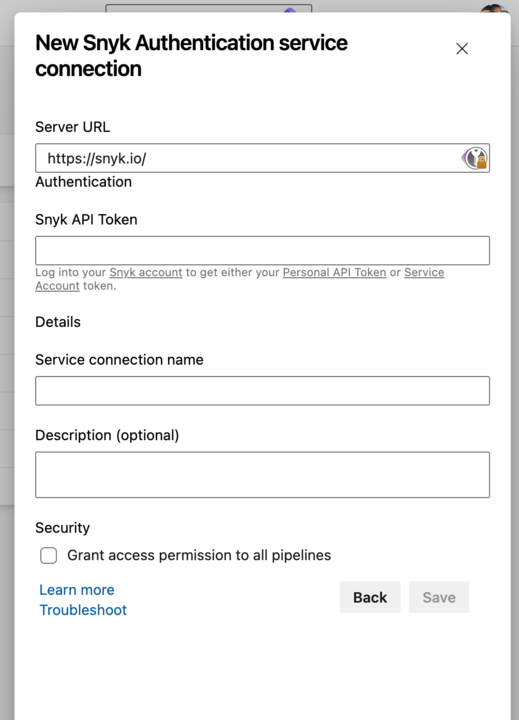
**Step 6**: Search and select the Snyk Authentication service connection:

**6.1** In the Snyk Authentication service connection, enter the Snyk API Token that we have taken in step 2.1

**6.2** Click Save, ensuring the new service connection appears in your list of service connections.

**Step 7:** Finally, you are good to go with pipeline scan.





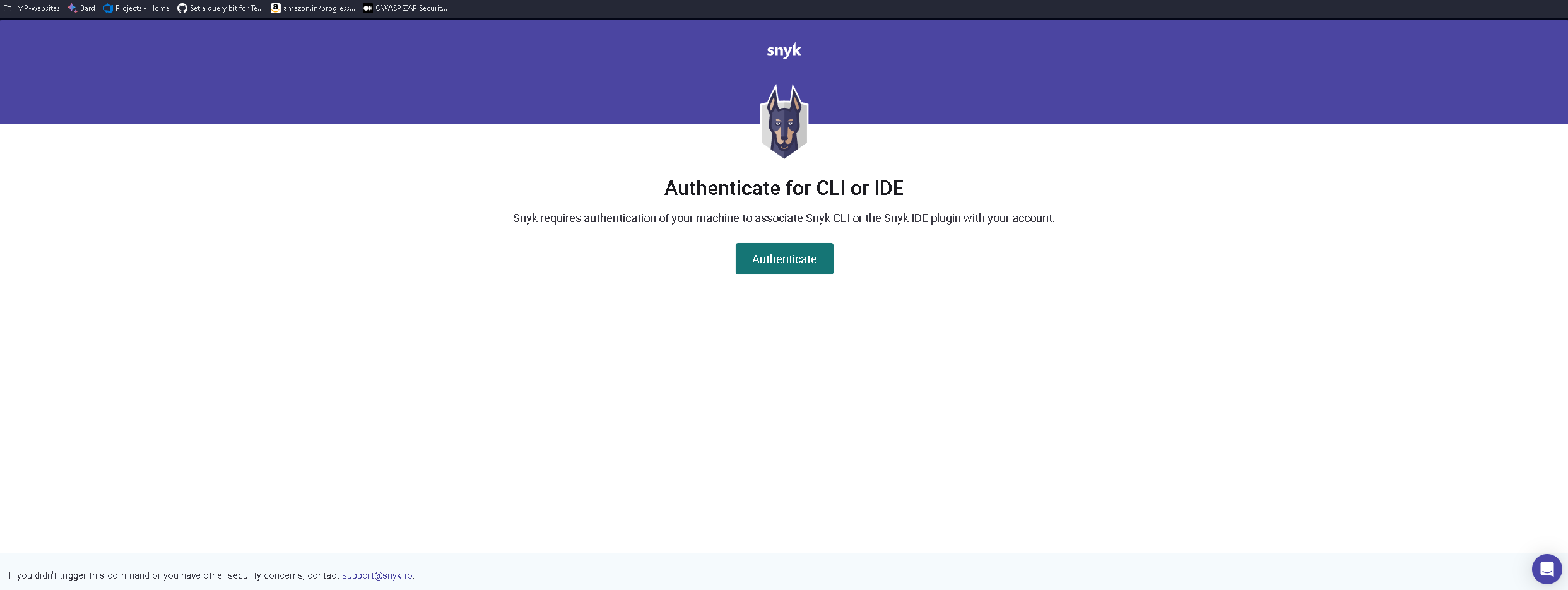
# Implementation steps with CLI (LOCAL SCANNING)

**Step 1**: Open PowerShell in admin mode.

**Step 2**: For window OS ,execute the below command curl [https://static.snyk.io/cli/latest/snyk-win.exe -o snyk.exe](https://static.snyk.io/cli/latest/snyk-win.exe%20-o%20snyk.exe)

**Step 3**: An Snyk executable file would have been downloaded in your system, add its path in environment variable.

**Step 4**: Execute the command snyk auth, It will open the interface shown in below image on browser. Click on Authenticate



**Step 5**: Now to do the analysis run the below command depending on your requirements from the root path of the project

* Scanning of project with source code

*snyk code test --org=2c3eda80-fad0-4717-8a34-026e93847424*

|  |  |
| --- | --- |
| snyk code test | Scans your source code for vulnerabilities introduced by your first party code. |
| org=<ORG\_ID> | Specifies the Organization ID to run Snyk commands for a specific organization. It influences where new projects are created after running the monitor command. Find the Org ID on your Organization’s Settings page (Settings > General). |

* Scanning of Containers

To scan container images for vulnerabilities copy the command below and specify the container image by **replacing <repository> and <tag>.**

1. To scan your projects locally

*snyk container test <repository>:<tag> --org=2c3eda80-fad0-4717-8a34-026e93847424*

1. To continuously monitor your projects and view the latest snapshots in Snyk Dashboard

*snyk container monitor <repository>:<tag> --org=2c3eda80-fad0-4717-8a34-026e93847424*

|  |  |
| --- | --- |
| snyk container test | Scans your container images for any known vulnerabilities. |
| snyk container monitor | Captures the container image layers and dependencies and monitor for vulnerabilities. View the latest snapshots and scan results in the Web UI, on the Projects page. |
| --all-projects | Auto-detects all projects in the working directory. |
| --org=<ORG\_ID> | Specifies the Organization ID to run Snyk commands for a specific organization. It influences where new projects are created after running the monitor command. Find the Org ID on your Organization’s Settings page (Settings > General). |

# References

[Snyk | Developer security | Develop fast. Stay secure. | Snyk](https://snyk.io/)