

Requirements to start using the Template

1.SPN - Service Principal Name

An Azure service principal is an identity created for use with applications, hosted services, and automated tools to access Azure resources. This access is restricted by the roles assigned to the service principal, giving control over which resources can be accessed and at which level. For security reasons, it is always recommended to use service principals with automated tools rather than allowing them to log in with a user identity.

We require 3 Service Principal Names (SPN).

- a. SPN for AKV [Azure Key Vault] - This is to connect GitHub actions.
 - Access Level– customize [Read and List]
- b. SPN for ACR (Azure Container Registry) [Azure Container Register] - To push and pull images from the CI pipeline.
 - Access Level – customize [Push and Pull]
- c. SPN for RG (Resource Group) [Resource Group]
 - Access Level – customize [Read and Write]

Request for SPN must be raised on <https://abinbevwww.service-now.com/>

Teams To Contact: OneABI-AzureAD-Support@ab-inbev.com

DL-Global_Cloud_Operations@ab-inbev.com

2.Service Email

A common Email used by Operations Team, this email is always linked to an admin email for approvals and password changes. When a service email id is requested, it should be made sure that multifactor authentication is deactivated.

Request for SPN must be raised on <https://abinbevwww.service-now.com/>

Teams To Contact:

3.Sonar Cloud:

SonarCloud is an online service to catch Bugs and Security Vulnerabilities in Pull Requests and throughout the code repositories. SonarCloud pairs with existing cloud-based CI/CD workflows and provides clear resolution guidance for any Code Quality or Security issue it detects. SonarCloud empowers development teams of all sizes to write cleaner and safer code, across more than 20 programming languages.

To get access to sonar cloud: <https://sonarcloud.io/> and integrate with the GitHub organization.

4.Snyk:

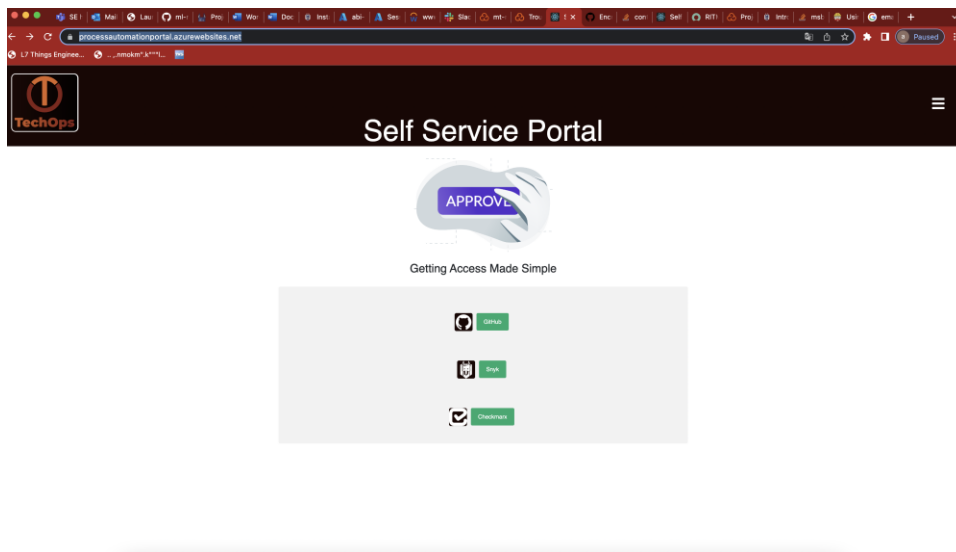
Snyk tests for vulnerabilities in the code, open-source dependencies, Container images, and Infrastructure as Code (IaC) configurations, and offers context, prioritization, and fixes.

For Snyk Integration with CI/CD pipeline the parameters required are

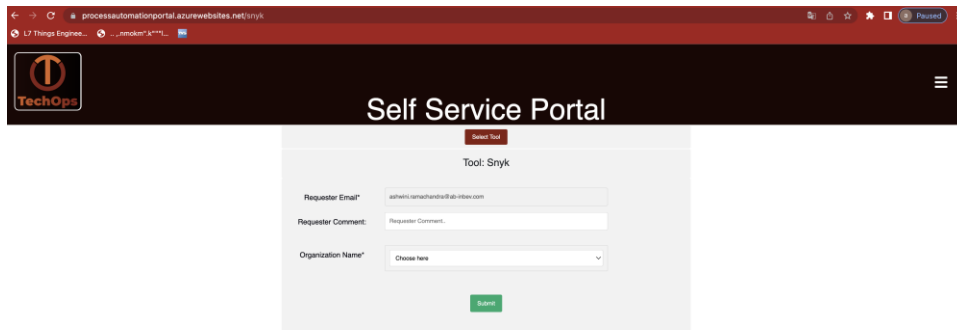
SNYK_TOKEN

SNYK_ORGID

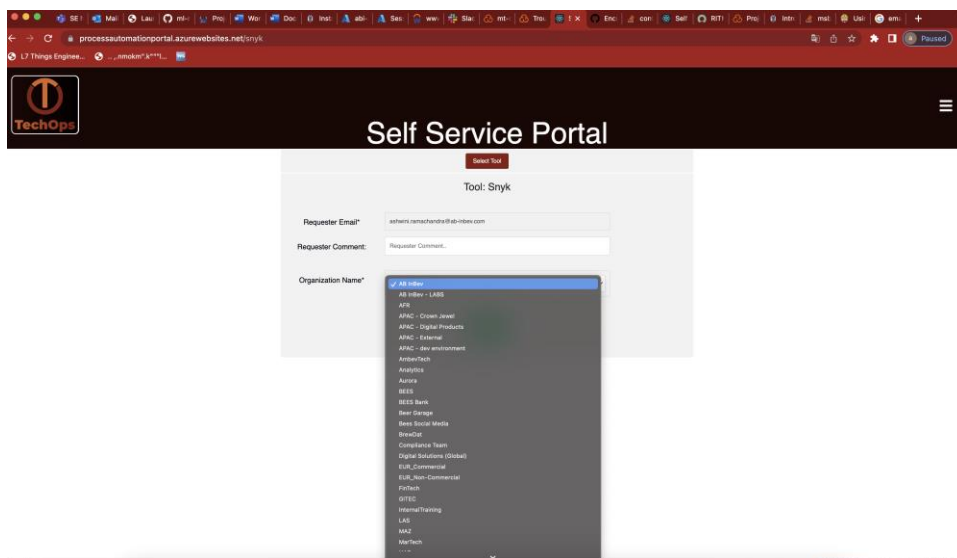
Self Service Portal <https://processautomationportal.azurewebsites.net/> can be used to raise request for Snyk access



-----> Click on Snky.



The screenshot shows a web browser window with the URL `processautomationportal.azurewebsites.net/snyk`. The page has a dark red header with the "TechOps" logo on the left and a hamburger menu on the right. The main content area is titled "Self Service Portal" and "Tool: Snky". Below this, there is a form with three fields: "Requester Email*" with the value `esherin.ramachandra@ab-vibex.com`, "Requester Comment:" which is empty, and "Organization Name*" with a dropdown menu showing "Choose here". A green "Submit" button is at the bottom of the form.



This screenshot is identical to the previous one, but the "Organization Name*" dropdown menu is open, displaying a list of organization names. The list includes: "AB India - LABS", "AFB", "AFAC - Client Dev", "AFAC - Digital Products", "AFAC - External", "AFAC - Dev environment", "Amesoft", "Analytics", "Antics", "BES", "BES Bank", "Best Sengs", "Best Social Media", "BroadCast", "Compliance Team", "Digital Solutions Global", "EUR_Commercial", "EUR_Non-Commercial", "FedTech", "GITEC", "Internal Training", "LAV", "MA2", "MarTech", and "..." at the bottom.

-----> Select your organization name.

5.CheckMarx:

CxFlow automates scanning earlier in the code management process by integrating directly into source control management systems or CI/CD tools.

1.Automated Project Creation.

2.Checkmarx CxFlow CLI is invoked, and it triggers security scan via Checkmarx Scan Manager.

For Checkmarx integration with CI/CD pipeline the parameters that are required are:

CHECKMARX_TEAMS

CHECKMARX_URL

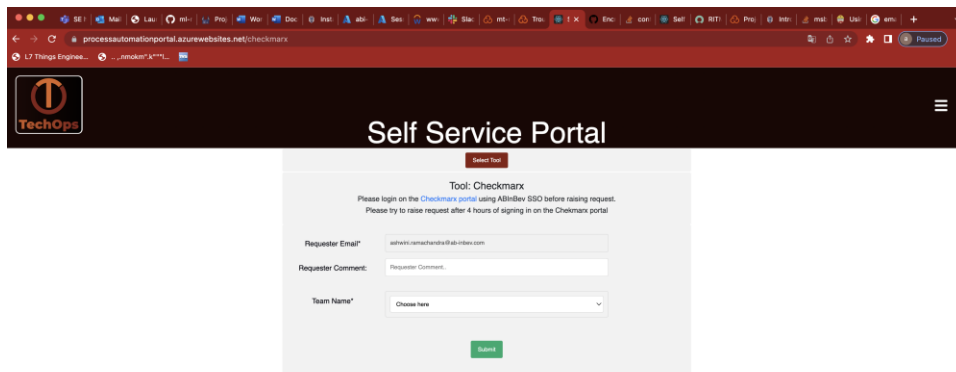
CHECKMARX_USERNAME

CHECKMARX_PASSWORD

CHECKMARX_CLIENT_SECRET

To get the above parameters to be created need to contact nandhagopal.s@ab-inbev.com and his team.

Self Service Portal <https://processautomationportal.azurewebsites.net/> can be used to get Checkmarx Access.

The image shows a web browser window displaying the 'Self Service Portal' for Checkmarx. The page has a dark header with the 'TechOps' logo on the left and a hamburger menu on the right. Below the header, there's a 'Select Tool' button. The main content area is titled 'Tool: Checkmarx' and includes instructions: 'Please login on the Checkmarx portal using AAD/B2B SSO before raising request. Please try to raise request after 4 hours of signing in on the Checkmarx portal'. There are three input fields: 'Requester Email*' with the value 'nandhagopal.s@ab-inbev.com', 'Requester Comment*' which is empty, and 'Team Name*' which is a dropdown menu showing 'Choose here'. A green 'Submit' button is at the bottom of the form.

-----> Select the team that was created with the help of Mr.Nandhagopal and his team.

6. Azure Database for MySQL[PaaS]:

Azure Database for MySQL is a relational database service powered by the MySQL community edition. You can use either Single Server or Flexible Server to host a MySQL database in Azure. It is a fully managed database as a service offering that can handle mission-critical workloads with predictable performance and dynamic scalability.

- a. Admin User and Admin Password must be created.
- b. To access the database from the code on local Ips of the users or the service from which it is accessed must be whitelisted from the portal
- c. To maintain the database or to whitelist the Ips individuals from the Operations team must raise access requests.
- d. Service Request can be raised on <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- e. Service Access can be raised on <https://abinbevww.service-now.com/>

7. Azure Container Registry [ACR]:

The Azure container registry is Microsoft's own hosting platform for Docker images. It is a private registry where you can store and manage private docker container images and other related artifacts. These images can then be pulled and run locally or used for container-based deployments to hosting platforms.

- a. To Access ACR the id and password of the SPN created to access the ACR must be used [to push and pull the images].
- b. Individuals from the Operations team must make a request to maintain the Service.
- c. Service Request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- d. Service Access request can be raised on: <https://abinbevww.service-now.com/>

8. Azure Key Vault [AKV]:

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

- a. Service Request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- b. Service Access Request can be raised on: <https://abinbevww.service-now.com/>

9.Azure Storage:

The Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers available, massively scalable, durable, and secure storage for a variety of data objects in the cloud. Azure Storage data objects are accessible from anywhere in the world over HTTP or HTTPS via a REST API.

- a. Individuals from the Operations team must make a request to maintain the Service.
- b. Service request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access Request can be raised on : <https://abinbevww.service-now.com/>

10.Azure App Service:

Azure App Services provide a hosting service that developers can use to develop mobile or web apps. Apart from this, developers can also use it to build API apps or Logic apps, which provide integration with SaaS. It replaces several separate Azure services, which include Azure Website, Azure Mobile Services, and Azure BizTalk Services, and gives you a single product called Azure App Services.

It also has DevOps features including continuous deployment via Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domains, and TLS/SSL certificates.

- a. Individuals from the Operations team have to raise a request to maintain the Service.
- b. Service request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access Request can be raised on: <https://abinbevww.service-now.com/>

11.Azure Container App:

Azure Container Apps is an app-centric service, empowering developers to focus on the differentiating business logic of their apps rather than on cloud infrastructure management. Azure Container Apps executes app code packaged in any Linux-based container without enforcing opinionated runtimes or programming models. Scale all the way down to zero or scale out to meet global demand in response to HTTP requests or events. Alternatively, Azure Container Apps supports running apps as always-on background services.

- a. Individuals from the Operations team must make a request to maintain the Service.

- b. Service Request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access can be raised on: <https://abinbevww.service-now.com/>

12.Azure Container Instance [ACI]:

Azure Container Instances (ACI) is a managed service that allows you to run containers directly on the Microsoft Azure public cloud, without requiring the use of virtual machines (VMs).

- a. Individuals from the Operations team must make a request to maintain the Service.
- b. Service Request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access request can be raised on: <https://abinbevww.service-now.com/>

13.Azure VM:

An Azure virtual machine is an on-demand, scalable computer resource that is available in Azure. Virtual machines are used to host applications when the customer requires more control over the computing environment than what is offered by other compute resources.

- a. Individuals from the Operations team must make a request to maintain the Service.
- b. Service Request can be raised on: <https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access request can be raised on : <https://abinbevww.service-now.com/>

14.Azure App Gateway:

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

- a. Individuals from the Operations team must make a request to maintain the Service.
- b. Service Request can be raised on:<https://abinbevww.service-now.com/abiex?id=cloudbolt>
- c. Service Access Request can be raised on: <https://abinbevww.service-now.com/>

15.Resource Group:

A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Generally, add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.

- a. Request to Create a resource Group: <https://abinbevwww.service-now.com/>