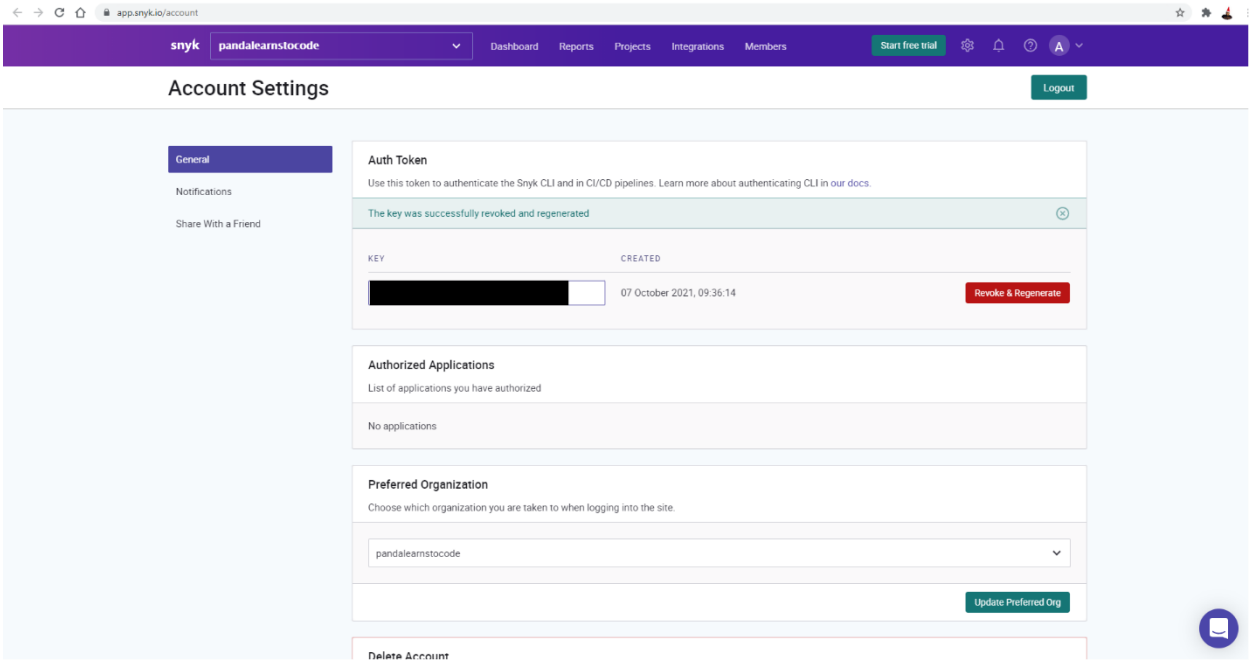
Container scanning using snyk

Step 1: Login to snyk.io → Login using GitHub account or SSO → Import a repository you want to scan.

Step 2: Go to https://app.snyk.io/account → Generate API token → Copy the value and keep it → Go to GitHub repository secret → Create a new env variable → Name of the variable will be `SNYK_TOKEN` and copy paste the value generated in the link above → save.



Step 3: Add the synk related section in GitHub action.

```
with:
  login-server: <docker registry name goes here.>
  username: ${{ secrets.REGISTRY_USERNAME }}
  password: ${{ secrets.REGISTRY_PASSWORD }}
run: |
  docker build . -t <docker registry name goes here.>/<docker image name>:${{ github.sha }}
  docker push <docker registry name goes here.>/<docker image name>:${{ github.sha }}
  docker build . -t <docker registry name goes here.>/<docker image name>:latest
  docker push <docker registry name goes here.>/<docker image name>:latest
name: Run Snyk to check Docker image for vulnerabilities
continue-on-error: true
uses: snyk/actions/docker@master
env:
  SNYK_TOKEN: ${{ secrets.SNYK_TOKEN }}
with:
  image: <docker registry name goes here.>/<docker image name>:${{ github.sha }}
  args: --file=Dockerfile
name: Upload result to GitHub Code Scanning
uses: github/codeql-action/upload-sarif@v1
with:
  sarif_file: snyk.sarif
```

Reference:

1. snyk.io
2. https://github.com/snyk/actions/tree/master/docker
3. https://github.com/pandalearnstocode/python-library-template/blob/develop/others/ci/ado_lib_publish/ado_lib_publisher.yaml
4. https://github.com/snyk/actions#getting-your-snyk-token