ODK Project Encryption Process (April 2024 ver. 1.0)

This document describes the **required** process for encrypting an ODK cloud or self-hosted project. IMPORTANT: All ODK projects **must** be encrypted as described herein. A more concise version of this document can be found within CI's Gitlab instance[1].

> **Prerequisites:**
>
> 1. The environment for the Compassion Outcomes Framework (COF) has been setup on your computer.
>
> 2. You have a login setup for a Compassion developer AWS account.
>
> 3. Visual Studio Code (VSCode) has been installed on your computer.
>
> 4. You are connected to the VPN.

For this document, we need to see three different tools as it follows:

STEP1: ODK

In ODK we need to verify the project ID number which appears on the URL as it is shown on the following capture. This can be found in any environment (Cloud or selfhost)
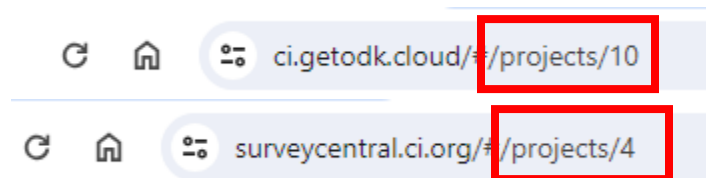
For the above examples those project IDs would be 10 and 4 respectively.

After you have found the project ID, then you can move to the next step.

STEP 2: VSCODE

Open your VSCode and on your cof.yaml file you can make changes according to the project ID and the environment. All environments are on it, so it can be selected as it is shown on the following.
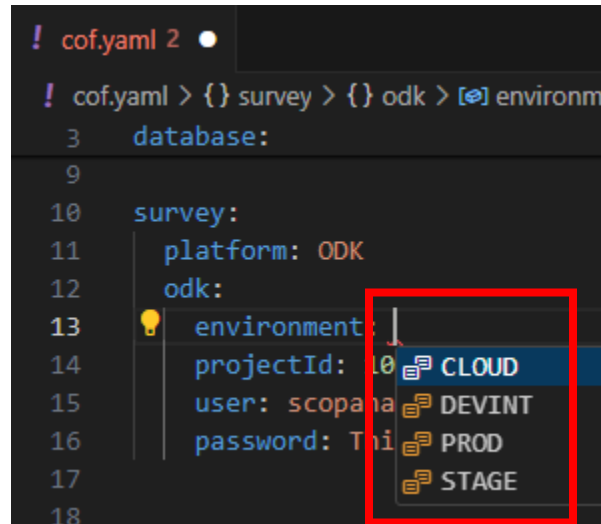
---

[1] https://gitlab.com/ciorg/sharedteams/data-works/cof/cof-tools/-/blob/master/doc/SetupEncryptionGuide.md?ref_type=heads
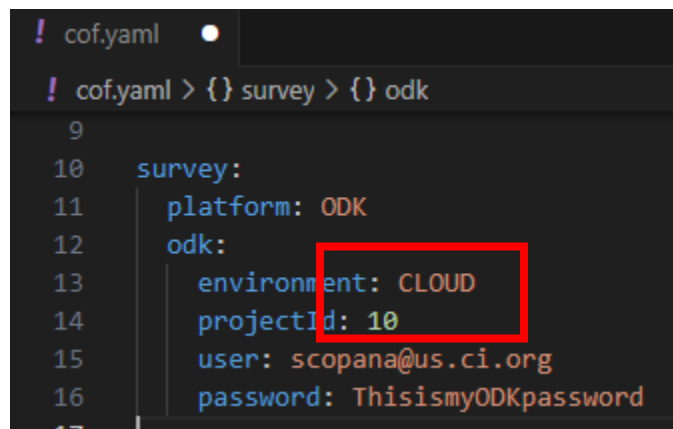
ODK Project Encryption Process (April 2024 ver. 1.0)

The following ODK environments are supported:

a. CLOUD: This is the ODK Cloud / SaaS environment.

b. DEVINT: The ODK DEVINT environment hosted by CI.

c. STAGE: The ODK STAGE environment hosted by CI.

d. PROD: The ODK PROD environment host by CI.

- For ODK Cloud example

- For ODK Selfhost example (PROD)

ODK Project Encryption Process (April 2024 ver. 1.0)


```yaml
! cof.yaml
! cof.yaml > ...
  3     database:
  9
 10     survey:
 11       platform: ODK
 12       odk:
 13         environment: PROD
 14         projectId: 4
 15         user: scopana@us.ci.org
 16         password: ThisismyODKpassword
 17
```

Once you have set your yaml file, close and save your yaml file.

Finally open your terminal and run the following commands:

We need to make sure you are logged in to AWS, running the following command: `aws sso login --profile=ba-dev`

Press ENTER and two screens will appear making sure you are in AWS. Note that the code: "JMLD-DSWG" comes from the challenge from your AWS login.
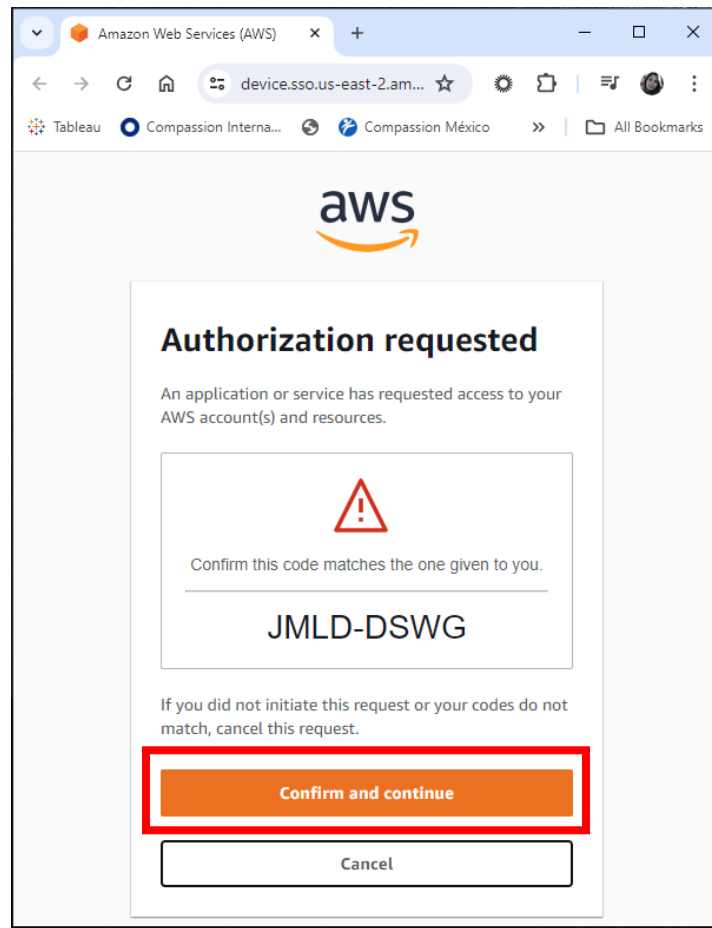
Click on Confirm and continue. Then you will see another screen:

ODK Project Encryption Process (April 2024 ver. 1.0)
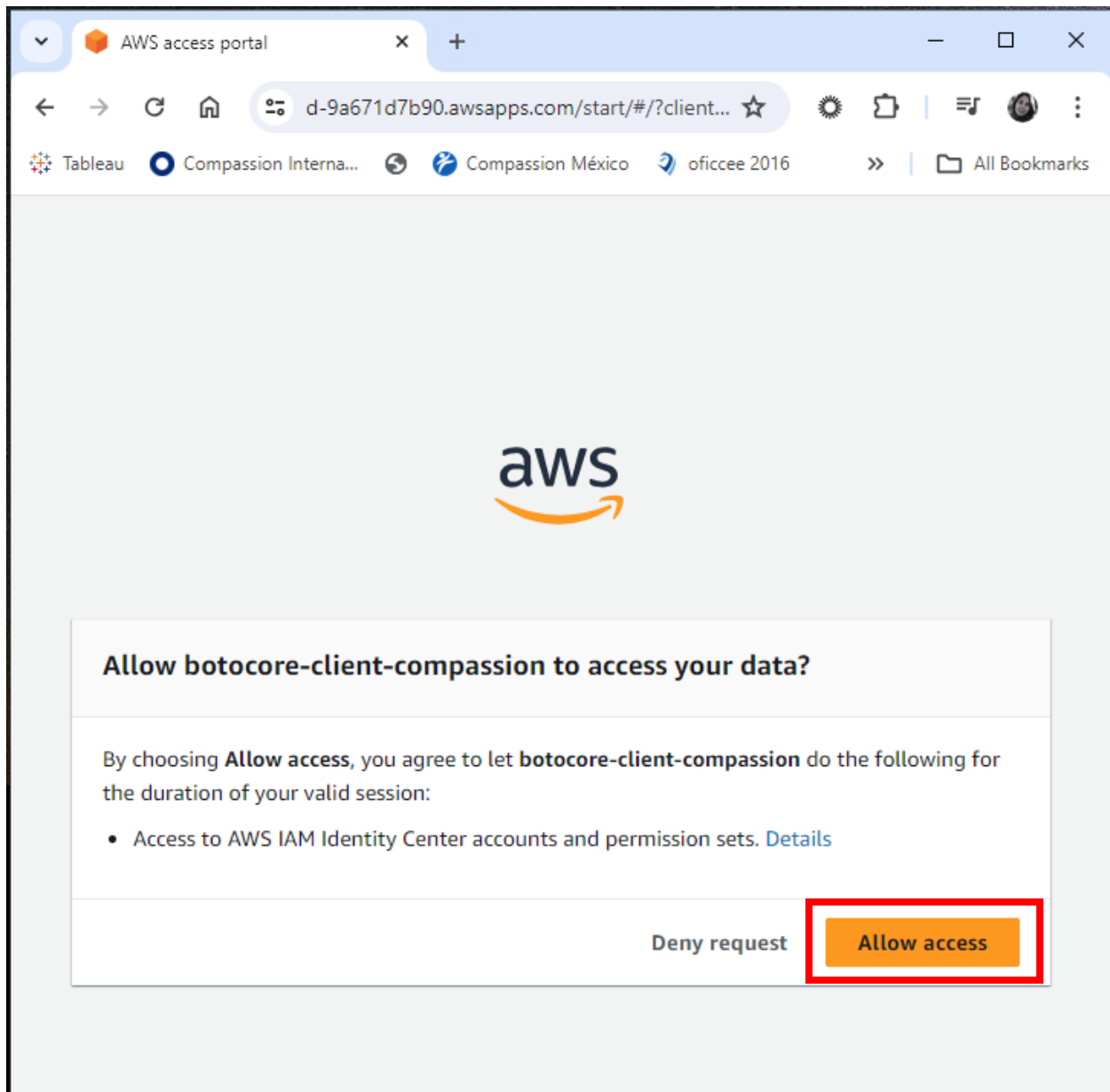
Click on Allow access.

ODK Project Encryption Process (April 2024 ver. 1.0)

The following screen will show you that a user has been successfully logged into AWS.
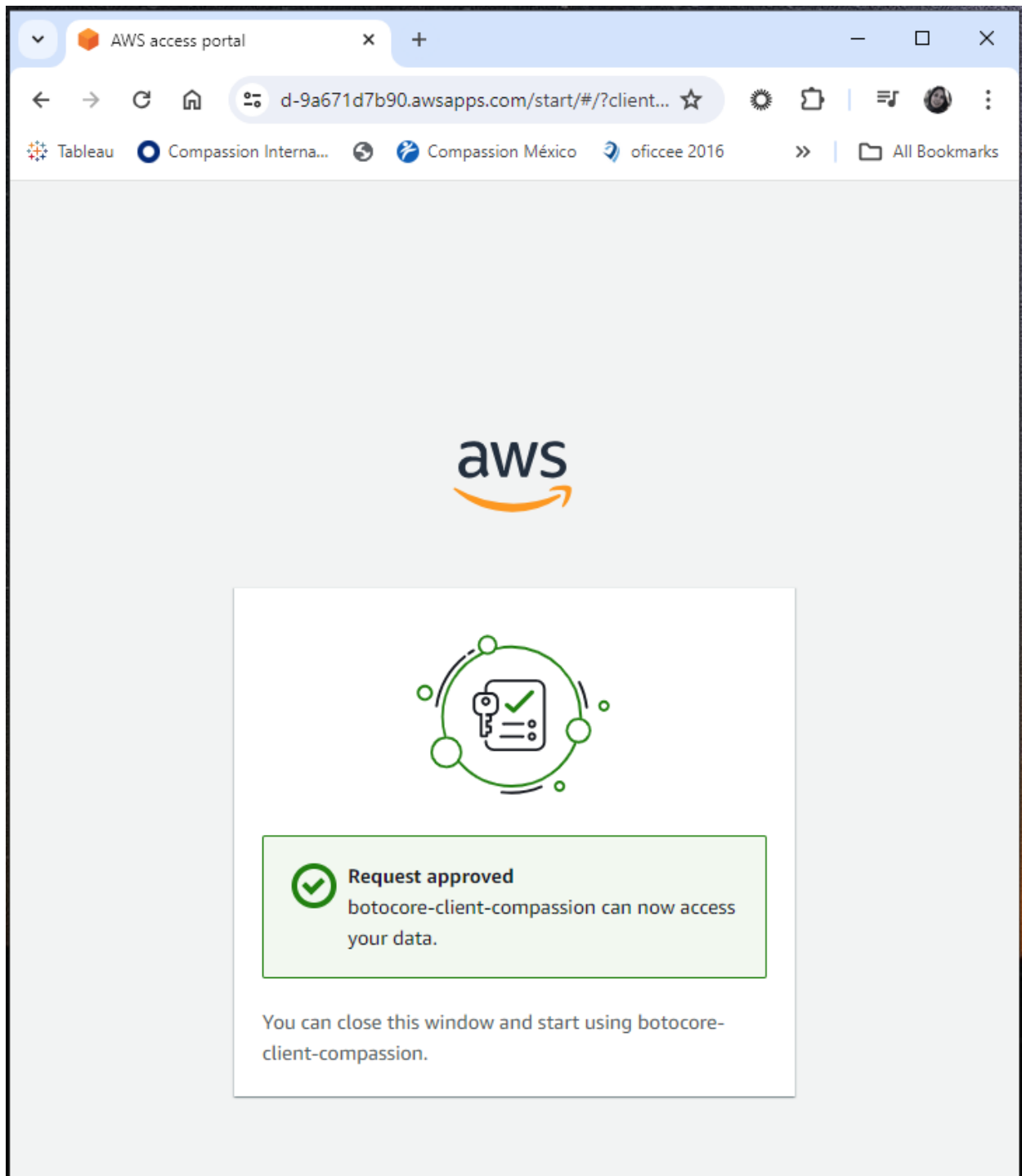
ODK Project Encryption Process (April 2024 ver. 1.0)

A user can see the same in VSCode as It Is shown:

Once you are in AWS, you can run the following command to encrypt a project: **`cof config encrypt`** then press **ENTER**

To make sure you are encrypting a project VSCode will ask for It. Typing YES or just the letter Y when It pops up. This process can be done as It Is shown:

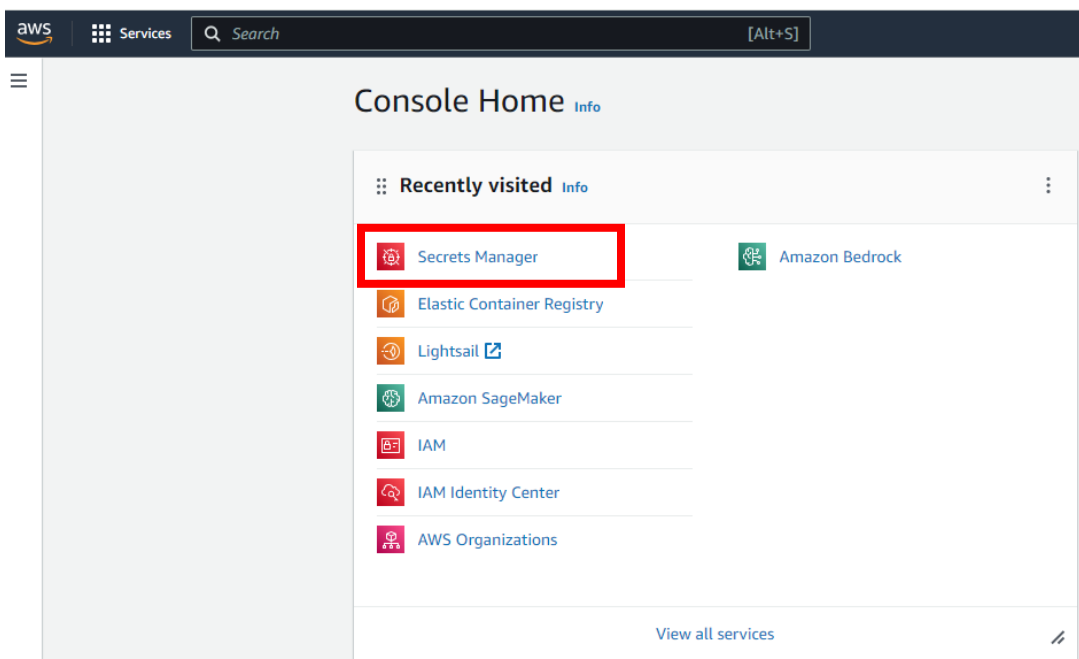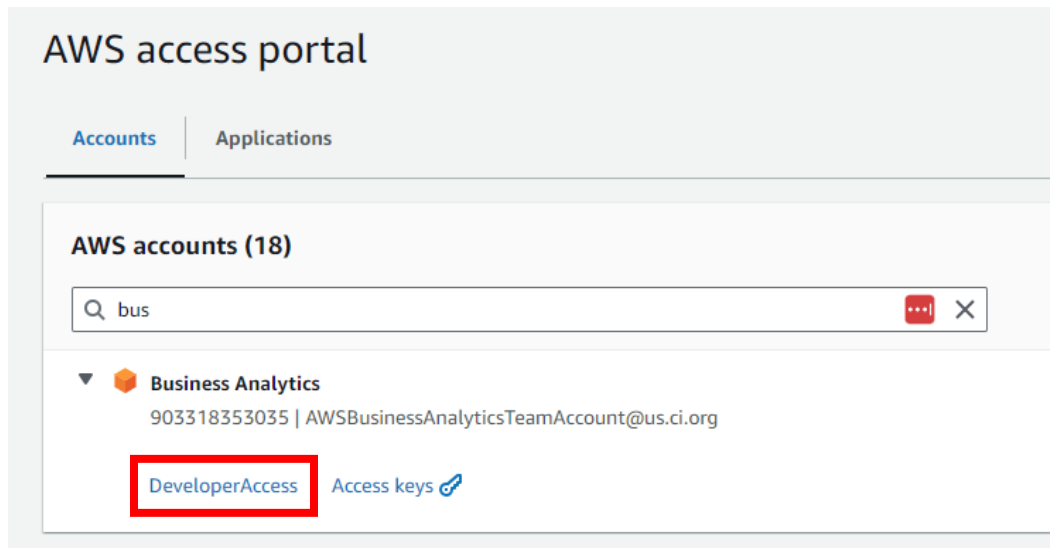# ODK Project Encryption Process (April 2024 ver. 1.0)

Press ENTER and a project Is encrypted:

ODK Project Encryption Process (April 2024 ver. 1.0)
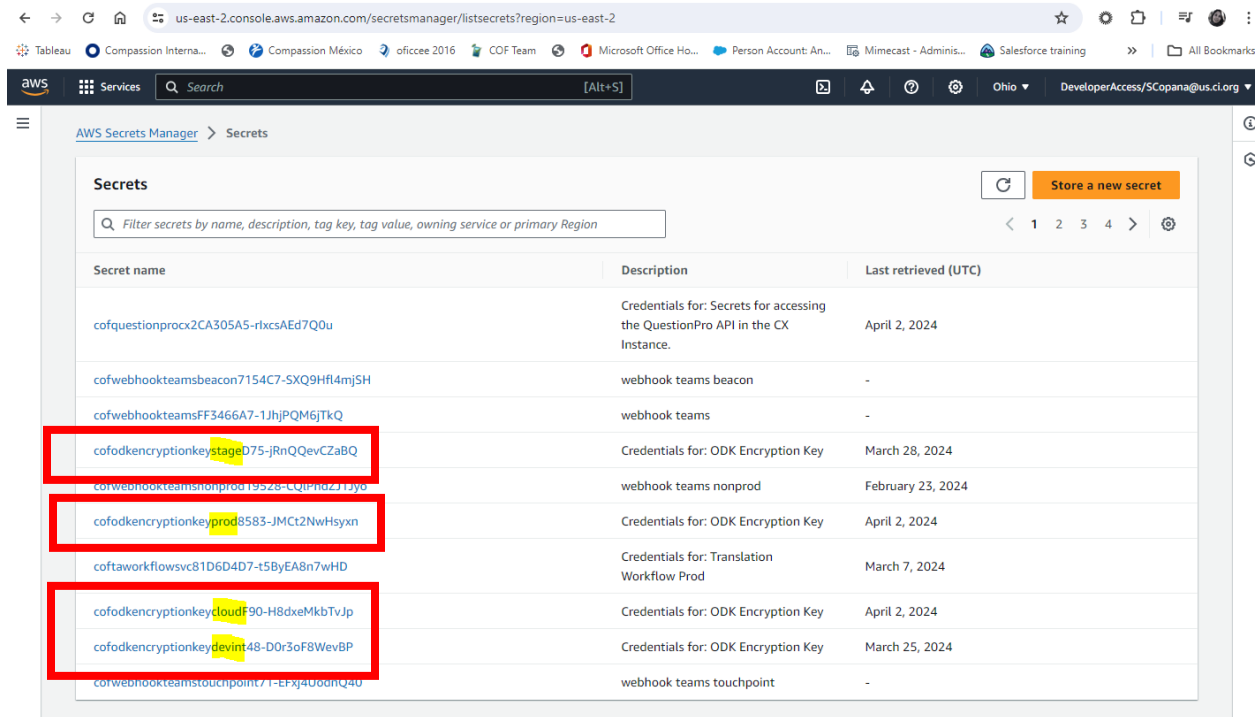
All Passphrases are stored in AWS.

If you'd like to review existing passphrases, then follow these instructions.

Get Into AWS, with a Business Analytics account on Developer Access, on Secrets

ODK Project Encryption Process (April 2024 ver. 1.0)

Finally, you can see all projects according to the environment as It Is shown on the following:

--- This Is the end of the document ---