Amazon S3 Guide for eOSCE

Last update May 2023

Welcome to the user guide for creating and configuring Amazon S3 buckets for the eOSCE applications. This guide will give you step-by-step instructions on how to create and configure an S3 bucket specifically for eOSCE.

Table of Content

1. Create/Login into your Amazon Web Services Account

1) If you don't already have an Amazon Web Services (AWS) account, you need to create one on https://aws.amazon.com/
2) Sign in into your AWS account

2. Create a new S3 bucket

1) In the top search bar, type *"S3"* and click on the *"S3"* service appearing in the results.
   Tip: Click on the little star to pin the S3 service page
2) Once the Amazon S3 panel has loaded, click on "Create Bucket"

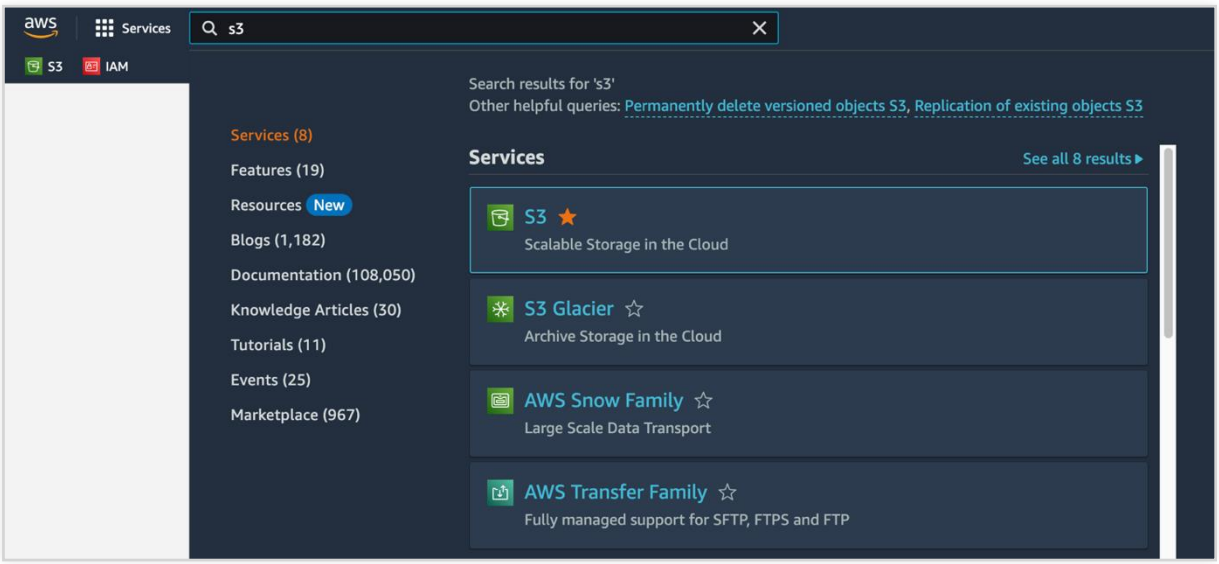


Figure 1 – Search for the S3 Service

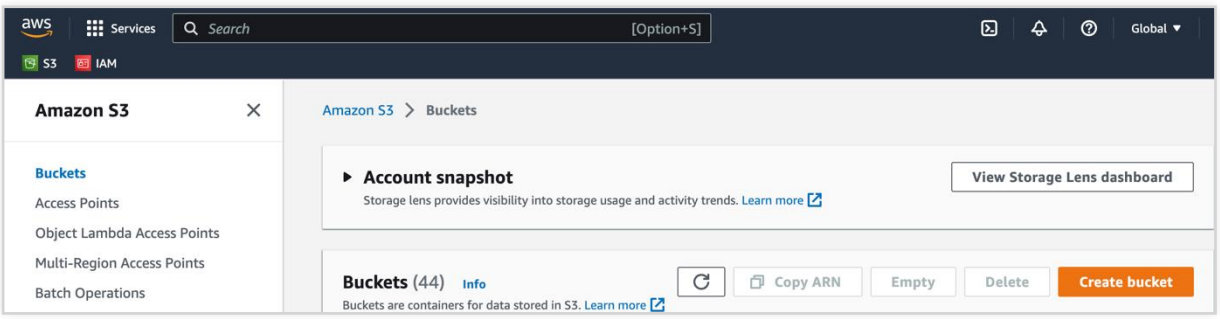


Figure 2 – Amazon S3 Buckets Page

2.1. Bucket Configuration

1) Choose a bucket name to your liking. However, you might have to be creative, as the bucket name needs to be unique worldwide.
2) Choose the nearest AWS region from your exam location.
3) Make sure to tick *"Block all public access"* to secure your bucket.
4) Enable *"Bucket Versioning"*. (Optional, but strongly recommended)

Hint: Copy the bucket name to a text editor on your computer, as you will need it for the next steps.

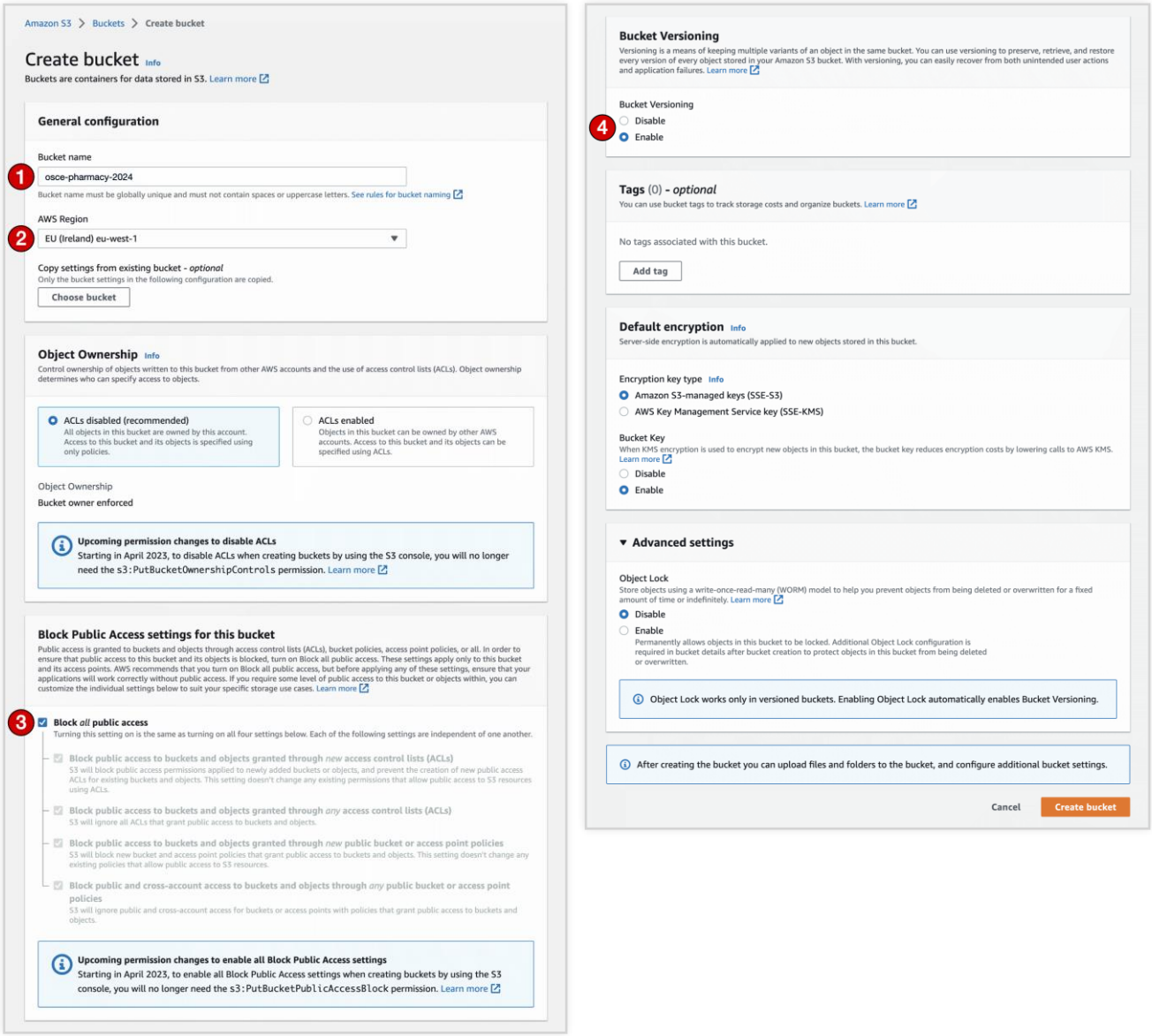


Figure 3 – New Bucket Configuration

3. Open Identity and Access Management (IAM)

1) In the top search bar, type *"IAM"* and click on the *"IAM"* service appearing in the results.
   Tip: Click on the little star to pin the IAM service page

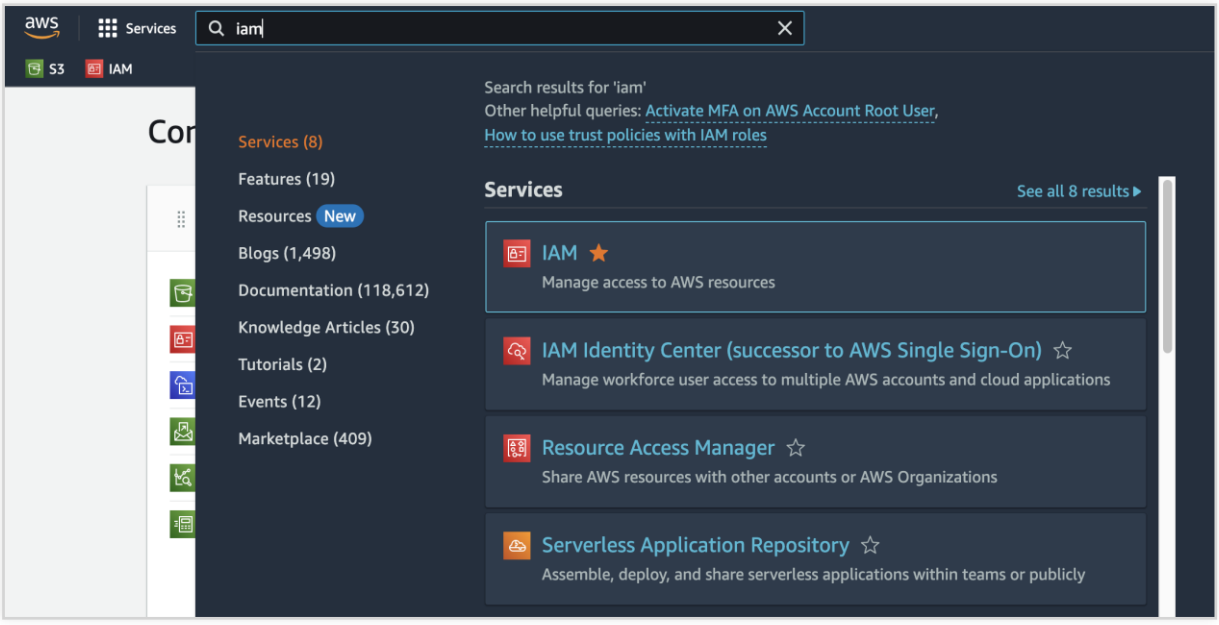


Figure 4 – Search for IAM

4. Create a New Policy

1) Click on *“Policies”* in the navigation on the left side
2) Click on *“Create policy”*

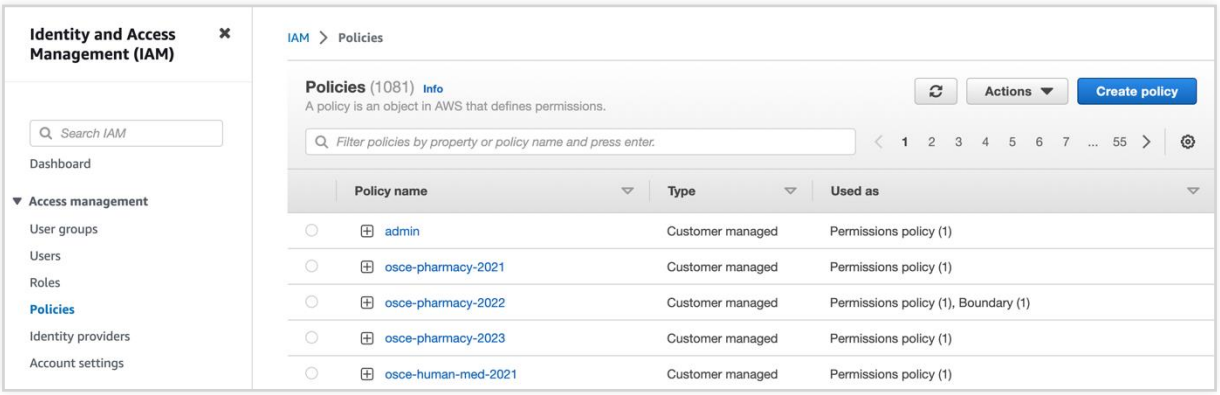


Figure 5 – Policies Page

4.1. Policy Configuration

1) Click on the "*JSON*" tab
2) Paste the policy template below or download it from our server
3) Adapt the policy to meet your needs (replace the term **BUCKET_NAME** with the name of the bucket created earlier)
4) Click on "*Next*"

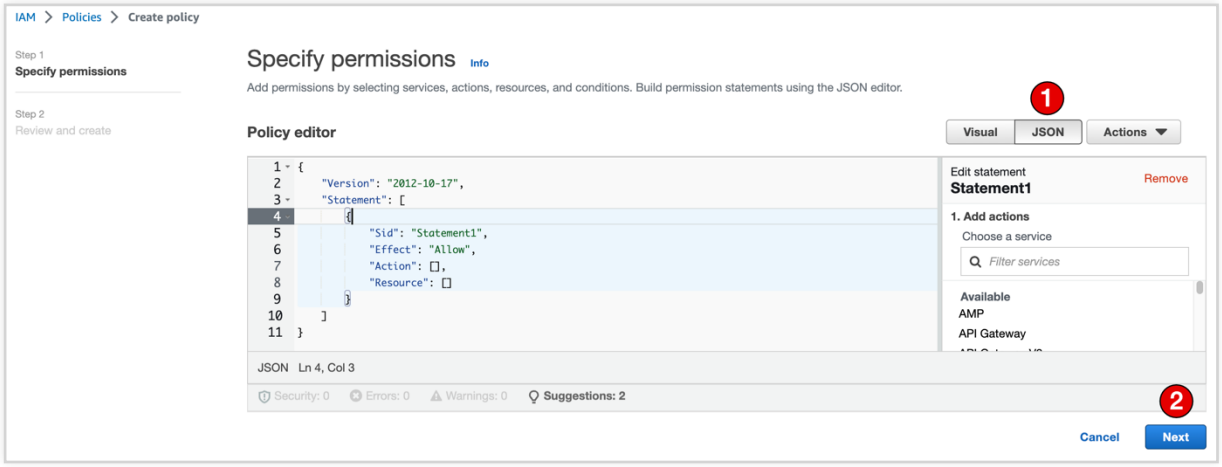


Figure 6 – Policy Configuration Text Editor

```
{
   "Version": "2012-10-17",
   "Statement":
   [
      {
      "Action": [
         "s3:*"
      ],
      "Effect": "Allow",
      "Resource": [
         "arn:aws:s3:::BUCKET_NAME",
         "arn:aws:s3:::BUCKET_NAME/*"
      ]
      },
      {
      "Action": [
         "s3:ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "*"
      }
   ]
}
```

Figure 7 – Policy Template

4.2. Policy Review

5) Use the bucket name created earlier as the policy name
6) Optionally you can add a description
7) Click on *"Create Policy"*

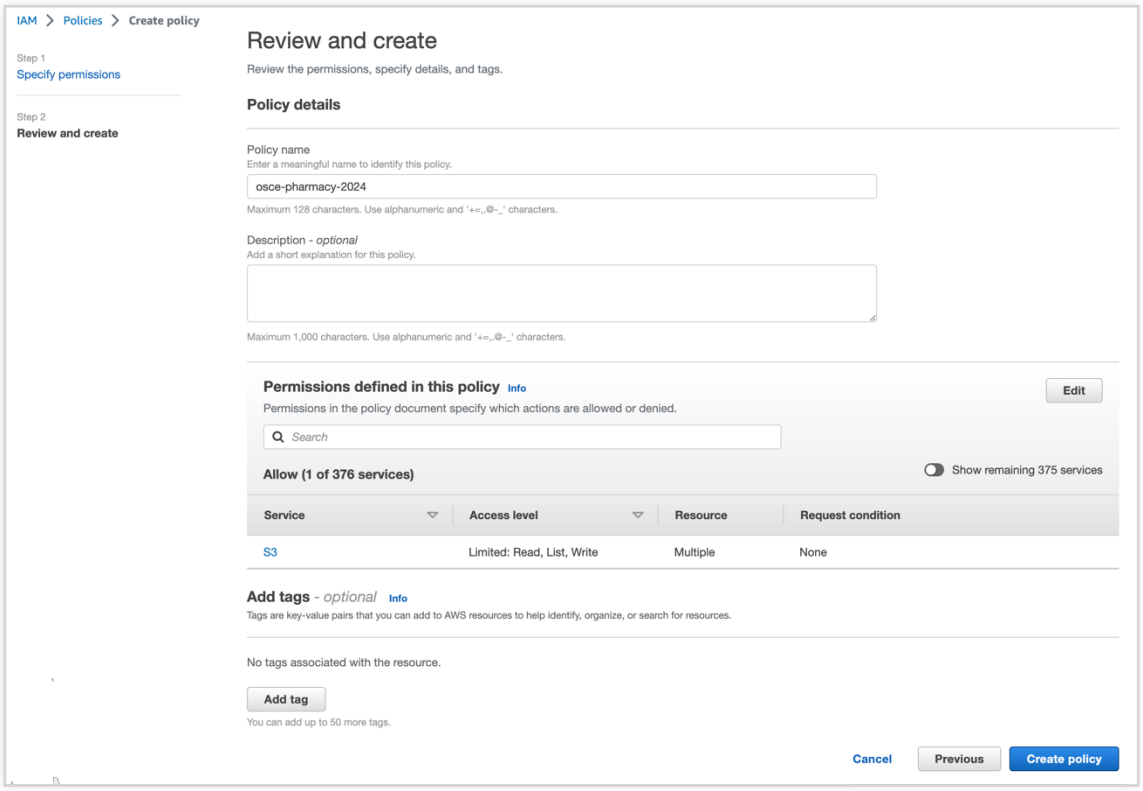


Figure 8 - Policy Review

5. Create a New User

8) Click now on *"Users"* in the navigation on the left side
9) Click on *"Add user"* to proceed

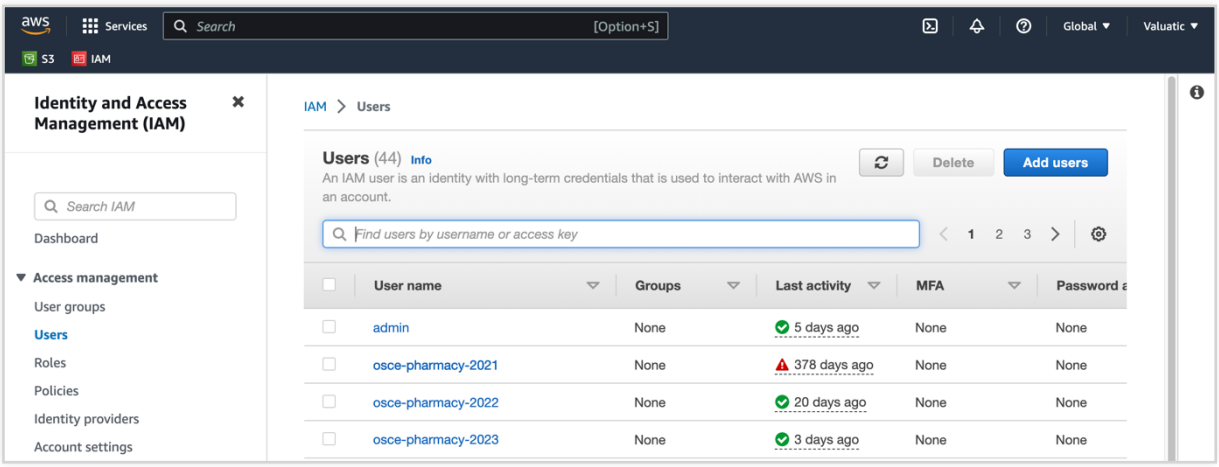


Figure 9 – Users page

5.1. User Details

1) As username, use the bucket name previously created
2) Click on *"Next"*

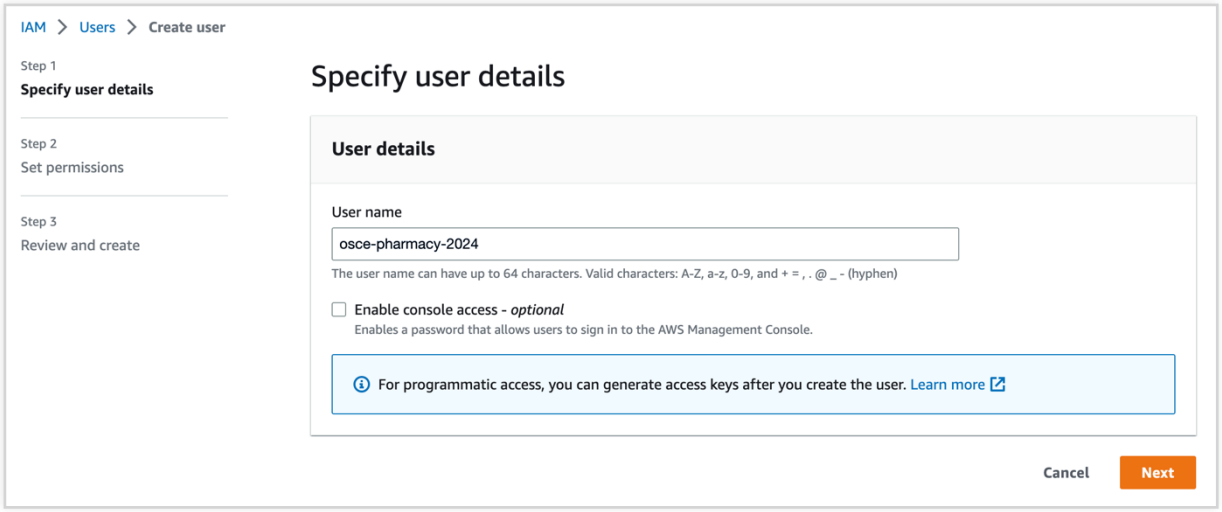


Figure 10 – Details of the new user

5.2. Permissions

1) Under *“Permissions options”* select *“Attach policies directly”*
2) Under “*Permissions policies”*, search for the name of the policy created earlier
3) Tick the checkbox in front of it
4) Click on *“Next”*

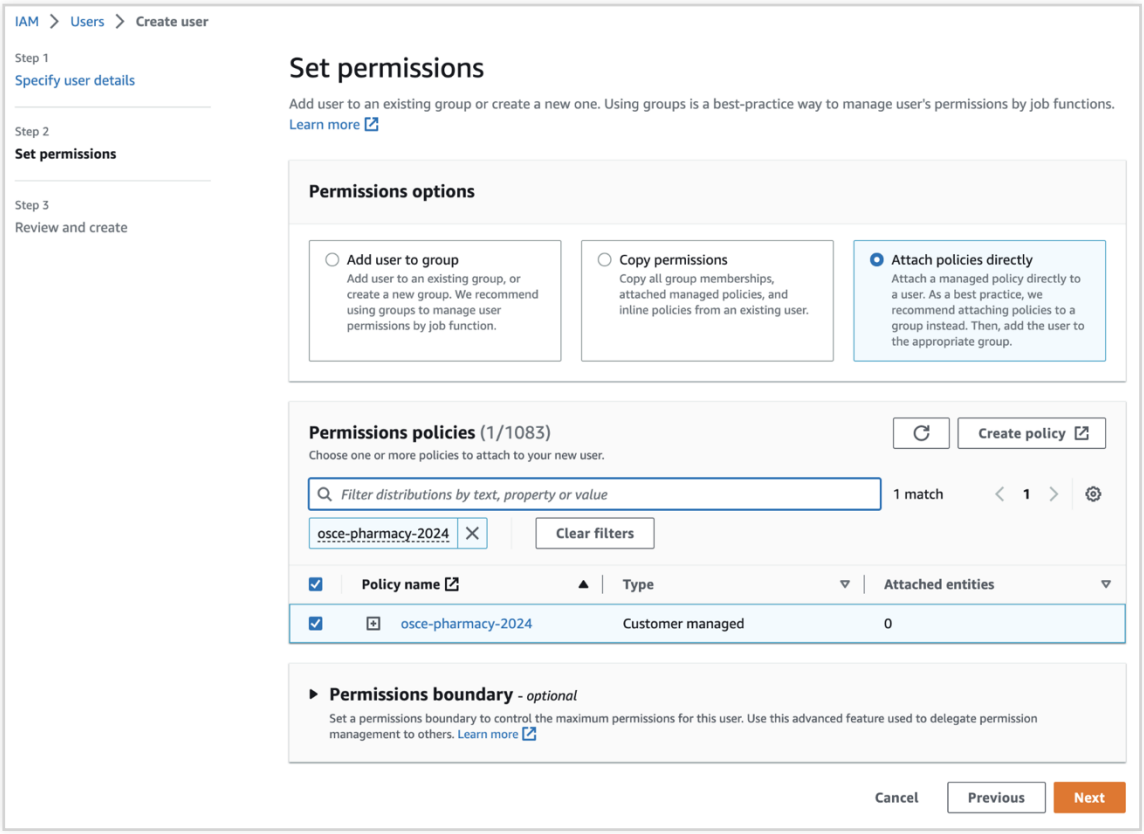


Figure 11 – Selection of the appropriate policy

5.3. Review and Create

1) Verify if the information is correct
2) Click on "*Create user*"

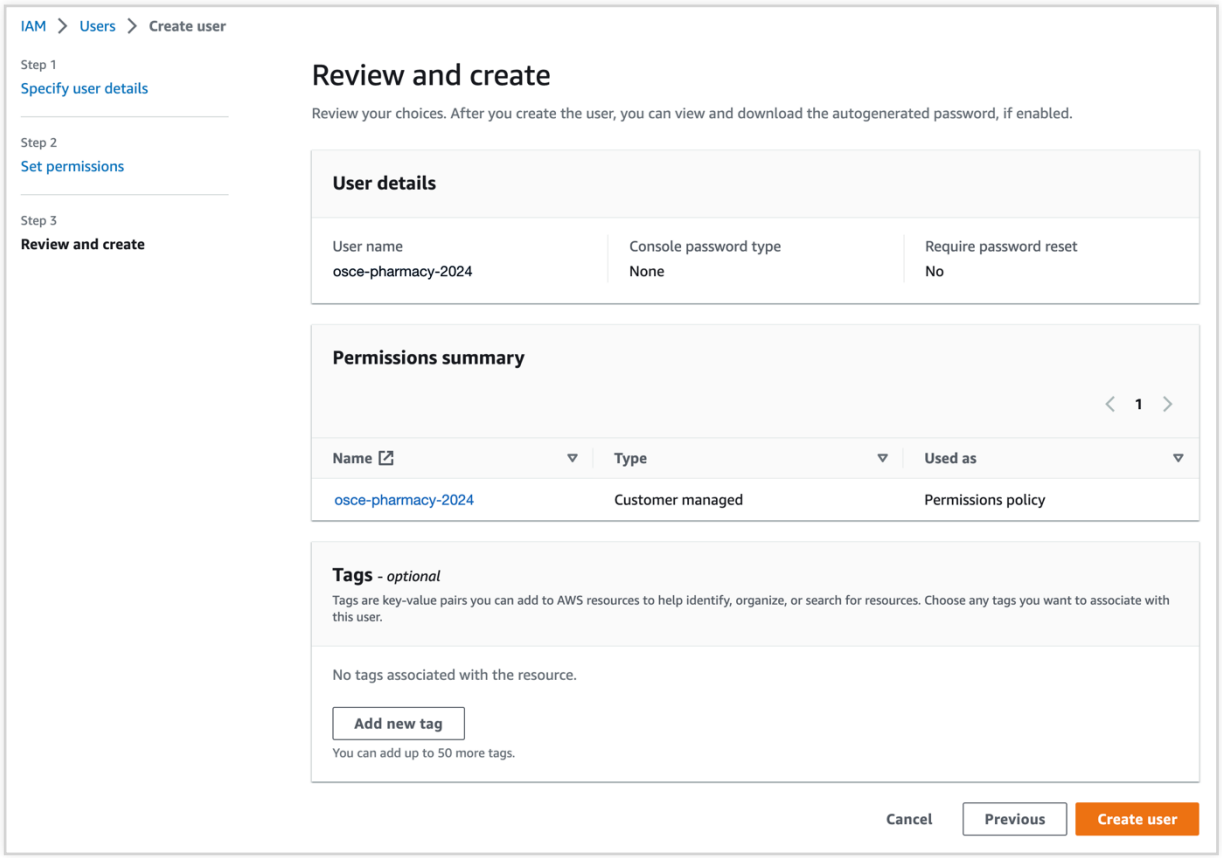


Figure 12 – Review user information

6. Create User Access Key

1) When the user is created, you are redirected to the list of users with a green banner on top. Click on *"View user"* in that banner
2) In the user details, click on the "*Security credentials*" tab
3) At the bottom on the page, click on *"Create access key"*

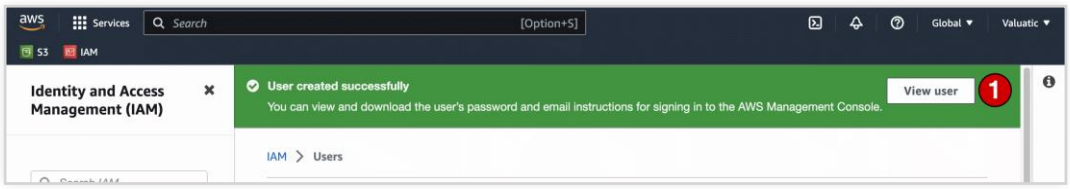


Figure 13 – User Created Success Message

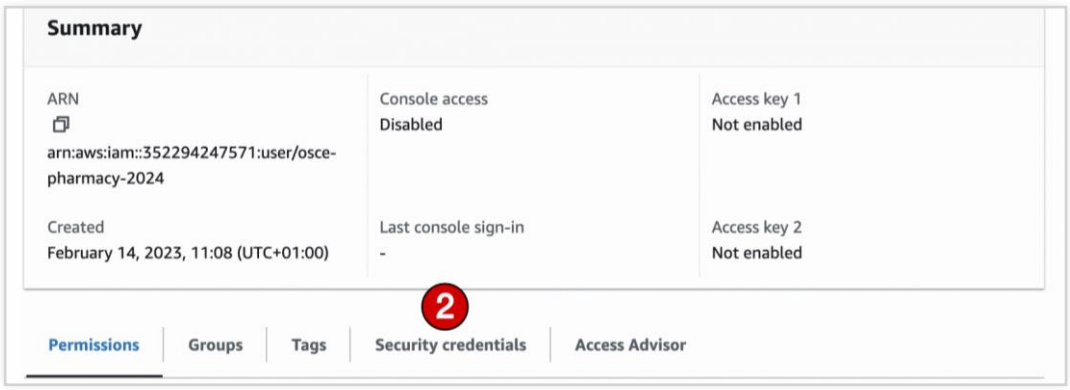


Figure 14 – User Summary and Permissions

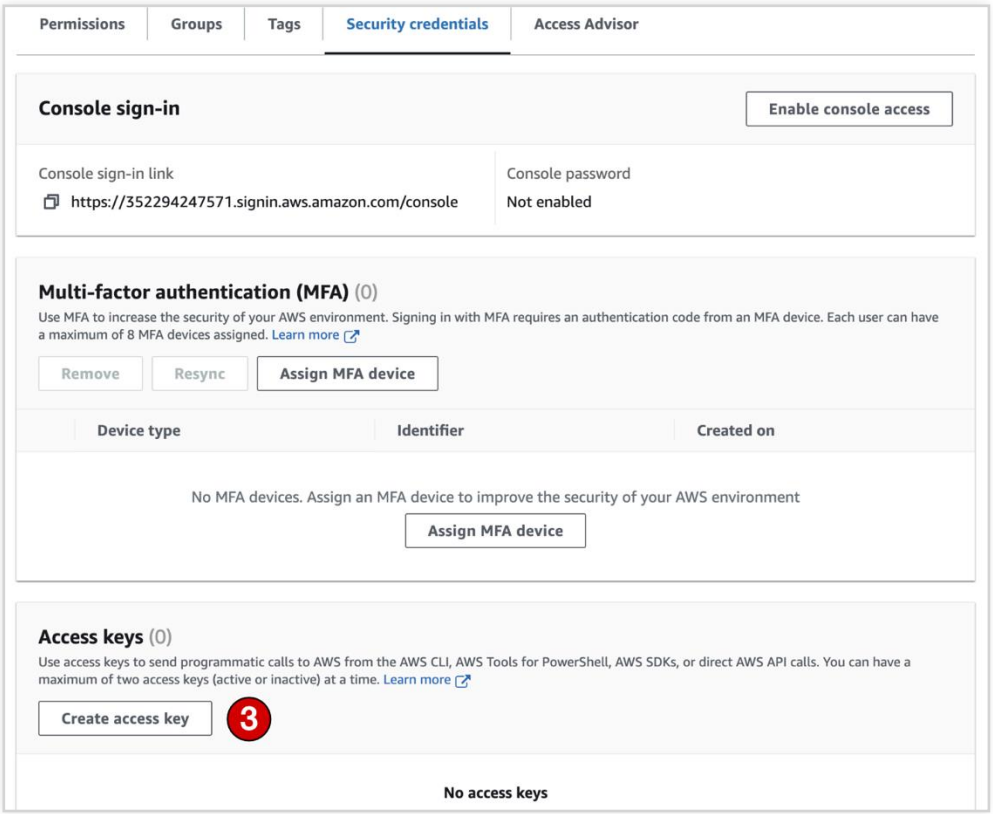


Figure 15 - User Security Credentials

6.1. Access Key Configuration

1) At step 1, select the option *"Application running outside AWS"* and click on *"Next"*
2) At step 2, use the name of the bucket previously created as *"Description tag value"*
3) Click on *"Create access key"*

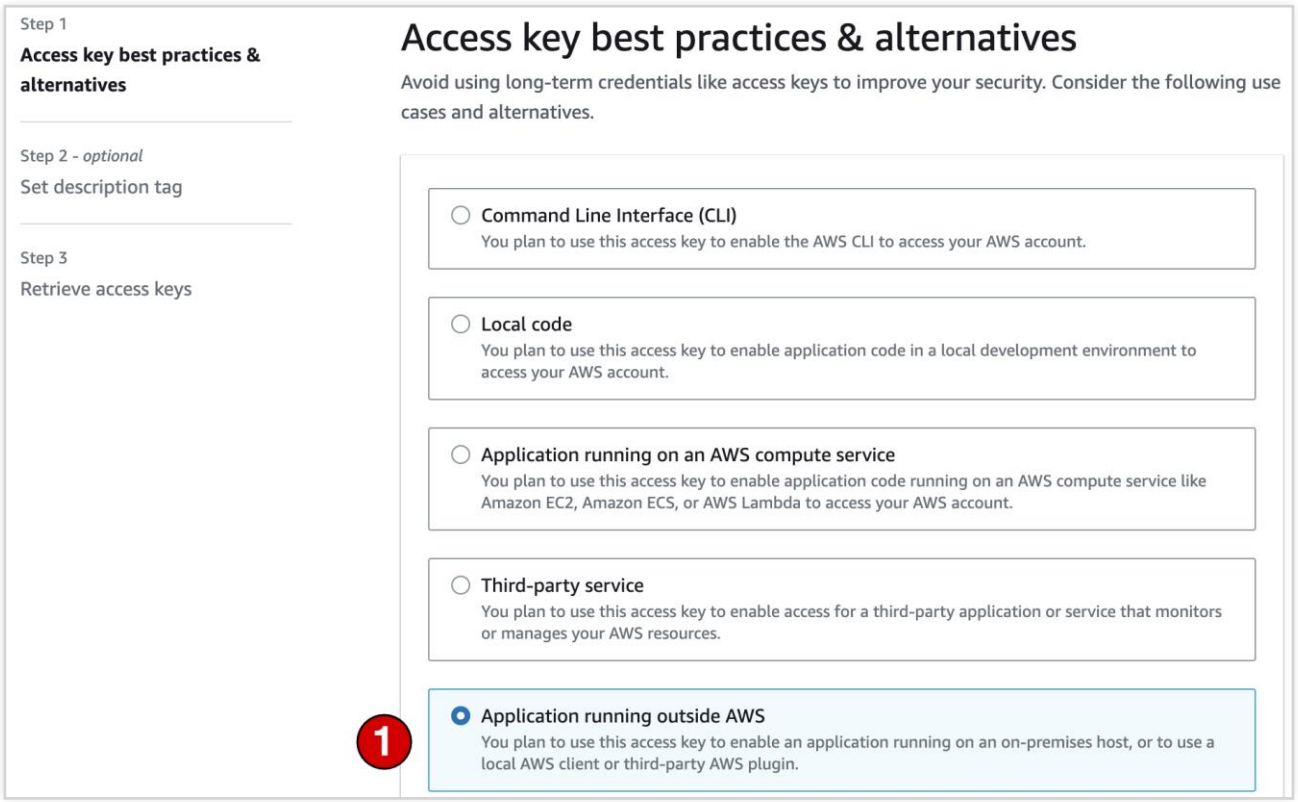


Figure 16 – Access Key Usage Selection

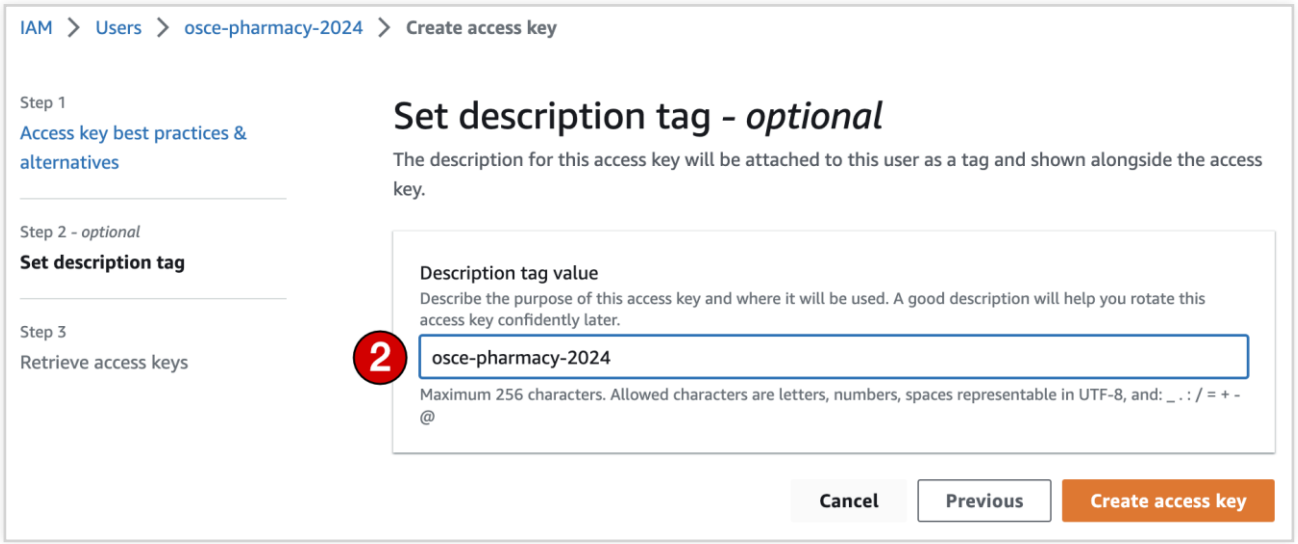


Figure 17 – Access Key Description Tag

4) Once the access key is created, you should save both the "*access key*" AND "*secret access key*" to a file on your computer. It is not possible to copy or save it later after you leave this page.
You can either copy-paste them or download them as a csv file.csv file.

Make sure to store these two keys safely and securely – they grant access to your exam files and although they still are strongly encrypted, you don't want the public to have access to your files and delete them.

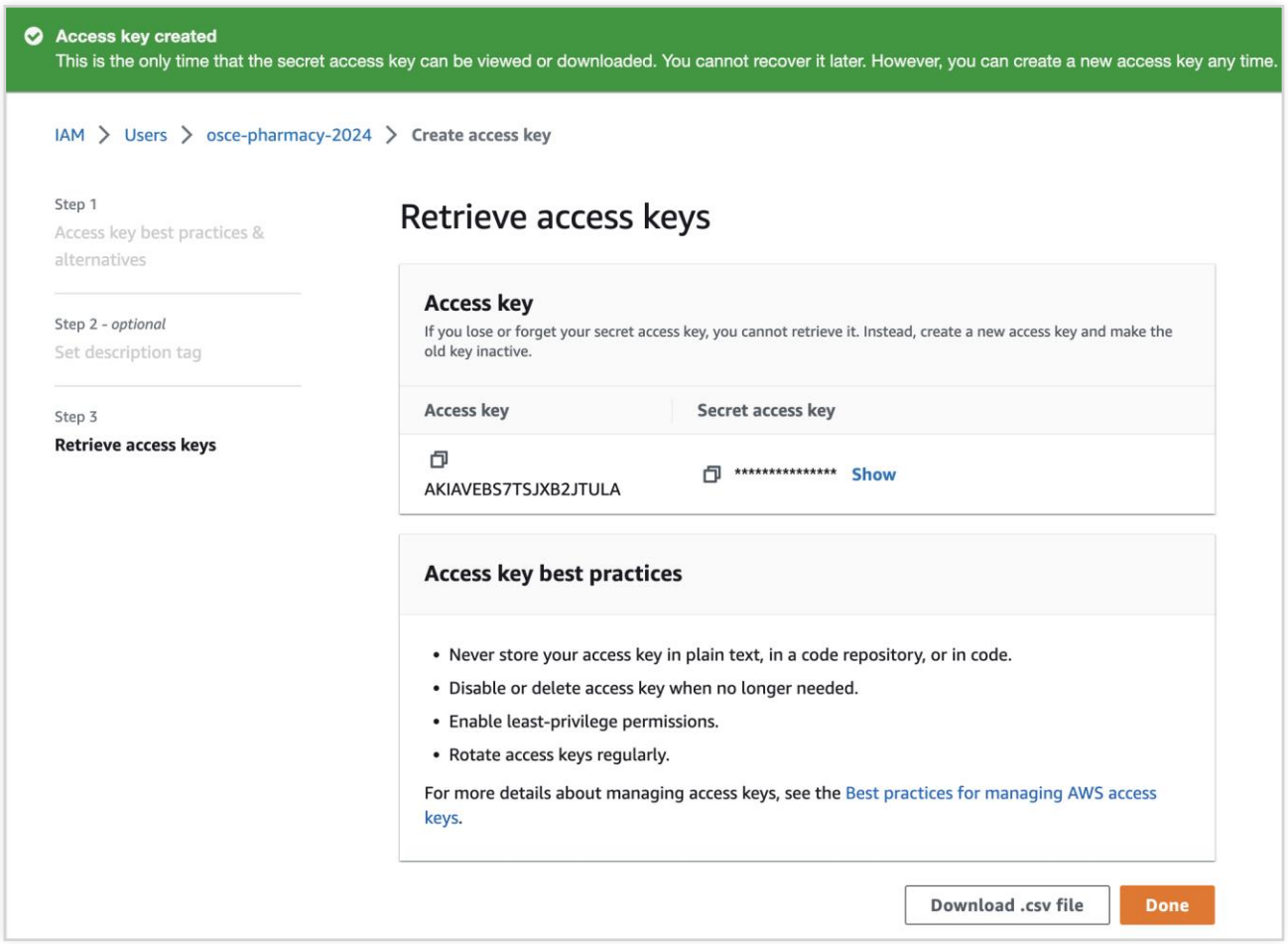
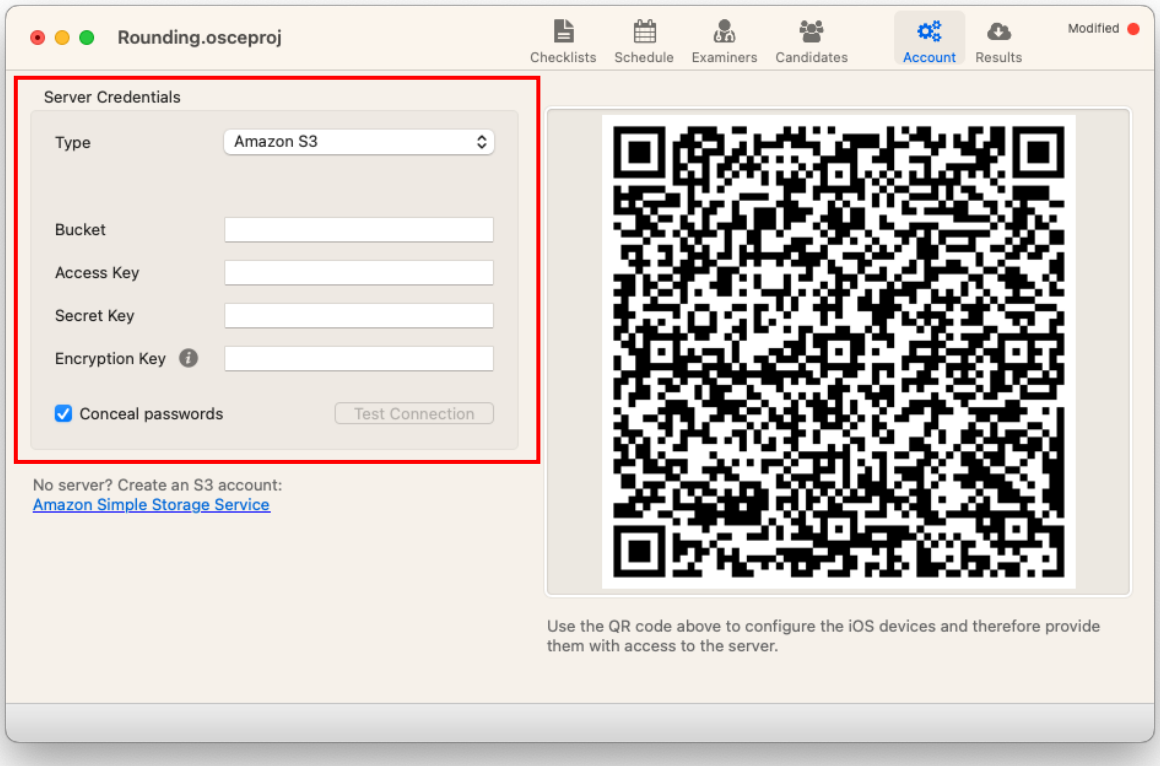


Figure 18 – Retrieve access keys

7. Success!

Once you have accomplished all these steps, you can use the credentials (*Bucket Name*, *Access Key ID* and *Secret Key*) to configure your eOSCE System to communicate with your Amazon S3 bucket.



8. Best Practice

Please note that we advise to create a new amazon S3 bucket for each exam to prevent accidental data loss and increase data security.

We strongly discourage the creation of new buckets using the application “Cyberduck” or other file manager applications. Although it is possible and may even be easier, it is considered **unsafe** and weakens the security of your AWS account.

For each new bucket, it is crucial to create new access keys to guarantee that in the event a malicious individual obtains the keys for a specific bucket, they will not be able to access data from other buckets or gain control of your AWS account.

9. Contact and Support

If you have any question regarding this manual or the eOSCE applications, please contact us at

support@eosce.ch