



# 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

Table of Content .....	2
<b>1. Create/Login into your Amazon Web Services Account .....</b>	<b>3</b>
<b>2. Create a new S3 bucket .....</b>	<b>3</b>
2.1. <i>Bucket Configuration</i> .....	4
<b>3. Open Identity and Access Management (IAM) .....</b>	<b>5</b>
<b>4. Create a New Policy .....</b>	<b>6</b>
4.1. <i>Policy Configuration</i> .....	7
4.2. <i>Policy Review</i> .....	8
<b>5. Create a New User .....</b>	<b>9</b>
5.1. <i>User Details</i> .....	9
5.2. <i>Permissions</i> .....	10
5.3. <i>Review and Create</i> .....	11
<b>6. Create User Access Key .....</b>	<b>12</b>
6.1. <i>Access Key Configuration</i> .....	13
<b>7. Success! .....</b>	<b>15</b>
<b>8. Best Practice .....</b>	<b>15</b>
<b>9. Contact and Support .....</b>	<b>16</b>



## 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"

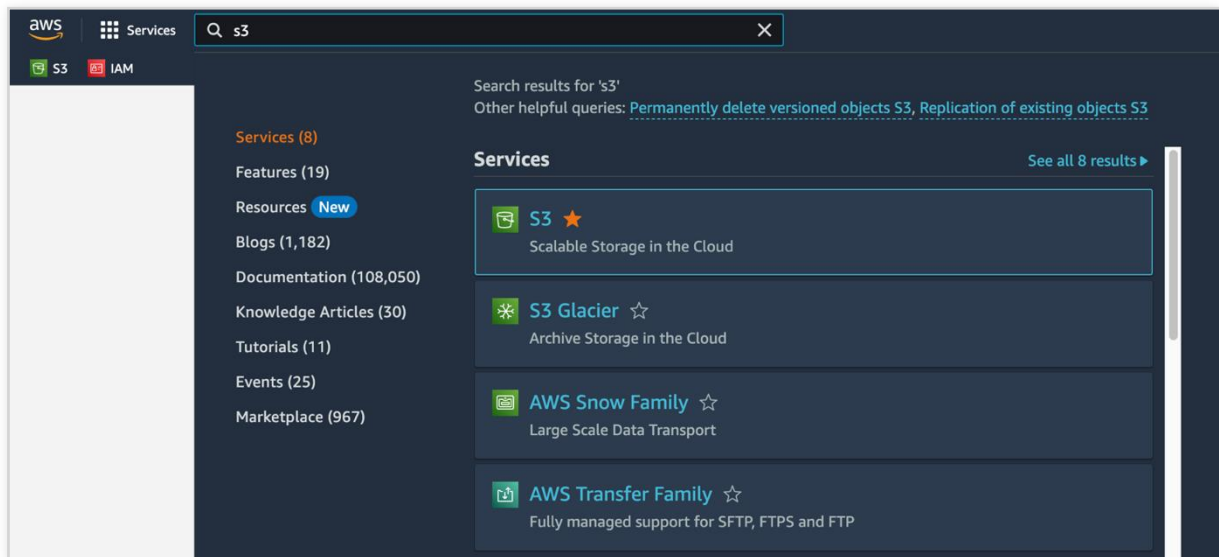


Figure 1 – Search for the S3 Service

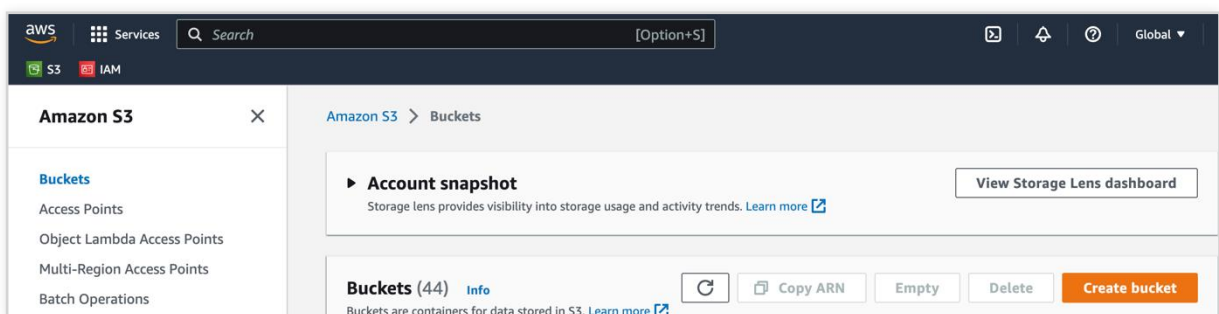


Figure 2 – Amazon S3 Buckets Page



## 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.

Amazon S3 > Buckets > Create bucket

### Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

#### General configuration

1 **Bucket name**  
osce-pharmacy-2024  
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

2 **AWS Region**  
EU (Ireland) eu-west-1

**Copy settings from existing bucket - optional**  
Only the bucket settings in the following configuration are copied.

#### Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced

Upcoming permission changes to disable ACLs  
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketOwnershipControls` permission. [Learn more](#)

#### Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

3  **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Upcoming permission changes to enable all Block Public Access settings  
Starting in April 2023, to enable all Block Public Access settings when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

#### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

4 **Bucket Versioning**  
 Disable  
 Enable

**Tags (0) - optional**  
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

#### Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption key type Info**  
 Amazon S3-managed keys (SSE-S3)  
 AWS Key Management Service key (SSE-KMS)

**Bucket Key**  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)  
 Disable  
 Enable

#### Advanced settings

**Object Lock**  
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)  
 Disable  
 Enable  
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

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*

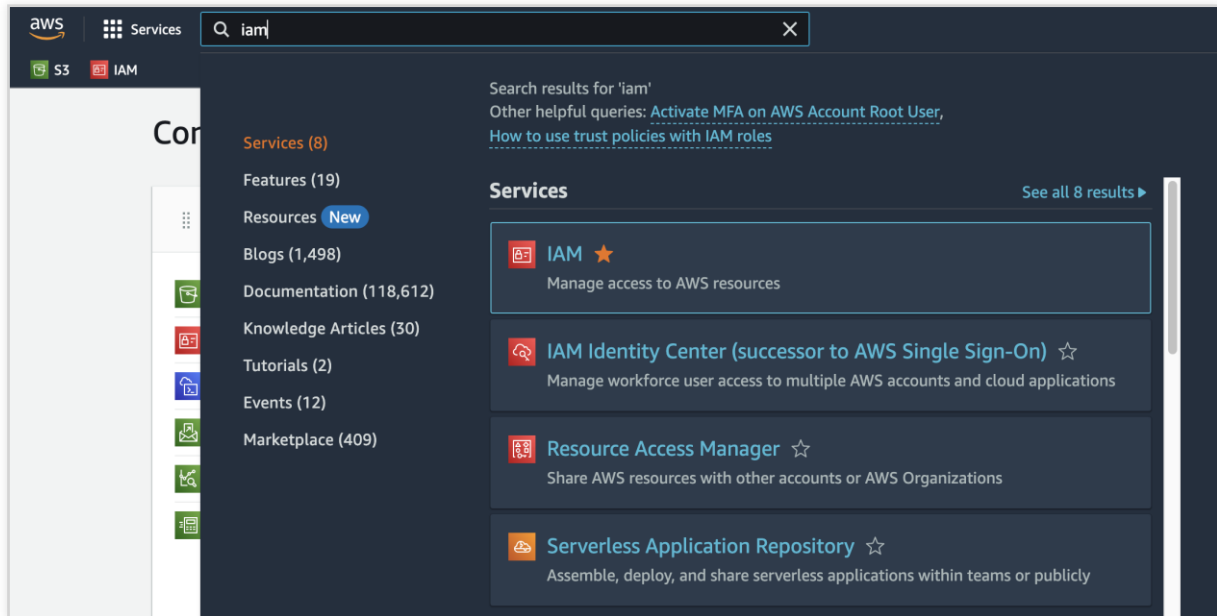


Figure 4 – Search for IAM



## 4. Create a New Policy

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

The screenshot displays the AWS IAM console interface. On the left, the navigation pane is open to 'Identity and Access Management (IAM)', with 'Policies' selected under the 'Access management' section. The main content area shows the 'Policies (1081)' page, which includes a search bar, a 'Create policy' button, and a table of existing policies.

Policy name	Type	Used as
<input type="radio"/> <a href="#">admin</a>	Customer managed	Permissions policy (1)
<input type="radio"/> <a href="#">osce-pharmacy-2021</a>	Customer managed	Permissions policy (1)
<input type="radio"/> <a href="#">osce-pharmacy-2022</a>	Customer managed	Permissions policy (1), Boundary (1)
<input type="radio"/> <a href="#">osce-pharmacy-2023</a>	Customer managed	Permissions policy (1)
<input type="radio"/> <a href="#">osce-human-med-2021</a>	Customer managed	Permissions policy (1)

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”

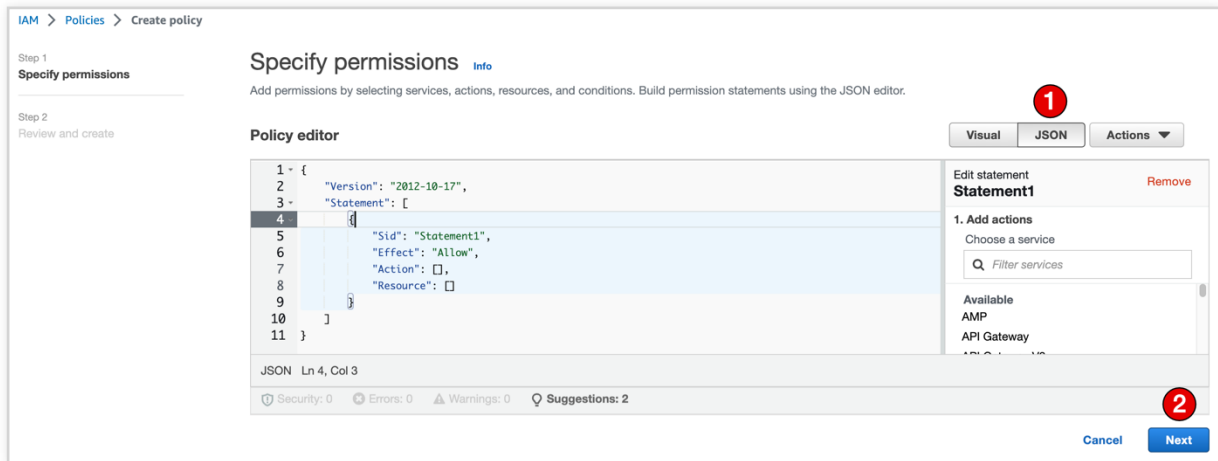


Figure 6 – Policy Configuration Text Editor

```
{
  "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”

The screenshot shows the 'Review and create' step of the AWS IAM console. The breadcrumb navigation is 'IAM > Policies > Create policy'. The left sidebar shows 'Step 1 Specify permissions' and 'Step 2 Review and create'. The main content area is titled 'Review and create' and includes the following sections:

- Policy details:** A text input field for 'Policy name' containing 'osce-pharmacy-2024'. Below it is a text area for 'Description - optional'.
- Permissions defined in this policy:** A search bar with 'Search' text. Below it is a table with columns: Service, Access level, Resource, and Request condition. The table shows one entry: S3, Limited: Read, List, Write, Multiple, None. A toggle switch 'Show remaining 375 services' is on the right.
- Add tags - optional:** A section with 'Add tag' button and text 'You can add up to 50 more tags.'

At the bottom right, there are three buttons: 'Cancel', 'Previous', and '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

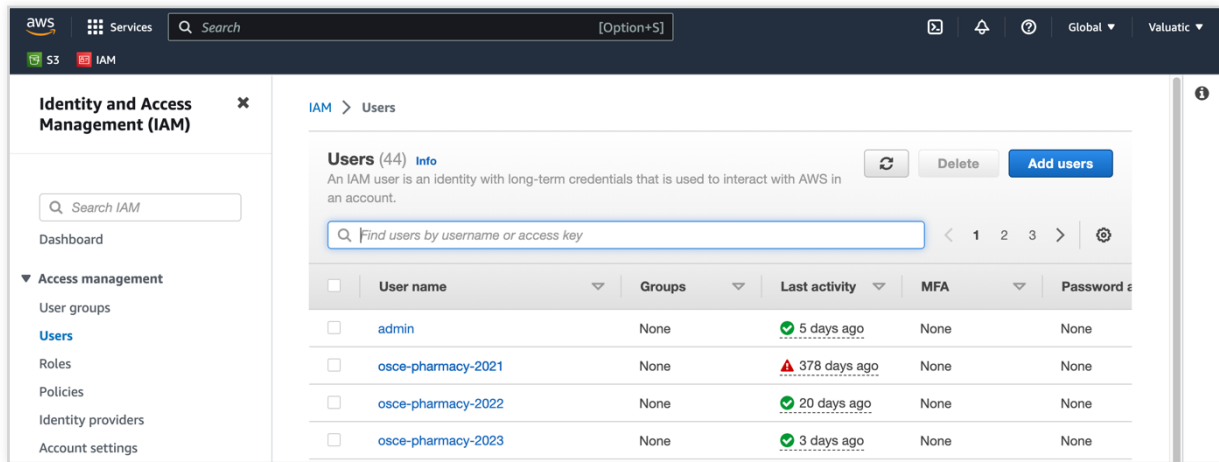


Figure 9 – Users page

### 5.1. User Details

- 1) As username, use the bucket name previously created
- 2) Click on “Next”

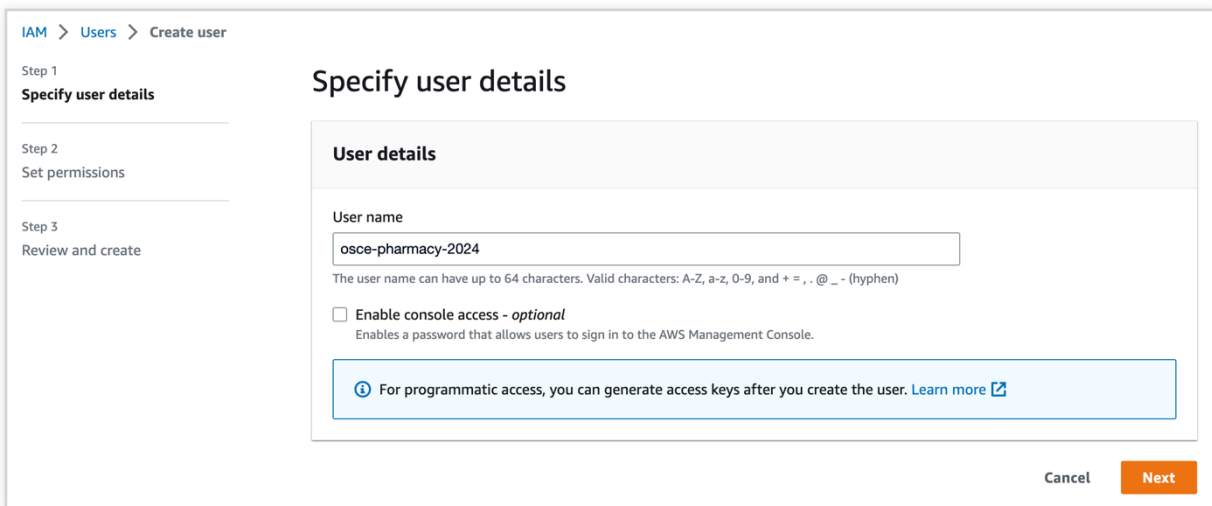


Figure 10 – Details of the new user



## 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”

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
**Set permissions**

Step 3  
Review and create

### Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

#### Permissions options

- Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

#### Permissions policies (1/1083)

Choose one or more policies to attach to your new user. [Refresh](#) [Create policy](#)

Filter distributions by text, property or value 1 match < 1 > [Settings](#)

osce-pharmacy-2024 [Clear filters](#)

<input checked="" type="checkbox"/>	<a href="#">Policy name</a>	Type	Attached entities
<input checked="" type="checkbox"/>	osce-pharmacy-2024	Customer managed	0

#### Permissions boundary - optional

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel [Previous](#) [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”

The screenshot shows the 'Review and create' step in the AWS IAM console. The breadcrumb trail is 'IAM > Users > Create user'. The left sidebar shows three steps: 'Step 1 Specify user details', 'Step 2 Set permissions', and 'Step 3 Review and create' (which is the active step). The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

**User details**

User name osce-pharmacy-2024	Console password type None	Require password reset No
---------------------------------	-------------------------------	------------------------------

**Permissions summary**

< 1 >

Name <a href="#">🔗</a>	Type	Used as
osce-pharmacy-2024	Customer managed	Permissions policy

**Tags - optional**

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Buttons: Cancel, Previous, 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”

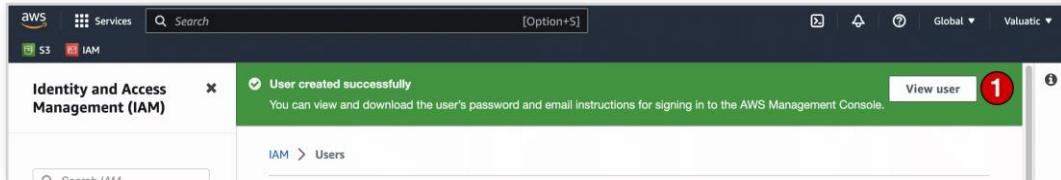


Figure 13 – User Created Success Message

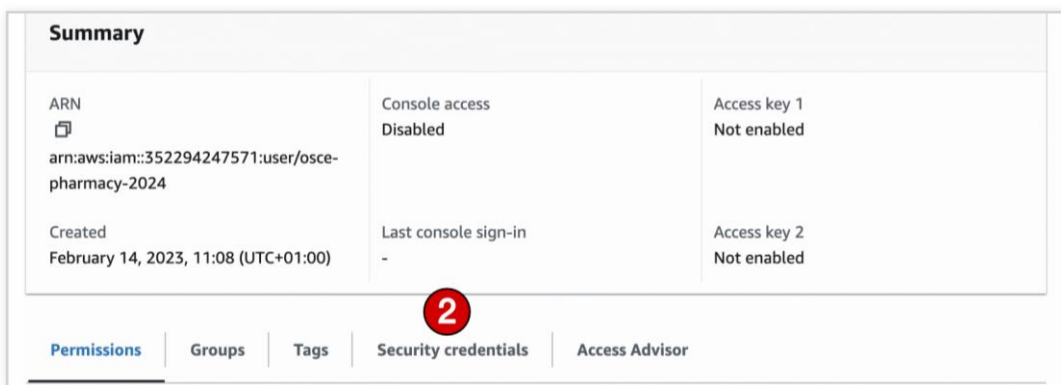


Figure 14 – User Summary and Permissions

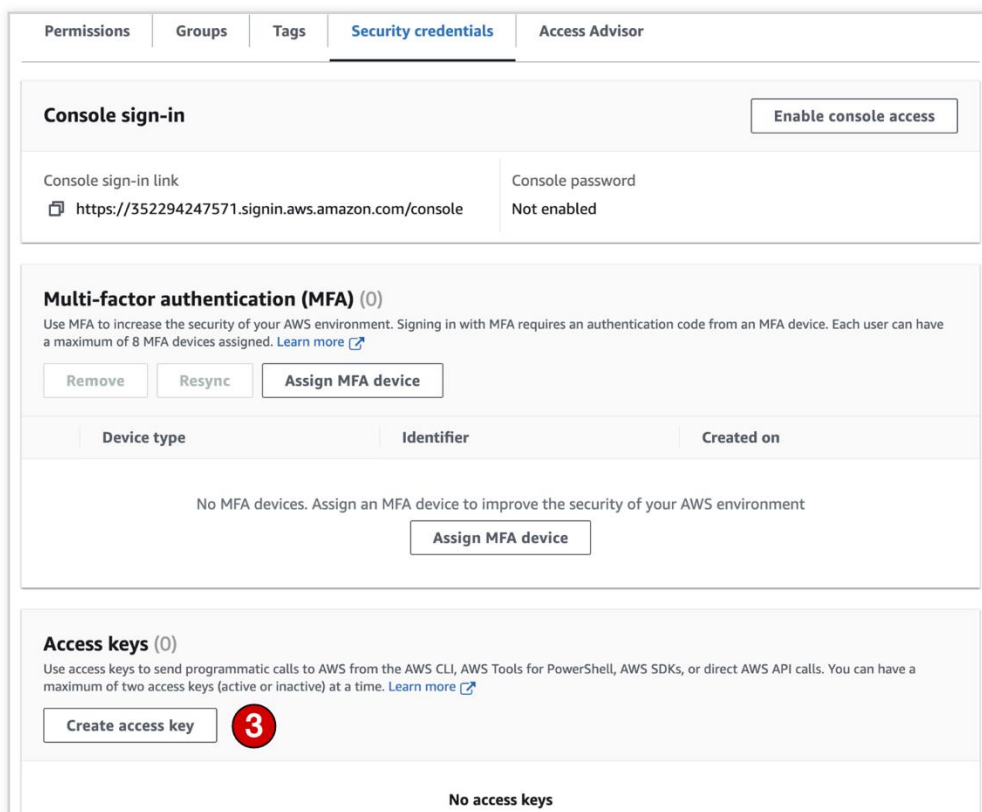


Figure 15 - User Security Credentials



## 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”

Step 1  
**Access key best practices & alternatives**

Step 2 - optional  
Set description tag

Step 3  
Retrieve access keys

### Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

- Command Line Interface (CLI)**  
You plan to use this access key to enable the AWS CLI to access your AWS account.
- Local code**  
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- Application running on an AWS compute service**  
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- Third-party service**  
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- Application running outside AWS**  
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

Figure 16 – Access Key Usage Selection

IAM > Users > osce-pharmacy-2024 > Create access key

Step 1  
[Access key best practices & alternatives](#)

Step 2 - optional  
**Set description tag**

Step 3  
Retrieve access keys

### Set description tag - optional

The description for this access key will be attached to this user as a tag and shown alongside the access key.

**Description tag value**  
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ . / = + - @

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.*

Access key created  
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > osce-pharmacy-2024 > Create access key

Step 1  
Access key best practices & alternatives

Step 2 - optional  
Set description tag

Step 3  
Retrieve access keys

### Retrieve access keys

**Access key**  
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAVEBS7TSJXB2JTULA	***** <a href="#">Show</a>

**Access key best practices**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

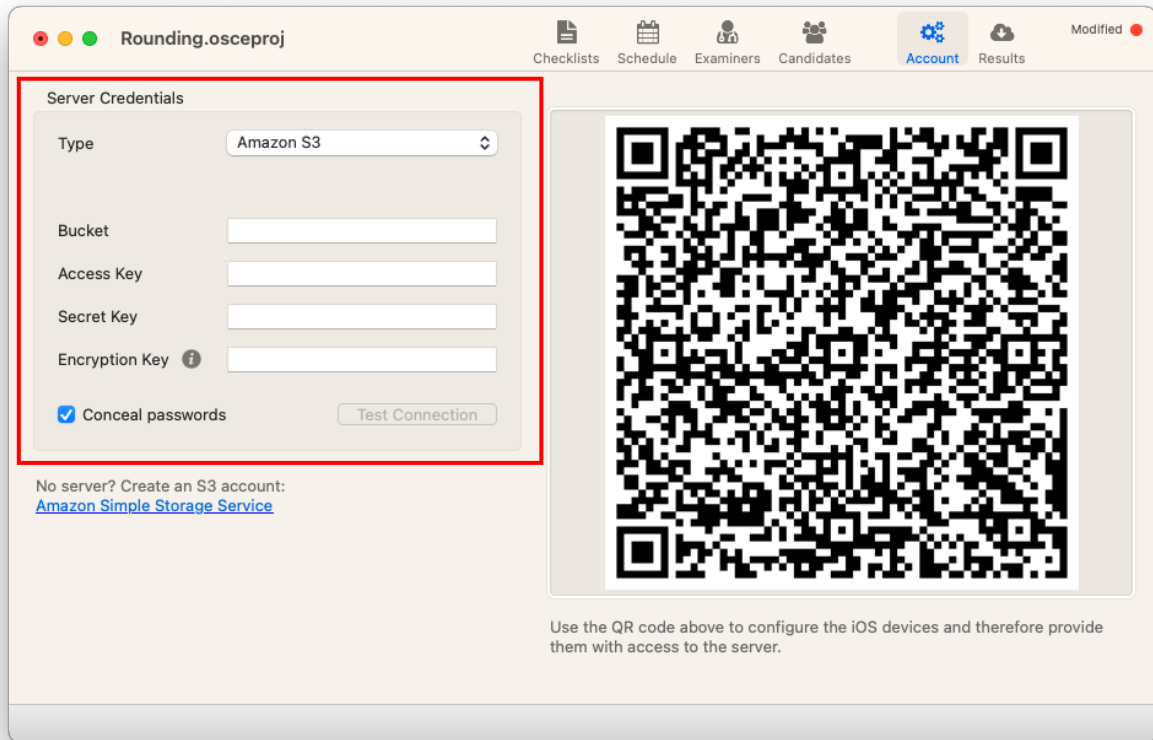
[Download .csv file](#) [Done](#)

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](mailto:support@eosce.ch)