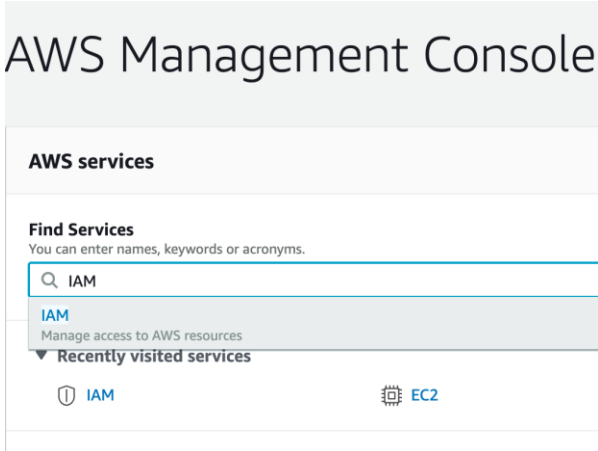


*n*Lighten™

AWS S3 Read Access Configuration Guide

Stage 1: Create IAM Security Credentials in AWS

1. Add an access key to your Amazon Web Services account to allow for remote access and give the ability to read files in S3. Log into AWS and type **IAM** in the search field.



2. By creating a Cybraics IAM user account, you can give the IAM user a unique set of security credentials. You can also grant different permissions to the user. If necessary, you can change or revoke an IAM user's permissions at any time.

For more information on IAM users and AWS best practice, read here: <http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html>

3. Create an IAM cybraics user to access your S3 bucket by clicking **Add User**. You're taken to a screen where you can create an IAM User. Select **Programmatic access**

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)


Select AWS access type


Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)


- Access type*
- Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
 - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

4. Click **Next: Permission**, do not apply group or policy configuration. **Select Next: Tags**

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

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](#)

Add user to group

▶ Set permissions boundary

[Cancel](#) [Previous](#) [Next: Tags](#)

5. Click **Next: Review**, Optional: apply tag information

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	


You can add 50 more tags.

[Cancel](#) [Previous](#) [Next: Review](#)

6. Click: **Create User**

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

 **This user has no permissions**
You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details


User name	cybraics
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Tags

No tags were added.

[Cancel](#) [Previous](#) [Create user](#)

7. After creating the user account, send the AWS Access and Secret keys to a Cybraics Engineer. **Ensure to send via encrypted email or other secure means.**

 **Success**
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://460648525681.signin.aws.amazon.com/console>

 [Download .csv](#)

	User	Access key ID	Secret access key
▶	 cybraics	AKIAWWQGV5YYS27PAZV	***** Show

Stage 2: Configuring your S3 Bucket Policy

1. Select the S3 Bucket where the cybraics user will download the required logs. Choose **Bucket Policy** and paste JSON below. Edit to match your AWS account settings. **In some cases, you may need to merge the policy listed with existing permissions. Consult with your AWS IAM team to ensure there will be no conflict.**



Bucket policy editor ARN: arn:aws:s3:::cdca-repo
Type to add a new policy or edit an existing policy in the text area below.

The block public access settings turned on for this bucket prevent granting public access.

```
1 {
2   "Statement": [
3     {
4       "Sid": "CybraicsReadOnlyAccess",
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::123456789:user/cybraics"
9         ]
10      },
11      "Action": [
12        "s3:GetObject",
13        "s3:ListBucket"
14      ],
15      "Resource": [
16        "arn:aws:s3:::MyExampleBucket",
17        "arn:aws:s3:::MyExmpleBucket/*"
18      ]
19    }
20  ]
21 }
22
```

```
{
  "Statement": [
    {
      "sid": "cybraicsReadOnlyAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789:user/cybraics"
        ]
      },
      "Action": [
```